

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CHIEF'S PREFACE

The mission of the South St. Paul Police Department is to ensure public safety and provide assistance to the community through prompt response, thorough investigation, pro-active policing and community involvement. We hold ourselves to the values of integrity, professionalism, and courtesy.

Our Department Manual was established on January 1, 1979 and is a composite of current orders, policies and rules pertaining to the department. All employees of the department are to abide by the orders, policies and provisions contained in the Department Manual.

RULES OF REASONABLENESS

Each employee is required to thoroughly review this manual and be familiar with its provisions keeping in mind there is not a substitute for common sense and reasonableness. When making decisions within this manual's guidelines, each employee should apply the rule of reasonableness in much the same way as deciding what are reasonable grounds to make an arrest. That is, would others view your actions as being reasonable under the same set of circumstances?

AMENDEMENTS, ADDITIONS, DELETIONS

This department manual is continuous work product that will be amended or altered, by the Chief of Police's approval, to meet the changing needs of the department and community. Additions or revisions will be distributed. It is your responsibility to maintain a current department manual.

If an order, policy or procedure contained in this department manual is in conflict with any past orders or directives, this manual will supersede those past orders and/or directives.

If any provisions contained in this manual are in conflict with state laws, civil service regulations or contract, then the appropriate statute will supersede those provisions; local ordinance or civil service regulation shall not be superseded by any portion or provision of this manual. If any portion of this manual is found to be illegal or otherwise incorrect or inapplicable, such finding shall not affect the validity of the remaining portion of the department manual.

The Chief of Police expressly reserves all management rights granted by the Civil Service Commission, the Mayor and City Council, the laws and statutes of the State of Minnesota, the ordinances of the City of South Saint Paul and the articles of the Agreement.

All general orders, policies, procedures, other contents, amendments and additions contained in the Department Manual, upon its adoption by the Chief of Police, are in effect continuously.

Brian J Wicke

Chief of Police

South Saint Paul Police Department

S Saint Paul PD Policy Manual

LAW ENFORCEMENT CODE OF ETHICS

As a law enforcement officer, my fundamental duty is to serve the community; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation and the peaceful against abuse or disorder; and to respect the constitutional rights of all to liberty, equality and justice.

I will keep my private life unsullied as an example to all and will behave in a manner that does not bring discredit to me or to my agency. I will maintain courageous calm in the face of danger, scorn or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed both in my personal and official life, I will be exemplary in obeying the law and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, political beliefs, aspirations, animosities or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or ill will, never employing unnecessary force or abuse and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of police service. I will never engage in acts of corruption or bribery, nor will I condone such acts by other police officers. I will cooperate with all legally authorized agencies and their representatives in the pursuit of justice.

I know that I alone am responsible for my own standard of professional performance and will take every reasonable opportunity to enhance and improve my level of knowledge and competence.

I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession . . . law enforcement.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Table of Contents

CHIEF'S PREFACE.	1
Law Enforcement Code of Ethics.	2
Chapter 1 - Law Enforcement Role and Authority.	7
100 - Law Enforcement Authority.	8
101 - Chief Executive Officer.	10
102 - Oath of Office.	11
103 - Policy Manual.	12
Chapter 2 - Organization and Administration.	15
200 - Organizational Structure and Responsibility.	16
201 - Departmental Directive and Special Orders.	18
202 - Emergency Operations Plan.	19
203 - Electronic Mail.	20
204 - Supervision Staffing Levels.	21
205 - Retiree Concealed Firearms.	22
206 - Handgun Purchase and Transfer Permit.	24
207 - Training.	26
Chapter 3 - General Operations.	29
300 - Use of Force.	30
301 - Handcuffing and Restraints.	38
302 - Control Devices.	42
303 - Conducted Energy Device.	46
304 - Officer-Involved Shootings and Deaths.	51
305 - Firearms.	60
306 - Vehicle Pursuits.	68
307 - Officer Response to Calls.	81
308 - Canines.	84
309 - Domestic Abuse.	92
310 - Search and Seizure.	99
311 - Temporary Custody of Juveniles.	101
312 - Adult Abuse.	110
313 - Discriminatory Harassment.	115
314 - Child Abuse.	120
315 - Missing Persons.	128
316 - Public Alerts.	138
317 - Victim and Witness Assistance.	142
318 - Standards of Conduct.	145
319 - Hate or Prejudice Crimes.	152
320 - Information Technology Use.	155
321 - Report Preparation.	159
322 - News Media Relations.	163

South Saint Paul Police Department

S Saint Paul PD Policy Manual

323 - Court Appearance and Subpoenas.	167
324 - Outside Agency Assistance.	169
325 - Registered Predatory Offender.	171
326 - Major Incident Notification.	177
328 - Death Investigation.	179
329 - Identity Theft.	183
330 - Private Persons Arrests.	185
331 - Limited English Proficiency Services.	187
333 - Pupil Arrest Reporting.	195
334 - Biological Samples.	196
335 - Chaplains.	198
336 - Service Animals.	204
337 - Police Reserve and Explorer Programs.	207
338 - Native American Graves Protection and Repatriation.	213
339 - Off-Duty Law Enforcement Actions.	215
340 - Department Use of Social Media.	217
343 - Extreme Risk Protection Orders.	220
344 - ADA Compliance.	224
 Chapter 4 - Patrol Operations.	 233
400 - Patrol Function.	234
401 - Bias-Based Policing.	236
402 - Crime and Disaster Scene Integrity.	239
403 - Ride-Along Policy.	241
404 - Hazardous Material Response.	244
405 - Hostage and Barricade Incidents.	246
406 - Response to Bomb Calls.	251
407 - Civil Commitments.	256
408 - Citation Releases.	259
409 - Foreign Diplomatic and Consular Representatives.	261
410 - Rapid Response and Deployment.	265
412 - Immigration Violations.	268
413 - Patrol Rifles.	271
414 - Aircraft Accidents.	273
415 - Field Training Officer Program.	277
416 - Shift Sergeants.	280
417 - Mobile Video Recorders.	281
418 - Mobile Digital Computer Use.	287
419 - Policy Title.	290
420 - Portable Audio/Video Recorders.	291
421 - Foot Pursuits.	297
422 - Automated License Plate Readers (ALPR).	302
423 - Criminal Conduct on School Buses.	306
424 - Public Recording of Law Enforcement Activity.	307
425 - Medical Aid and Response.	310
426 - First Amendment Assemblies.	313
427 - Crisis Intervention Incidents.	320

South Saint Paul Police Department

S Saint Paul PD Policy Manual

428 - Civil Disputes.	325
429 - Medical Cannabis.	327
430 - Suspicious Activity Reporting.	330
432 - Body-Worn Cameras.	332
433 - School Resource Officers.	343
Chapter 5 - Traffic Operations.	346
500 - Traffic Function and Responsibility.	347
501 - Traffic Collisions.	349
502 - Vehicle Towing.	353
503 - Disabled Vehicles.	356
504 - Abandoned Vehicle Violations.	357
Chapter 6 - Investigation Operations.	359
600 - Investigation and Prosecution.	360
601 - Sexual Assault Investigations.	363
602 - Asset Forfeiture.	365
603 - Informants.	372
604 - Eyewitness Identification.	379
605 - Brady Material Disclosure.	383
Chapter 7 - Equipment.	386
700 - Department-Owned and Personal Property.	387
701 - Personal Communication Devices.	389
702 - Vehicle Maintenance.	393
703 - Vehicle Use.	395
704 - Personal Protective Equipment.	402
Chapter 8 - Support Services.	407
800 - Evidence Room.	408
801 - Records Section.	417
802 - Records Maintenance and Release.	420
803 - Protected Information.	427
804 - CJIS Policy.	431
806 - [Animal Control].	439
807 - CJIS Access, Maintenance, and Security.	442
Chapter 9 - Custody.	447
900 - Temporary Custody of Adults.	448
901 - Custodial Searches.	458
902 - Prison Rape Elimination.	463
903 - Transporting Persons in Custody.	473
Chapter 10 - Personnel.	478
1000 - Anti-Retaliation.	479
1001 - Reporting of Employee Convictions and Court Orders.	482

South Saint Paul Police Department

S Saint Paul PD Policy Manual

1002 - Communicable Diseases.	484
1003 - Personnel Complaints.	488
1004 - Seat Belts.	498
1005 - Body Armor.	500
1006 - Personnel Records.	502
1007 - Commendations and Awards.	506
1008 - Fitness for Duty.	509
1009 - Lactation Breaks.	512
1010 - Call Back Procedure; Voluntary and Mandatory.	513
1011 - Outside Employment.	518
1012 - Occupational Disease, Personal Injury and Death Reporting.	522
1013 - Personal Appearance Standards.	525
1014 - Uniform Regulations.	527
1015 - Department Badges.	537
1016 - Temporary Modified-Duty Assignments.	539
1017 - Employee Speech, Expression and Social Networking.	542
1018 - POST Licensing.	546
1019 - Line-of-Duty Deaths.	547
1022 - Wellness Program.	559
Attachments.	567
MN POST Professional Conduct of Peace Officers Model Policy.pdf.	568
Model Sexual Assault Investigation Policy 02.16.21.pdf.	569
Confidential Informants Model Policy .pdf.	570
Model Sexual Assault Investigation Policy.pdf.	571
7 CJIS Security Policy_v5-7_20180816.pdf.	572
Model Sexual Assault Investigation Policy 03-03-21.pdf.	573
Eyewitness Identification Procedures Model Policy.pdf.	574
MN Public Assembly-First Amendment Rights Model Policy .pdf.	575

Chapter 1 - Law Enforcement Role and Authority

Law Enforcement Authority

100.1 PURPOSE AND SCOPE

The purpose of this policy is to affirm the authority of the members of the South Saint Paul Police Department to perform their functions based on established legal authority.

100.2 PEACE OFFICER POWERS

Licensed officers of this department are peace officers pursuant to Minn. Stat. § 626.84 Subd. 1.

100.2.1 ARREST AUTHORITY WITHIN THE JURISDICTION OF THE SOUTH SAINT PAUL POLICE DEPARTMENT

Arrest authority of a full-time officer or part-time officer extends to any place within the jurisdiction of the department when (Minn. Stat. § 629.34, Subd. 1 and Minn. Stat. § 629.40):

- (a) Made pursuant to a warrant.
- (b) The person is being arrested for a felony.
- (c) The person is being arrested for a non-felony crime that was attempted or committed in the officer's presence.
- (d) The person is being arrested for a non-felony crime that was not attempted or committed in the officer's presence but an arrest is permitted by statute (e.g., domestic abuse, restraining order, and no contact order violations).
- (e) The person is a juvenile committed to the custody of the commissioner of corrections and committed a felony after he/she escaped from custody (Minn. Stat. § 609.485).
- (f) There is reasonable cause to believe that the person to be arrested has committed or attempted to commit theft from a merchant (Minn. Stat. § 629.366).

The arrest authority of a part-time peace officer is applicable only while on-duty (Minn. Stat. § 629.34, Subd. 1(b)).

100.2.2 ARREST AUTHORITY OUTSIDE THE JURISDICTION OF THE SOUTH SAINT PAUL POLICE DEPARTMENT

Full- and part-time, on-duty officers may make an arrest outside the jurisdiction of the South Saint Paul Police Department (Minn. Stat. § 629.40):

- (a) Anytime the officer may by law make an arrest for a criminal offense committed within the jurisdiction of the South Saint Paul Police Department, and the person to be arrested escapes from custody or flees out of the officer's jurisdiction.
- (b) Whenever the officer is authorized by a court order.
- (c) Under the same conditions as if the officer was in the jurisdiction of the department, whenever the officer is acting in the course and scope of employment.

A full-time officer's warrantless arrest authority when off-duty and outside the jurisdiction of the department is limited to circumstances that would permit the officer to use deadly force under Minn. Stat. § 609.066 (see the Use of Force Policy) (Minn. Stat. § 629.40, Subd. 4). Under any

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Law Enforcement Authority

other circumstances, the full-time off-duty officer is limited to the same power as are members of the general public.

An officer making an arrest should, as soon as practicable after making the arrest, notify the agency having jurisdiction where the arrest was made.

100.2.3 GRANTING AUTHORITY TO OTHERS

An officer may summon the aid of private persons when making an arrest pursuant to a warrant (Minn. Stat. § 629.30).

100.3 INTERSTATE PEACE OFFICER POWERS

Peace officer powers may be extended within other states:

- (a) As applicable under interstate compacts and memorandums of understanding in compliance with the laws of each state.
- (b) When an officer enters Iowa or Wisconsin in fresh pursuit of a felony subject (Iowa Code § 806.1; Wis. Stat. § 976.04).
- (c) When an officer enters North Dakota or South Dakota in pursuit of a subject who committed any offense (N.D.C.C. § 29-06-05; SDCL 23A-3-9; SDCL 23A-3-10).

Whenever an officer makes an arrest in another state, the officer shall take the offender to a magistrate or judge in the county where the arrest occurred as soon as practicable (Iowa Code § 806.2; N.D.C.C. § 29-06-06; SDCL 23A-3-12; Wis. Stat. § 976.04).

100.4 POLICY

It is the policy of the South Saint Paul Police Department to limit its members to only exercise the authority granted to them by law.

While this department recognizes the power of peace officers to make arrests and take other enforcement action, officers are encouraged to use sound discretion in the enforcement of the law. This department does not tolerate abuse of law enforcement authority.

100.5 CONSTITUTIONAL REQUIREMENTS

All members shall observe and comply with every person's clearly established rights under the United States and Minnesota Constitutions.

Chief Executive Officer

101.1 PURPOSE AND SCOPE

The Minnesota Legislature acting through the Minnesota Board of Peace Officer Standards and Training (POST Board) has mandated that all peace officers employed within the State of Minnesota shall hold a POST Board license (Minn. Stat. § 626.846).

101.1.1 CHIEF LAW ENFORCEMENT OFFICER REQUIREMENTS

Any chief law enforcement officer of this department, as defined in Minn. R. 6700.0100, shall as a condition of employment hold a license as a peace officer with the POST Board (Minn. R. 6700.0800; Minn. R. 6700.0501), possess a bachelor's degree from an accredited college and have 10 years of employment with the South St Paul Police Department (SSP PD Civil Service Rule 7). The peace officer license shall be renewed every three years as required by Minn. R. 6700.1000.

Oath of Office

102.1 POLICY

It is the policy of the South Saint Paul Police Department that, when appropriate, department members affirm the oath of their office as an expression of commitment to the constitutional rights of those served by the Department and the dedication of its members to their duties (Minn. Stat. § 358.05).

102.2 PURPOSE AND SCOPE

Officers of this department are sworn to uphold the federal and state constitutions and to enforce federal, state and local laws.

102.3 OATH OF OFFICE

Upon employment, all employees shall be required to affirm, sign and date the oath of office expressing commitment and intent to respect constitutional rights in discharging the duties of the position, regardless of whether law mandates such an oath. The oath shall be as follows:

I, (employee name), do solemnly swear that I will support the Constitution of the United States and the Constitution of the State of Minnesota, and that I will faithfully discharge the duties of (applicable position or office) within and for the (name of political entity) and State.

102.4 MAINTENANCE OF RECORDS

Oaths mandated by law shall be filed as required by law (Minn. Stat. § 387.01; Minn. Stat. § 387.14). Other oaths shall be maintained consistent with other personnel employment records.

Policy Manual

103.1 PURPOSE AND SCOPE

The manual of the South Saint Paul Police Department is hereby established and shall be referred to as the Policy Manual or the manual. The manual is a statement of the current policies, rules and guidelines of this department. All members are to conform to the provisions of this manual.

All prior and existing manuals, orders and regulations that are in conflict with this manual are rescinded, except to the extent that portions of existing manuals, procedures, orders and other regulations that have not been included herein shall remain in effect, provided that they do not conflict with the provisions of this manual.

103.2 POLICY

Except where otherwise expressly stated, the provisions of this manual shall be considered as guidelines. It is recognized that the work of law enforcement is not always predictable and circumstances may arise which warrant departure from these guidelines. It is the intent of this manual to be viewed from an objective standard, taking into consideration the sound discretion entrusted to members of this department under the circumstances reasonably available at the time of any incident.

103.2.1 DISCLAIMER

The provisions contained in the Policy Manual are not intended to create an employment contract nor any employment rights or entitlements. The policies contained within this manual are for the internal use of the South Saint Paul Police Department and shall not be construed to create a higher standard or duty of care for civil or criminal liability against the City, its officials or members. Violations of any provision of any policy contained within this manual shall only form the basis for department administrative action, training or discipline. The South Saint Paul Police Department reserves the right to revise any policy content, in whole or in part.

103.3 AUTHORITY

The Chief of Police shall be considered the ultimate authority for the content and adoption of the provisions of this manual and shall ensure compliance with all applicable federal, state and local laws. The Chief of Police or the authorized designee is authorized to issue Departmental Directives, which shall modify those provisions of the manual to which they pertain. Departmental Directives shall remain in effect until such time as they may be permanently incorporated into the manual.

103.4 DEFINITIONS

The following words and terms shall have these assigned meanings throughout the Policy Manual, unless it is apparent from the content that they have a different meaning:

Adult - Any person 18 years of age or older.

CFR- Code of Federal Regulations.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Policy Manual

Child- Any person under the age of 18 years.

City - The City of South Saint Paul.

Civilian - Employees and volunteers who are not licensed peace officers.

Department/SSP PD - The South Saint Paul Police Department.

DPS- The Minnesota Department of Public Safety.

DVS- The Minnesota Department of Driver and Vehicle Services.

Employee/personnel - Any person employed by the Department.

Lead worker or unit leader- A person assigned to direct or control employees and operations and who assigns, directs and critiques job performance of designated staff during the course of a work assignment or daily task. A lead worker does not have the authority to reward, discipline or promote. A lead worker includes assignment to the role of "**officer-in-charge**" or "**OIC.**"

Manual - The South Saint Paul Police Department Policy Manual.

May - Indicates a permissive, discretionary or conditional action.

Member - Any person who is employed or appointed by the South Saint Paul Police Department including licensed officers, part-time officers, civilian employees and volunteers.

MSP- Minnesota State Patrol.

Officer - Those employees, regardless of rank, who are licensed peace officer employees of the South Saint Paul Police Department.

On-duty - A member's status during the period when he/she is actually engaged in the performance of his/her assigned duties.

Order - A written or verbal instruction issued by a superior.

Peace officer- An employee of the Department who is required to be certified by POST pursuant to Minn. Stat. § 626.84, Subd. 1 or otherwise holds a peace officer license. The term includes licensed full-time and part-time officers who perform the duties of a peace officer.

POST- The Minnesota Board of Peace Officer Standards and Training.

Rank - The title of the classification held by an officer.

Shall or will - Indicates a mandatory action.

Should - Indicates a generally required or expected action, absent a rational basis for failing to conform.

Supervisor - A person in a position of authority regarding hiring, transfer, suspension, promotion, discharge, assignment, reward or discipline of other department members, directing the work of other members or having the authority to adjust grievances. The supervisory exercise of authority may not be merely routine or clerical in nature but requires the use of independent judgment.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Policy Manual

The term "supervisor" may also include any person (e.g., officer-in-charge, lead or senior worker) given responsibility for the direction of the work of others without regard to a formal job title, rank or compensation.

When there is only one department member on-duty, that person may also be the supervisor, except when circumstances reasonably require the notification or involvement of the member's off-duty supervisor or an on-call supervisor.

USC- United States Code.

103.5 ISSUING THE POLICY MANUAL

An electronic version of the Policy Manual will be made available to all members on the department network for viewing and printing. No changes shall be made to the manual without authorization from the Chief of Police or the authorized designee.

Each member shall acknowledge that he/she has been provided access to, and has had the opportunity to review the Policy Manual and Departmental Directives. Members shall seek clarification as needed from an appropriate supervisor for any provisions that they do not fully understand.

103.6 PERIODIC REVIEW OF THE POLICY MANUAL

The Chief of Police will ensure that the Policy Manual is periodically reviewed and updated as necessary.

103.7 REVISIONS TO POLICIES

All revisions to the Policy Manual will be provided to each member on or before the date the policy becomes effective. Each member will be required to acknowledge that he/she has reviewed the revisions and shall seek clarification from an appropriate supervisor as needed.

Members are responsible for keeping abreast of all Policy Manual revisions.

The Chief will ensure that members are aware of any Policy Manual revision.

All department members suggesting revision of the contents of the Policy Manual shall forward their written suggestions to their Division Commanders, who will consider the recommendations and forward them to the Chief as appropriate.

Chapter 2 - Organization and Administration

Organizational Structure and Responsibility

200.1 PURPOSE AND SCOPE

The organizational structure of the Department is designed to create an efficient means to accomplish the mission and goals and to provide for the best possible service to the public.

200.2 DIVISIONS

The Chief of Police is responsible for administering and managing the South Saint Paul Police Department. There are two divisions in the Police Department as follows:

- Administration Division
- Patrol Division
- Investigation Division

200.2.1 ADMINISTRATION DIVISION

The Administration Division is commanded by a Commander, whose primary responsibility is to provide general management, direction and control for the Administration Division, including management of the department budget. The Administration Division consists of Technical Services and Administrative Services.

Annually, the Administration Division Commander shall develop and submit to the Chief of Police a budget and an inventory of capital property, equipment and assets. Property, equipment and assets with a beginning value of more than \$5,000 and other items specifically identified for inclusion regardless of value, are capital property, equipment and assets.

200.2.2 PATROL DIVISION

The Patrol Division is commanded by a Commander, whose primary responsibility is to provide general management, direction and control for the Patrol Division. The Patrol Division consists of Uniformed Patrol and Special Operations, which includes Traffic, Dispatch and Police Aides/ Assistants.

200.2.3 INVESTIGATION DIVISION

The Investigation Division is commanded by a Commander whose primary responsibility is to provide general management, direction and control for the Investigation Division. The Investigation Division consists of the Investigations, Crime Analysis Unit, Property Bureau and Forensic Services.

200.3 COMMAND PROTOCOL

200.3.1 SUCCESSION OF COMMAND

The Chief of Police exercises command over all personnel in the Department. During planned absences the chief deputy or assistant chief shall act with the authority of the Chief of Police.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Organizational Structure and Responsibility

Except when designated as above, the order of command authority in the absence or unavailability of the Chief of Police is as follows:

- (a) Senior Commander
- (b) Commander
- (c) Senior Sergeant

200.3.2 UNITY OF COMMAND

The principles of unity of command ensure efficient supervision and control within the Department. Generally, each employee shall be accountable to one supervisor at any time for a given assignment or responsibility. Except where specifically delegated authority may exist by policy or special assignment (e.g., Canine, SWAT), any supervisor may temporarily direct any subordinate if an operational necessity exists.

200.3.3 ORDERS

Members shall respond to and make a good faith and reasonable effort to comply with the lawful order of superior officers and other proper authority.

200.3.4 UNLAWFUL AND CONFLICTING ORDERS

No member is required to obey any order that outwardly appears to be in direct conflict with any federal law, state law or local ordinance. If the legality of an order is in doubt, the affected member shall ask the issuing supervisor to clarify the order or confer with a higher authority. Responsibility for refusal to obey rests with the member, who shall subsequently be required to justify the refusal.

Unless it would jeopardize the safety of any individual, members who are presented with an order that is in conflict with a previous order, department policy or other directive, shall respectfully inform the issuing supervisor of the conflict. The issuing supervisor is responsible for either resolving the conflict or clarifying that the order is intended to countermand the previous order or directive, in which case the member is obliged to comply. Members who are compelled to follow a conflicting order after having given the issuing supervisor the opportunity to correct the conflict are not held accountable for disobedience of the order or directive that was initially issued.

The person countermanding the original order shall notify, in writing, the person issuing the original order, indicating the action taken and the reason therefore.

Departmental Directive and Special Orders

201.1 PURPOSE AND SCOPE

Departmental Directives and Special Orders establish an interdepartmental communication that may be used by the Chief of Police to make immediate changes to policy and procedure consistent with the current Memorandum of Understanding or other collective bargaining agreement. Departmental Directives will immediately modify or change and supersede sections of this manual to which they pertain.

201.1.1 DEPARTMENTAL DIRECTIVES PROTOCOL

Departmental Directives will be incorporated into the manual as required upon approval of staff. Departmental Directives will modify existing policies or create a new policy as appropriate and will be rescinded upon incorporation into the manual.

All existing Departmental Directives have now been incorporated in the updated Policy Manual as of the below revision date.

Any Departmental Directives issued after publication of the manual shall be numbered consecutively starting with the last two digits of the year, followed by the number "01." For example, 10-01 signifies the first Departmental Directive for the year 2010.

201.1.2 SPECIAL ORDERS PROTOCOL

Special Orders establish a temporary policy or procedure on a given subject for a specific length of time. Special Orders are issued to the organization as a whole, to a division, to a unit or to an individual thereof and are temporary in nature. Special Orders become inoperative with the passing of the incident or situation that caused the order's issuance.

201.2 RESPONSIBILITIES

201.2.1 STAFF

The staff shall review and approve revisions of the Policy Manual, which will incorporate changes originally made by Departmental Directive.

201.2.2 CHIEF OF POLICE

The Chief of Police or designee shall issue all Departmental Directives and Special Orders.

201.3 ACCEPTANCE OF DEPARTMENTAL DIRECTIVES AND SPECIAL ORDERS

All employees are required to read and obtain any necessary clarification of all Departmental Directives or special orders. All employees are required to acknowledge in writing the receipt and review of any new Departmental Directive or special order.

Signed acknowledgement forms and/or e-mail receipts showing an employee's acknowledgement will be maintained by the Support Services Commander.

Emergency Operations Plan

202.1 PURPOSE AND SCOPE

The City has prepared, in compliance with the Minnesota Emergency Management Act of 1996 (Minn. Stat. § 12.09), an Emergency Operations Plan Manual. This manual is for the guidance and use by all employees in the event of a major disaster, civil disturbance, mass arrest or other emergency event. The manual provides for a strategic response by all employees and assigns specific responsibilities in the event the plan is activated.

202.2 ACTIVATING THE EMERGENCY OPERATIONS PLAN

The Emergency Operations Plan can be activated in a number of ways. For the Police Department, the Chief of Police, the highest ranking official on-duty or an on-scene responder may activate the Emergency Operations Plan in response to a major emergency.

202.2.1 RECALL OF PERSONNEL

In the event that the Emergency Operations Plan is activated, all employees of the South Saint Paul Police Department are subject to immediate recall. Employees may also be subject to recall during extraordinary circumstances as deemed necessary by the Chief of Police or the authorized designee.

Failure to promptly respond to an order to report for duty may result in discipline.

202.3 LOCATION OF MANUALS

The electronic manual is available on the Police Network titled "South St. Paul EOP." A hard copy of the manual is located in Chief's office and the patrol office area.

202.4 PLAN REVIEW

The Administration Division Commander shall annually review the Emergency Operation Plan and recommend updates when applicable. The annual review, update, and approval of the plan and supporting documents must be in accord with the guidance provided by the Department of Public Safety, Division of Emergency Management and should incorporate a full or partial exercise, tabletop or command staff discussion (Minn. Stat. § 299J.10).

202.5 PLAN TRAINING

The Department shall provide training in the Emergency Operations Plan for all supervisors and other appropriate personnel. All supervisors should familiarize themselves with the Emergency Operations Plan and the roles police personnel will play when the plan is implemented.

Electronic Mail

203.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper use and application of the electronic mail (email) system provided by the Department. Email is a communication tool available to employees to enhance efficiency in the performance of job duties. It is to be used in accordance with generally accepted business practices and current law (e.g., Minnesota Data Practices Act). Messages transmitted over the email system must only be those that involve official business activities or contain information essential to employees for the accomplishment of business-related tasks and/or communication directly related to the business, administration or practices of the Department.

203.2 EMAIL RIGHT OF PRIVACY

All email messages, including attachments, transmitted over the Department computer network or accessed through a web browser accessing the Department system are considered Department records and, therefore, are the property of the Department. The Department has the right to access, audit and disclose for whatever reason, all messages, including attachments, transmitted or received through its email system or placed into its storage.

Unless it is encrypted, the email system is not a confidential system since all communications transmitted on, to or from the system are the property of the Department. Therefore, the email system is not appropriate for confidential or personal communication. If a communication must be private, an alternative method to communicate the message should be used instead of email. Employees using the Department email system shall have no expectation of privacy concerning communications utilizing the system.

203.3 PROHIBITED USE OF E-MAIL

Personal use of the Department e-mail system should be kept to a minimum.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive and harassing or any other inappropriate messages on the email system is prohibited, will constitute just cause for discipline, and will result in discipline, up to and including termination of employment

It is a violation of this policy to transmit a message under another user's name or e-mail address or to use the password of another to log onto the system. Users should make an effort log off the network or lock the workstation when their computer is unattended. This added security measure would minimize the misuse of an individual's email, name and/or password.

Supervision Staffing Levels

204.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that proper supervision is available for all shifts. The Department intends to balance the employee's needs against its need and inherent managerial right to have flexibility and discretion in using personnel to meet operational needs. While balance is desirable, the paramount concern is the need to meet operational requirements of the Department.

204.2 MINIMUM STAFFING LEVELS

Minimum staffing levels should result in the scheduling of at least one Sergeant on-duty whenever possible. Sergeants will ensure efficient operations of that particular shift.

204.2.1 SUPERVISION DEPLOYMENTS

In order to accommodate training, vacations, illness/injury and other unforeseen circumstances, an officer may be designated as "Officer in Charge (OIC)" when a Sergeant is not available. The OIC will, typically, be the most senior officer working at the time with the exception of those officers who have made it officially known they are unwilling to serve in that capacity or those officers who have been designated by the Chief as prohibited to serve as OIC. If the Chief or a Division Commander is on duty, an OIC will not be designated.

Retiree Concealed Firearms

205.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the issuance, denial, suspension or revocation of South Saint Paul Police Department identification cards under the Law Enforcement Officers' Safety Act (LEOSA) (18 USC § 926C).

205.2 FIREARM PERMIT

A retired employee of this department may only carry a firearm if granted a permit to do so as specified in Minn. Stat. § 624.714 and associated statutes.

205.3 LEOSA

The Chief of Police may issue an identification card for LEOSA purposes to any former officer of this department who (18 USC § 926C(c)):

- (a) Separated from service in good standing from this department as an officer.
- (b) Before such separation, had regular employment as an officer for an aggregate of 10 years or more or, separated from service with the agency after completing any applicable probationary period due to a service-connected disability, as determined by this department.
- (c) Has not been disqualified for reasons related to physical or mental health.
- (d) Has not entered into an agreement with this department where the officer acknowledges that he/she is not qualified to receive a firearm qualification certificate for reasons related to mental health.
- (e) Is not prohibited by federal law from receiving or possessing a firearm.

205.3.1 LEOSA IDENTIFICATION CARD FORMAT

The LEOSA identification card should contain a photograph of the former officer and identify him/her as having been employed as an officer.

If the South Saint Paul Police Department qualifies the former officer, the LEOSA identification card or separate certification should indicate the date the former officer was tested or otherwise found by the Department to meet the active duty standards for qualification to carry a firearm.

205.3.2 AUTHORIZATION

Any qualified former law enforcement officer, including a former officer of this department, may carry a concealed firearm under 18 USC § 926C when he/she is:

- (a) In possession of photographic identification that identifies him/her as having been employed as a law enforcement officer, and one of the following:
 - 1. An indication from the person's former law enforcement agency that he/she has, within the past year, been tested or otherwise found by the law enforcement agency to meet agency-established active duty standards for qualification in firearms training to carry a firearm of the same type as the concealed firearm.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Retiree Concealed Firearms

2. A certification, issued by either the state in which the person resides or by a certified firearms instructor who is qualified to conduct a firearms qualification test for active duty law enforcement officers within that state, indicating that the person has, within the past year, been tested or otherwise found to meet the standards established by the state or, if not applicable, the standards of any agency in that state.
- (b) Not under the influence of alcohol or another intoxicating or hallucinatory drug or substance.
- (c) Not prohibited by federal law from receiving a firearm.
- (d) Not in a location prohibited by state law or by a private person or entity on his/her property if such prohibition is permitted by Minnesota law.

205.4 FORMER OFFICER RESPONSIBILITIES

A former officer with a card issued under this policy shall immediately notify the Sergeant of his/her arrest or conviction in any jurisdiction, or that he/she is the subject of a court order, in accordance with the Reporting of Employee Convictions and Court Orders Policy.

205.4.1 RESPONSIBILITIES UNDER LEOSA

In order to obtain or retain a LEOSA identification card, the former officer shall:

- (a) Sign a waiver of liability of the Department for all acts taken related to carrying a concealed firearm, acknowledging both his/her personal responsibility as a private person for all acts taken when carrying a concealed firearm as permitted by LEOSA and also that these acts were not taken as an employee or former employee of the Department.
- (b) Remain subject to all applicable department policies and federal, state and local laws.
- (c) Demonstrate good judgment and character commensurate with carrying a loaded and concealed firearm.
- (d) Successfully pass an annual criminal history background check indicating that he/she is not prohibited by law from receiving or possessing a firearm.

205.5 DENIAL, SUSPENSION OR REVOCATION

A LEOSA identification card may be denied or revoked upon a showing of good cause as determined by the Department. In the event that an identification card is denied, suspended or revoked, the former officer may request a review by the Chief of Police. The decision of the Chief of Police is final.

205.6 FIREARM QUALIFICATIONS

The Operations Commander may provide former officers from this department an opportunity to qualify. Written evidence of the qualification and the weapons used will be provided and will contain the date of the qualification. The Operations Commander will maintain a record of the qualifications and weapons used.

Handgun Purchase and Transfer Permit

206.1 PURPOSE AND SCOPE

The Chief of Police is given the statutory authority to issue a permit to purchase or transfer a pistol to persons within the community. This policy provides a written process for the application and issuance of such permits.

206.2 APPLICATION PROCESS

To apply for a permit to purchase or transfer a pistol, the applicant must complete and submit a signed and dated Minnesota Uniform Firearm Application/Receipt to the Department (Minn. Stat. § 624.7131, Subd. 1). These forms shall be freely available to members of the community at locations determined by the Chief of Police. Applications are also available on the internet (Minn. Stat. § 624.7131, Subd. 3).

Incomplete applications are not suitable for processing and may not be accepted.

The Department shall provide the applicant a dated receipt upon the presentation of the application (Minn. Stat. § 624.7131, Subd. 1).

206.3 INVESTIGATION

The Department shall conduct an investigation of the applicant to determine if he/she is eligible for a permit (Minn. Stat. § 624.7131, Subd. 2). The investigation shall include no less than:

- (a) A check of criminal histories, records, and warrants regarding the applicant through Minnesota crime information systems, the national criminal record repository, and the National Instant Criminal Background Check System.
- (b) A reasonable effort to check other available state and local record-keeping systems.
- (c) A check for any commitment history through the Minnesota Department of Human Services of the applicant.

206.4 GROUNDS FOR DISQUALIFICATION

The Chief of Police shall deny a permit to an applicant when the applicant is prohibited by state or federal law from possessing a pistol or semiautomatic military-style assault weapon, determined to be a danger to themselves or the public when in possession of a firearm, or listed in the criminal gang investigative data system (Minn. Stat. § 624.7131, Subd. 4).

206.5 GRANTING OR DENIAL OF PERMIT

The Chief of Police shall issue a transferee permit or deny the application within 30 days of application for the permit. The permits and their renewal shall be granted free of charge (Minn. Stat. § 624.7131, Subd. 5).

The Chief of Police shall provide an applicant with written notification of a denial and the specific reason for the denial (Minn. Stat. § 624.7131, Subd. 5).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Handgun Purchase and Transfer Permit

When the refusal to grant a permit is due to a substantial likelihood that the applicant is a danger to themselves or the public when in possession of a firearm, the written notification shall provide the specific factual basis justifying the denial, including the source, and inform the applicant that they may submit additional documentation within 20 business days (Minn. Stat. § 624.7131, Subd. 4).

Upon receipt of additional documentation, the Chief of Police shall reconsider the denial and inform the applicant within 15 business days of the result of the reconsideration. A notice of denial after reconsideration must be in the same form and substance as the original denial, specifically address any continued deficiencies, and inform the applicant of the right to judicial review of the denial (Minn. Stat. § 624.7131, Subd. 4).

A permit holder whose permit was denied may seek a judicial review by filing a petition in the district court for the county in which the application was submitted (Minn. Stat. § 624.7131, Subd. 8).

206.6 VOIDING OR REVOKING PERMIT

The permit becomes void at the time that the holder becomes prohibited from possessing or receiving a pistol under Minn. Stat. § 624.713, in which event the holder is required to return the permit within five days to the Department.

The Chief of Police shall revoke a permit once they become aware the permit holder is ineligible to possess firearms and shall provide the holder with written notice (Minn. Stat. § 624.7131, Subd. 7).

Training

207.1 PURPOSE AND SCOPE

This policy establishes general guidelines for how training is to be identified, conducted, and documented. This policy is not meant to address all specific training endeavors or identify every required training topic.

207.2 PHILOSOPHY

The Department seeks to provide ongoing training and encourages all personnel to participate in advanced training and formal education on a continual basis. Training is provided within the confines of funding, requirements of a given assignment, staffing levels and legal mandates. Whenever reasonably possible, the Department will use courses certified by the Minnesota Board of Peace Officer Standards and Training (POST) or other regulatory or nationally recognized entities. Examples of these entities may be, but are not limited to, the American Correctional Association and the American Jail Association.

207.3 OBJECTIVES

The objectives of the training program are to:

- (a) Enhance the level of law enforcement service to the public.
- (b) Increase the technical expertise and overall effectiveness of department members.
- (c) Provide for continued professional development of department members.
- (d) Ensure compliance with POST rules and regulations concerning law enforcement training.

207.4 DAILY TRAINING BULLETINS

The Lexipol Daily Training Bulletins (DTBs) are contained in a web-accessed system that provides training on the South Saint Paul Police Department Policy Manual and other important topics. Generally, one training bulletin is available for each day of the month. However, the number of DTBs may be adjusted by the Support Services Commander.

Members assigned to participate in DTBs shall only use login credentials assigned to them by the Support Services Commander. Members should not share their password with others and should frequently change their password to protect the security of the system. After each session, members should logoff the system to prevent unauthorized access. The content of the DTBs is copyrighted material and shall not be shared with others outside of the Department.

Members who are assigned to participate in the DTB program should complete each DTB at the beginning of their shift, or as otherwise directed by their supervisor. Members should not allow uncompleted DTBs to build up over time, and may be required to complete DTBs missed during extended absences (e.g., vacation, medical leave) upon returning to duty. Although the DTB system can be accessed from any internet-enabled computer, members shall only take DTBs as part of their on-duty assignments, unless directed otherwise by a supervisor.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Training

Supervisors will be responsible for monitoring the progress of those under their command to ensure compliance with this policy.

207.5 CLASSROOM DISCRIMINATION

The Support Services Commander shall ensure that procedures for the investigation and resolution of allegations of classroom discrimination are developed and implemented, and include the required elements (Minn. R. 6700.0900; Minn. R. 6700.0902).

207.6 POLICY

The Department shall administer a training program that will meet the standards of federal, state, local, and POST training requirements. It is a priority of this department to provide continuing education and training for the professional growth and development of its members.

207.7 SUPPORT SERVICES COMMANDER

The Chief of Police shall designate a Support Services Commander who is responsible for developing, reviewing, updating, and maintaining the department training plan so that required training is completed. The Support Services Commander should review the training plan annually.

207.7.1 SUPPORT SERVICES COMMANDER RESPONSIBILITIES

The Support Services Commander shall ensure that all sworn members annually review the department policies identified in Minn. R. 6700.1615 (Minn. R. 6700.1615, Subd. 2).

207.8 TRAINING ATTENDANCE

- (a) All members assigned to attend training shall attend as scheduled unless previously excused by their immediate supervisor. Excused absences should be limited to:
 - 1. Court appearances.
 - 2. Previously approved vacation or time off.
 - 3. Illness or medical leave.
 - 4. Physical limitations preventing the member's participation.
 - 5. Emergency situations or department necessity.
- (b) Any member who is unable to attend training as scheduled shall notify the member's supervisor as soon as practicable but no later than one hour prior to the start of training and shall:
 - 1. Document the member's absence in a memorandum to the member's supervisor.
 - 2. Make arrangements through the member's supervisor or the Support Services Commander to attend the required training on an alternate date.

207.9 REPORTING TRAINING TO POST

The POST Board distributes license renewals directly to licensed peace officers and requires the licensee to report completed continuing education courses from the previous license period.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Training

Officers are responsible for responding to these requests in a timely manner and otherwise maintaining their licensed status.

207.10 TRAINING RECORDS

The Support Services Commander is responsible for the creation, filing, and storage of all training records. Training records shall be retained in accordance with the established records retention schedule.

Chapter 3 - General Operations

Use of Force

300.1 PURPOSE AND SCOPE

This policy provides guidelines on the reasonable use of force. While there is no way to specify the exact amount or type of reasonable force to be applied in any situation, every member of this department is expected to use these guidelines to make such decisions in a professional, impartial, and reasonable manner (Minn. Stat. § 626.8452).

In addition to those methods, techniques, and tools set forth below, the guidelines for the reasonable application of force contained in this policy shall apply to all policies addressing the potential use of force, including but not limited to the Control Devices and Conducted Energy Device policies.

300.1.1 DEFINITIONS

Definitions related to this policy include:

Bodily harm - Physical pain or injury.

Deadly force - Force reasonably anticipated and intended to create a substantial likelihood of causing death or great bodily harm.

Feasible - Reasonably capable of being done or carried out under the circumstances to successfully achieve the arrest or lawful objective without increasing risk to the officer or another person.

Force - The application of physical techniques or tactics, chemical agents, or weapons to another person. It is not a use of force when a person allows him/herself to be searched, escorted, handcuffed, or restrained.

Great bodily harm - Bodily injury which creates a high probability of death, or which causes serious, permanent disfigurement, or which causes a permanent or protracted loss or impairment of the function of any bodily member or organ or other serious bodily harm.

Imminent - Ready to take place; impending. Note that imminent does not mean immediate or instantaneous.

Totality of the circumstances - All facts and circumstances known to the officer at the time, taken as a whole, including the conduct of the officer and the subject leading up to the use of force.

300.2 POLICY

The use of force by law enforcement personnel is a matter of critical concern, both to the public and to the law enforcement community. Officers are involved on a daily basis in numerous and varied interactions and, when warranted, may use reasonable force in carrying out their duties.

Officers must have an understanding of, and true appreciation for, their authority and limitations. This is especially true with respect to overcoming resistance while engaged in the performance of law enforcement duties.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Use of Force

The South Saint Paul Police Department recognizes and respects the value of all human life and dignity without prejudice to anyone. Vesting officers with the authority to use reasonable force and to protect the public welfare requires monitoring, evaluation, and a careful balancing of all interests.

300.2.1 DUTY TO INTERCEDE AND REPORT

Any officer present and observing another law enforcement officer or a member using force that is clearly beyond that which is objectively reasonable under the circumstances shall, when in a position to do so, intercede to prevent the use of unreasonable force (Minn. Stat. § 626.8452; Minn. Stat. § 626.8475).

Any officer who observes another law enforcement officer or a member use force that is potentially beyond that which is objectively reasonable under the circumstances shall report these observations to a supervisor as soon as feasible (Minn. Stat. § 626.8452; Minn. Stat. § 626.8475).

300.2.2 ADDITIONAL REQUIREMENTS

An officer reporting a use of force by another law enforcement officer or member pursuant to this policy shall also make the report in writing to the Chief of Police within 24 hours (Minn. Stat. § 626.8475).

300.2.3 PERSPECTIVE

When observing or reporting force used by a law enforcement officer, each officer should take into account the totality of the circumstances and the possibility that other law enforcement officers may have additional information regarding the threat posed by the subject.

300.3 USE OF FORCE

Officers shall use only that amount of force that reasonably appears necessary given the facts and circumstances perceived by the officer at the time of the event to accomplish a legitimate law enforcement purpose.

The reasonableness of force will be judged from the perspective of a reasonable officer on the scene at the time of the incident. Any evaluation of reasonableness must allow for the fact that officers are often forced to make split-second decisions about the amount of force that reasonably appears necessary in a particular situation, with limited information and in circumstances that are tense, uncertain, and rapidly evolving.

Given that no policy can realistically predict every possible situation an officer might encounter, officers are entrusted to use well-reasoned discretion in determining the appropriate use of force in each incident.

It is also recognized that circumstances may arise in which officers reasonably believe that it would be impractical or ineffective to use any of the tools, weapons, or methods provided by this department. Officers may find it more effective or reasonable to improvise their response to rapidly unfolding conditions that they are confronting. In such circumstances, the use of any improvised

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Use of Force

device or method must nonetheless be reasonable and utilized only to the degree that reasonably appears necessary to accomplish a legitimate law enforcement purpose.

While the ultimate objective of every law enforcement encounter is to avoid or minimize injury, nothing in this policy requires an officer to retreat or be exposed to possible physical injury before applying reasonable force.

300.3.1 USE OF FORCE TO EFFECT AN ARREST

An officer may use reasonable force (Minn. Stat. § 609.06 and Minn. Stat. § 629.33):

- (a) In effecting a lawful arrest.
- (b) In the execution of a legal process.
- (c) In enforcing an order of the court.
- (d) In executing any other duty imposed by law.
- (e) In preventing the escape, or to retake following the escape, of a person lawfully held on a charge or conviction of a crime.
- (f) In restraining a person with a mental illness or a person with a developmental disability from self-injury or injury to another.
- (g) In self-defense or defense of another.

An officer who makes or attempts to make an arrest need not retreat or desist from his/her efforts by reason of resistance or threatened resistance of the person being arrested; nor shall such officer be deemed the aggressor or lose his/her right to self-defense by the use of reasonable force to effect the arrest or to prevent escape or to overcome resistance.

300.3.2 FACTORS USED TO DETERMINE THE REASONABLENESS OF FORCE

When determining whether to apply force and evaluating whether an officer has used reasonable force, a number of factors should be taken into consideration, as time and circumstances permit. These factors include but are not limited to:

- (a) Immediacy and severity of the threat to officers or others.
- (b) The conduct of the individual being confronted, as reasonably perceived by the officer at the time.
- (c) Officer/subject factors (e.g., age, size, relative strength, skill level, injuries sustained, level of exhaustion or fatigue, the number of officers available vs. subjects).
- (d) The effects of suspected drug or alcohol use.
- (e) The individual's mental state or capacity.
- (f) The individual's ability to understand and comply with officer commands.
- (g) Proximity of weapons or dangerous improvised devices.
- (h) The degree to which the individual has been effectively restrained and his/her ability to resist despite being restrained.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Use of Force

- (i) The availability of other reasonable and feasible options and their possible effectiveness (Minn. Stat. § 626.8452).
- (j) Seriousness of the suspected offense or reason for contact with the individual.
- (k) Training and experience of the officer.
- (l) Potential for injury to officers, suspects, and others.
- (m) Whether the individual appears to be resisting, attempting to evade arrest by flight, or is attacking the officer.
- (n) The risk and reasonably foreseeable consequences of escape.
- (o) The apparent need for immediate control of the individual or a prompt resolution of the situation.
- (p) Whether the conduct of the individual being confronted no longer reasonably appears to pose an imminent threat to the officer or others.
- (q) Prior contacts with the individual or awareness of any propensity for violence.
- (r) Any other exigent circumstances.

300.3.3 PAIN COMPLIANCE TECHNIQUES

Pain compliance techniques may be effective in controlling a physically or actively resisting individual. Officers may only apply those pain compliance techniques for which they have successfully completed department-approved training. Officers utilizing any pain compliance technique should consider:

- (a) The degree to which the application of the technique may be controlled given the level of resistance.
- (b) Whether the individual can comply with the direction or orders of the officer.
- (c) Whether the individual has been given sufficient opportunity to comply.

The application of any pain compliance technique shall be discontinued once the officer determines that compliance has been achieved.

300.3.4 ALTERNATIVE TACTICS - DE-ESCALATION

When circumstances reasonably permit, officers should use non-violent strategies and techniques to decrease the intensity of a situation, improve decision-making, improve communication, reduce the need for force, and increase voluntary compliance.

300.3.5 STATE RESTRICTIONS ON THE USE OF OTHER RESTRAINTS

Officers may not use any of the following restraints unless the use of deadly force is authorized (Minn. Stat. § 609.06; Minn. Stat. § 609.066):

- (a) A chokehold. For purposes of this policy, a chokehold only refers to the method of applying sufficient pressure to an individual to make breathing difficult or impossible, and includes but is not limited to any pressure to the neck, throat, or windpipe that may prevent or hinder breathing, or reduce intake of air.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Use of Force

1. If applied, a chokehold is subject to the same guidelines and requirements as a carotid control hold.
- (b) Tying all of an individual's limbs together behind the person's back to render the person immobile.
- (c) Securing an individual in any way that results in transporting the person face down in a vehicle.

300.4 DEADLY FORCE APPLICATIONS

When reasonable, the officer shall, prior to the use of deadly force, make efforts to identify themselves as a peace officer and to warn that deadly force may be used, unless the officer has objectively reasonable grounds to believe the person is aware of those facts.

Use of deadly force is justified only if an objectively reasonable officer would believe, based on the totality of the circumstances known to the officer at the time and without the benefit of hindsight, that such force is necessary (Minn. Stat. § 609.066):

- (a) To protect the officer or another from death or great bodily harm.
- (b) To effect the arrest or capture, or prevent the escape, of an individual whom the officer knows or has reasonable grounds to believe has committed or attempted to commit a felony and the officer reasonably believes that the person will cause death or great bodily harm to another person unless immediately apprehended.

In both scenarios, the use of deadly force is only authorized provided that the threat (Minn. Stat. § 609.066):

- Can be articulated with specificity.
- Is reasonably likely to occur absent action by the officer.
- Must be addressed through the use of deadly force without unreasonable delay.

However, an officer shall not use deadly force against a person whose actions are a threat solely to themselves or property unless the person poses an imminent danger of death or serious physical injury to the officer or others in close proximity (Minn. Stat. § 609.066).

300.4.1 MOVING VEHICLES

Shots fired at or from a moving vehicle are rarely effective and involve considerations and risks in addition to the justification for the use of deadly force.

When feasible, officers should take reasonable steps to move out of the path of an approaching vehicle instead of discharging their firearm at the vehicle or any of its occupants.

An officer should only discharge a firearm at a moving vehicle or its occupants when the officer reasonably believes there are no other reasonable means available to avert the imminent threat of the vehicle, or if deadly force other than the vehicle is directed at the officer or others.

Officers should not shoot at any part of a vehicle in an attempt to disable the vehicle.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Use of Force

300.5 REPORTING THE USE OF FORCE

Any use of force by a member of this department shall be documented promptly, completely, and accurately in an appropriate report, depending on the nature of the incident. The officer should articulate the factors perceived and why he/she believed the use of force was reasonable under the circumstances.

To collect data for purposes of training, resource allocation, analysis, and related purposes, the Department may require the completion of additional report forms, as specified in department policy, procedure, or law. See the Report Preparation Policy for additional circumstances that may require documentation.

300.5.1 NOTIFICATIONS TO SUPERVISORS

Supervisory notification shall be made as soon as practicable following the application of force in any of the following circumstances:

- (a) The application caused a visible injury.
- (b) The application would lead a reasonable officer to conclude that the individual may have experienced more than momentary discomfort.
- (c) The individual subjected to the force complained of injury or continuing pain.
- (d) The individual indicates intent to pursue litigation.
- (e) Any application of the conducted energy device or control device.
- (f) Any application of a restraint device other than handcuffs, shackles, or belly chains.
- (g) The individual subjected to the force was rendered unconscious.
- (h) An individual was struck or kicked.
- (i) An individual alleges unreasonable force was used or that any of the above has occurred.

300.5.2 STATE REPORTING REQUIREMENTS

The Chief of Police shall provide for the filing of a report with the Bureau of Criminal Apprehension (BCA) on a monthly basis and in the form required by BCA (Minn. Stat. § 626.5534).

There may be additional reporting requirements regarding misconduct (see the Standards of Conduct Policy) (Minn. Stat. § 626.8457).

300.6 MEDICAL CONSIDERATIONS

Once it is reasonably safe to do so, medical assistance shall be obtained for any person who exhibits signs of physical distress, has sustained visible injury, expresses a complaint of injury or continuing pain, or was rendered unconscious. Any individual exhibiting signs of physical distress after an encounter should be continuously monitored until the individual can be medically assessed. Individuals should not be placed on their stomachs for an extended period, as this could impair their ability to breathe.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Use of Force

Based upon the officer's initial assessment of the nature and extent of the individual's injuries, medical assistance may consist of examination by an emergency medical services provider or medical personnel at a hospital or jail. If any such individual refuses medical attention, such a refusal shall be fully documented in related reports and, whenever practicable, should be witnessed by another officer and/or medical personnel. If a recording is made of the contact or an interview with the individual, any refusal should be included in the recording, if possible.

The on-scene supervisor or, if the on-scene supervisor is not available, the primary handling officer shall ensure that any person providing medical care or receiving custody of a person following any use of force is informed that the person was subjected to force. This notification shall include a description of the force used and any other circumstances the officer reasonably believes would be potential safety or medical risks to the subject.

Individuals who exhibit extreme agitation, violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics, and imperviousness to pain, or who require a protracted physical encounter with multiple officers to be brought under control, may be at an increased risk of sudden death. Calls involving these persons should be considered medical emergencies. Officers who reasonably suspect a medical emergency should request medical assistance as soon as practicable and have medical personnel stage away.

See the Medical Aid and Response Policy for additional guidelines.

300.7 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to a reported application of force resulting in visible injury, if reasonably available. When a supervisor is able to respond to an incident in which there has been a reported application of force, the supervisor is expected to:

- (a) Obtain the basic facts from the involved officers. Absent an allegation of misconduct or excessive force, this will be considered a routine contact in the normal course of duties.
- (b) Ensure that any injured parties are examined and treated.
- (c) When possible, separately obtain a recorded interview with the individual upon whom force was applied. If this interview is conducted without the individual having voluntarily waived his/her *Miranda* rights, the following shall apply:
 - 1. The content of the interview should not be summarized or included in any related criminal charges.
 - 2. The fact that a recorded interview was conducted should be documented in a property or other report.
 - 3. The recording of the interview should be distinctly marked for retention until all potential for civil litigation has expired.
- (d) Once any initial medical assessment has been completed or first aid has been rendered, ensure that photographs have been taken of any areas involving visible injury or complaint of pain, as well as overall photographs of uninjured areas.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Use of Force

1. These photographs should be retained until all potential for civil litigation has expired.
- (e) Identify any witnesses not already included in related reports.
- (f) Review and approve all related reports.
- (g) Determine if there is any indication that the individual may pursue civil litigation.
 1. If there is an indication of potential civil litigation, the supervisor should complete and route a notification of a potential claim through the appropriate channels.
- (h) Evaluate the circumstances surrounding the incident and initiate an administrative investigation if there is a question of policy noncompliance or if for any reason further investigation may be appropriate.

In the event that a supervisor is unable to respond to the scene of an incident involving the reported application of force, the supervisor is still expected to complete as many of the above items as circumstances permit.

300.8 TRAINING

Officers shall receive training on this policy, including the learning objectives as provided by the Board of Peace Officer Standards and Training (POST), and demonstrate their knowledge and understanding at least annually (Minn. Stat. § 626.8452, Subd. 3).

Subject to available resources, officers should receive periodic training on guidelines regarding vulnerable populations, including but not limited to children, elderly, pregnant persons, and individuals with physical, mental, or intellectual disabilities.

300.8.1 STATE-SPECIFIC TRAINING REQUIREMENTS

Warrior-style training, as defined in Minn. Stat. § 626.8434, whether provided directly by the Department or through a third party, is prohibited (Minn. Stat. § 626.8434).

300.9 POLICY REVIEW

The Chief of Police or the authorized designee should annually review and update this policy to reflect developing practices and procedures.

Handcuffing and Restraints

301.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of handcuffs and other restraints during detentions and arrests.

301.2 POLICY

The South Saint Paul Police Department authorizes the use of restraint devices in accordance with this policy, the Use of Force Policy, the Transporting Persons in Custody Policy, and department training. Restraint devices shall not be used to punish, to display authority, or as a show of force.

301.3 USE OF RESTRAINTS

Only members who have successfully completed South Saint Paul Police Department-approved training on the use of restraint devices described in this policy are authorized to use these devices.

When deciding whether to use any restraint, officers should carefully balance officer safety concerns with factors that include, but are not limited to:

- The circumstances or crime leading to the arrest.
- The demeanor and behavior of the arrested person.
- The age and health of the person.
- Whether the person is known to be pregnant.
- Whether the person has a hearing or speaking disability. In such cases, consideration should be given, safety permitting, to handcuffing to the front in order to allow the person to sign or write notes.
- Whether the person has any other apparent disability.

301.3.1 RESTRAINT OF DETAINEES

Situations may arise where it may be reasonable to restrain an individual who may, after brief investigation, be released without arrest. Unless arrested, the use of restraints on detainees should continue only for as long as is reasonably necessary to assure the safety of officers and others. When deciding whether to remove restraints from a detainee, officers should continuously weigh the safety interests at hand against the continuing intrusion upon the detainee.

301.3.2 RESTRAINT OF PREGNANT PERSONS

Persons who are known to be pregnant should be restrained in the least restrictive manner that is effective for officer safety. Leg restraints, waist chains, or handcuffs behind the body should not be used unless the officer has a reasonable suspicion that the person may resist, attempt escape, injure themselves or others, or damage property.

No person who is in labor, delivery, or recovery after delivery shall be handcuffed or restrained except in extraordinary circumstances, and only when a supervisor makes an individualized determination that such restraints are necessary for the safety of the detainee, officers, or others.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Handcuffing and Restraints

See the Transporting Persons in Custody Policy for guidelines relating to transporting pregnant persons.

301.3.3 RESTRAINT OF JUVENILES

A juvenile under 14 years of age should not be restrained unless he/she is suspected of a dangerous felony or when the officer has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the officer or damage property.

301.4 HANDCUFFS OR PLASTIC CUFFS

Handcuffs, including temporary nylon or plastic cuffs, may be used only to restrain a person's hands to ensure officer safety.

Although recommended for most arrest situations, handcuffing is discretionary and not an absolute requirement of the Department. Officers should consider handcuffing any person they reasonably believe warrants that degree of restraint. However, officers should not conclude that in order to avoid risk every person should be handcuffed, regardless of the circumstances.

In most situations handcuffs should be applied with the hands behind the person's back. When feasible, handcuffs should be double-locked to prevent tightening, which may cause undue discomfort or injury to the hands or wrists.

In situations where one pair of handcuffs does not appear sufficient to restrain the individual or may cause unreasonable discomfort due to the person's size, officers should consider alternatives, such as using an additional set of handcuffs or multiple plastic cuffs.

Handcuffs should be removed as soon as it is reasonable or after the person has been searched and is safely confined within a detention facility.

301.5 SPIT HOODS

Spit hoods/masks/socks are temporary protective devices designed to prevent the wearer from biting and/or transferring or transmitting fluids (saliva and mucous) to others.

Spit hoods may be placed upon persons in custody when the officer reasonably believes the person will bite or spit, either on a person or in an inappropriate place. They are generally used during application of a physical restraint, while the person is restrained, or during or after transport.

Officers utilizing spit hoods should ensure that the spit hood is fastened properly to allow for adequate ventilation and that the restrained person can breathe normally. Officers should provide assistance during the movement of restrained individuals due to the potential for impaired or distorted vision on the part of the individual. Officers should avoid comingling individuals wearing spit hoods with other detainees.

Spit hoods should not be used in situations where the restrained person is bleeding profusely from the area around the mouth or nose, or if there are indications that the person has a medical condition, such as difficulty breathing or vomiting. In such cases, prompt medical care should be obtained. If the person vomits while wearing a spit hood, the spit hood should be promptly removed.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Handcuffing and Restraints

and discarded. Persons who have been sprayed with oleoresin capicum (OC) spray should be thoroughly decontaminated including hair, head and clothing prior to application of a spit hood.

Those who have been placed in a spit hood should be continually monitored and shall not be left unattended until the spit hood is removed. Spit hoods shall be discarded after each use.

301.6 AUXILIARY RESTRAINT DEVICES

Auxiliary restraint devices include transport belts, waist or belly chains, transportation chains, leg restraints, and other similar devices. Auxiliary restraint devices are intended for use during long-term restraint or transportation. They provide additional security and safety without impeding breathing, while permitting adequate movement, comfort, and mobility.

Only department-authorized devices may be used. Any person in auxiliary restraints should be monitored as reasonably appears necessary.

301.7 LEG RESTRAINT DEVICES

Leg restraints may be used to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest or transportation. Only restraint devices approved by the department shall be used.

In determining whether to use the leg restraint, officers should consider:

- (a) Whether the officer or others could be exposed to injury due to the assaultive or resistant behavior of a suspect.
- (b) Whether it is reasonably necessary to protect the suspect from his/her own actions (e.g., hitting his/her head against the interior of the patrol unit, running away from the arresting officer while handcuffed, kicking at objects or officers).
- (c) Whether it is reasonably necessary to avoid damage to property (e.g., kicking at windows of the patrol unit).

301.7.1 GUIDELINES FOR USE OF LEG RESTRAINTS

When applying leg restraints, the following guidelines should be followed:

- (a) If practicable, officers should notify a supervisor of the intent to apply the leg restraint device. In all cases, a supervisor shall be notified as soon as practicable after the application of the leg restraint device.
- (b) Once applied, absent a medical or other emergency, restraints should remain in place until the officer arrives at the jail or other facility or the person no longer reasonably appears to pose a threat.
- (c) Once secured, the person should be placed in a seated or upright position, secured with a seat belt, and shall not be placed on their stomach for an extended period, as this could reduce the person's ability to breathe.
- (d) The restrained person should be continually monitored by an officer while in the leg restraint. The officer should ensure that the person does not roll onto and remain on their stomach.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Handcuffing and Restraints

- (e) The officer should look for signs of labored breathing and take appropriate steps to relieve and minimize any obvious factors contributing to this condition.

301.8 TRAINING

The Support Services Commander should ensure that officers receive periodic training on the proper use of handcuffs and other restraints, including:

- (a) Proper placement and fit of handcuffs and other restraint devices approved for use by the Department.
- (b) Response to complaints of pain by restrained persons.
- (c) Options for restraining those who may be pregnant without the use of leg restraints, waist chains, or handcuffs behind the body.
- (d) Options for restraining amputees or those with medical conditions or other physical conditions that may be aggravated by being restrained.
- (e) Proper placement of safely secured persons into an upright or seated position to avoid placement on the stomach for an extended period, as this could reduce the person's ability to breathe.

Control Devices

302.1 PURPOSE AND SCOPE

This policy provides guidelines for the use and maintenance of control devices that are described in this policy.

302.2 POLICY

In order to control subjects who are violent or who demonstrate the intent to be violent, the South Saint Paul Police Department authorizes officers to use control devices in accordance with the guidelines in this policy and the Use of Force Policy.

302.3 ISSUING, CARRYING AND USING CONTROL DEVICES

Control devices described in this policy may be carried and used by members of this department only if the device has been issued by the Department or approved by the Chief of Police or the authorized designee.

Only officers who have successfully completed department-approved training in the use of any control device are authorized to carry and use the device.

Control devices may be used when a decision has been made to control, restrain or arrest a subject who is violent or who demonstrates the intent to be violent, and the use of the device appears reasonable under the circumstances. When reasonable, a verbal warning and opportunity to comply should precede the use of these devices.

When using control devices, officers should carefully consider potential impact areas in order to minimize injuries and unintentional targets.

302.4 RESPONSIBILITIES

302.4.1 OPERATIONS COMMANDER RESPONSIBILITIES

The Operations Commander shall control the inventory and issuance of all control devices and shall ensure that all damaged, inoperative, outdated or expended control devices or munitions are properly disposed of, repaired or replaced.

Every control device will be periodically inspected by the Operations Commander or the designated instructor for a particular control device. The inspection shall be documented.

302.4.2 USER RESPONSIBILITIES

All normal maintenance, charging or cleaning shall remain the responsibility of personnel using the various devices.

Any damaged, inoperative, outdated or expended control devices or munitions, along with documentation explaining the cause of the damage, shall be returned to the Operations Commander for disposition. Damage to City property forms shall also be prepared and forwarded through the chain of command, when appropriate, explaining the cause of damage.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Control Devices

302.5 BATON GUIDELINES

The need to immediately control a suspect must be weighed against the risk of causing serious injury. The head, neck, throat, spine, heart, kidneys, and groin should not be intentionally targeted except when the officer reasonably believes the use of deadly force is appropriate. See the Use of Force Policy for additional guidance.

When carrying a baton, uniformed personnel shall carry the baton in its authorized holder on the equipment belt. Plainclothes and non-field personnel may carry the baton as authorized and in accordance with the needs of their assignment or at the direction of their supervisor.

302.6 OLEORESIN CAPSICUM (OC) GUIDELINES

As with other control devices, oleoresin capsicum (OC) spray and pepper projectiles may be considered for use to bring under control an individual or groups of individuals who are engaging in, or are about to engage in violent behavior. Pepper projectiles and OC spray, generally, should not be used against individuals or groups who merely fail to disperse or do not reasonably appear to present a risk to the safety of officers or the public absent special circumstances.

302.6.1 OC SPRAY

Uniformed personnel carrying OC spray shall carry the device in its holster on the equipment belt. Plainclothes and non-field personnel may carry OC spray as authorized, in accordance with the needs of their assignment or at the direction of their supervisor.

302.6.2 PEPPER PROJECTILE SYSTEMS

Pepper projectiles are plastic spheres that are filled with a derivative of OC powder. Because the compressed gas launcher delivers the projectiles with enough force to burst the projectiles on impact and release the OC powder, the potential exists for the projectiles to inflict injury if they strike the head, neck, spine, or groin. Therefore, personnel deploying a pepper projectile system should not intentionally target those areas, except when the officer reasonably believes the use of deadly force is appropriate. See the Use of Force Policy for additional guidance.

Officers encountering a situation that warrants the use of a pepper projectile system shall notify a supervisor as soon as practicable. A supervisor shall respond to all pepper projectile system incidents where the suspect has been hit or exposed to the chemical agent. The supervisor shall ensure that all notifications and reports are completed as required by the Use of Force Policy.

Each deployment of a pepper projectile system shall be documented when directed or pointed toward a suspect, whether or not the launcher was used. Unintentional discharges shall be promptly reported to a supervisor and documented on the appropriate report form. Only non-incident use of a pepper projectile system, such as training and product demonstrations, is exempt from the reporting requirement.

302.6.3 TREATMENT FOR OC SPRAY EXPOSURE

Persons who have been sprayed with or otherwise affected by the use of OC should be promptly provided with clean water to cleanse the affected areas. Those persons who complain of further severe effects shall be examined by appropriate medical personnel.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Control Devices

302.7 POST-APPLICATION NOTICE

Whenever tear gas or OC has been introduced into a residence, building interior, vehicle, or other enclosed area, officers should provide the owners or available occupants with notice of the possible presence of residue that could result in irritation or injury if the area is not properly cleaned. Such notice should include advisement that cleanup will be at the owner's expense. Information regarding the method of notice and the individuals notified should be included in related reports.

302.8 KINETIC ENERGY PROJECTILE GUIDELINES

This department is committed to reducing the potential for violent confrontations. Kinetic energy projectiles, when used properly, are less likely to result in death or serious physical injury and can be used in an attempt to de-escalate a potentially deadly situation.

302.8.1 DEPLOYMENT AND USE

Only department-approved kinetic energy munitions shall be carried and deployed. Approved munitions may be used to compel an individual to cease his/her actions when such munitions present a reasonable option.

Officers are not required or compelled to use approved munitions in lieu of other reasonable tactics if the involved officer determines that deployment of these munitions cannot be done safely. The safety of hostages, innocent persons and officers takes priority over the safety of subjects engaged in criminal or suicidal behavior.

Circumstances appropriate for deployment include, but are not limited to, situations in which:

- (a) The suspect is armed with a weapon and the tactical circumstances allow for the safe application of approved munitions.
- (b) The suspect has made credible threats to harm him/herself or others.
- (c) The suspect is engaged in riotous behavior or is throwing rocks, bottles or other dangerous projectiles at people and/or officers.
- (d) There is probable cause to believe that the suspect has already committed a crime of violence and is refusing to comply with lawful orders.

302.8.2 DEPLOYMENT CONSIDERATIONS

Before discharging projectiles, the officer should consider such factors as:

- (a) Distance and angle to target.
- (b) Type of munitions employed.
- (c) Type and thickness of subject's clothing.
- (d) The subject's proximity to others.
- (e) The location of the subject.
- (f) Whether the subject's actions dictate the need for an immediate response and the use of control devices appears appropriate.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Control Devices

A verbal warning of the intended use of the device should precede its application, unless it would otherwise endanger the safety of officers or when it is not practicable due to the circumstances. The purpose of the warning is to give the individual a reasonable opportunity to voluntarily comply and to warn other officers and individuals that the device is being deployed.

Officers should keep in mind the manufacturer's recommendations and their training regarding effective distances and target areas. However, officers are not restricted solely to use according to manufacturer recommendations. Each situation must be evaluated on the totality of circumstances at the time of deployment.

The need to immediately incapacitate the subject must be weighed against the risk of causing serious injury or death. The head and neck should not be intentionally targeted, except when the officer reasonably believes the use of deadly force is appropriate. See the Use of Force Policy for additional guidance.

302.8.3 SAFETY PROCEDURES

Officers will inspect the energy projectile system and projectiles at the beginning of each shift to ensure that the energy projectile system is in proper working order and the projectiles are of the approved type and appear to be free from defects.

When it is not deployed, the energy projectile system will be unloaded and properly and securely stored in the vehicle.

302.9 TRAINING FOR CONTROL DEVICES

The Support Services Commander shall ensure that all personnel who are authorized to carry a control device have been properly trained and certified to carry the specific control device and are retrained or recertified as necessary. Officers will receive training on the use of issued control devices and this policy, including the learning objectives as provided by POST, at least annually (Minn. Stat. § 626.8452, Subd. 3).

- (a) Proficiency training shall be monitored and documented by a certified, control-device weapons or tactics instructor.
- (b) All training and proficiency for control devices will be documented in the officer's training file.
- (c) Officers who fail to demonstrate proficiency with the control device or knowledge of this agency's Use of Force Policy will be provided remedial training. If an officer cannot demonstrate proficiency with a control device or knowledge of this agency's Use of Force Policy after remedial training, the officer will be restricted from carrying the control device and may be subject to discipline.

302.10 REPORTING USE OF CONTROL DEVICES AND TECHNIQUES

Any application of a control device or technique listed in this policy shall be documented in the related incident report and reported pursuant to the Use of Force Policy.

Conducted Energy Device

303.1 PURPOSE AND SCOPE

This policy provides guidelines for the issuance and use of the conducted energy device (CED).

303.2 POLICY

The CED is used in an attempt to control a violent or potentially violent individual. The appropriate use of such a device may result in fewer serious injuries to officers and suspects.

303.3 ISSUANCE AND CARRYING CEDS

Only members who have successfully completed department-approved training may be issued and may carry the CED.

The Operations Commander should keep a log of issued CED devices and the serial numbers of cartridges/magazines issued to members.

CEDs are issued for use during a member's current assignment. Those leaving a particular assignment may be required to return the device to the department inventory.

Officers shall only use the CED and cartridges/magazines that have been issued by the Department. Cartridges/magazines should not be used after the manufacturer's expiration date.

Uniformed officers who have been issued the CED shall wear the device in an approved holster.

Officers who carry the CED while in uniform shall carry it in a holster on the side opposite the duty weapon.

- (a) All CEDs shall be clearly distinguishable to differentiate them from the duty weapon and any other device.
- (b) Officers should not hold a firearm and the CED at the same time.

Non-uniformed officer may secure the CED in a concealed, secure location in the driver's compartment of their vehicles.

303.3.1 USER RESPONSIBILITIES

Officers shall be responsible for ensuring that the issued CED is properly maintained and in good working order. This includes a function test and battery life monitoring, as required by the manufacturer, and should be completed prior to the beginning of the officer's shift.

CEDs that are damaged or inoperative, or cartridges/magazines that are expired or damaged, shall be returned to the Operations Commander for disposition. Officers shall submit documentation stating the reason for the return and how the CED or cartridge/magazine was damaged or became inoperative, if known.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Conducted Energy Device

303.4 VERBAL AND VISUAL WARNINGS

A verbal warning of the intended use of the CED should precede its application, unless it would otherwise endanger the safety of officers or when it is not practicable due to the circumstances. The purpose of the warning is to:

- (a) Provide the individual with a reasonable opportunity to voluntarily comply.
- (b) Provide other officers and individuals with a warning that the CED may be deployed.

If, after a verbal warning, an individual fails to voluntarily comply with an officer's lawful orders and it appears both reasonable and feasible under the circumstances, the officer may, but is not required to, activate any warning on the device, which may include display of the electrical arc, an audible warning, or the laser in a further attempt to gain compliance prior to the application of the CED. The laser should not be intentionally directed into anyone's eyes.

The fact that a verbal or other warning was given or the reasons it was not given shall be documented by the officer deploying the CED in the related report.

303.5 DOCUMENTATION

Officers shall document all CED discharges in the related arrest/crime reports and the aggression/resistance form. Photographs should be taken of any obvious probe impact or drive-stun application sites and attached to the CED report form. Notification shall also be made to a supervisor in compliance with the Use of Force Policy. Unintentional discharges, pointing the device at a person, audible warning, laser activation, and arcing the device, other than for testing purposes, will also be documented on the report form. Data downloads from the CED after use on a subject should be done as soon as practicable using a department-approved process to preserve the data.

303.5.1 AGGRESSION/RESISTANCE FORM

As applicable based on the device type, items that shall be included in the aggression/resistance form are:

- (a) The brand, model, and serial number of the CED and any cartridge/magazine.
- (b) Date, time, and location of the incident.
- (c) Whether any warning, display, laser, or arc deterred a subject and gained compliance.
- (d) The number of probes deployed, CED activations, the duration of each cycle, the duration between activations, and (as best as can be determined) the duration that the subject received applications.
- (e) The range at which the CED was used.
- (f) The type of mode used (e.g., probe deployment, drive-stun).
- (g) Location of any probe impact.
- (h) Location of contact in drive-stun mode.
- (i) Description of where missed probes went.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Conducted Energy Device

- (j) Whether medical care was provided to the subject.
- (k) Whether the subject sustained any injuries.
- (l) Whether any officers sustained any injuries.

303.5.2 REPORTS

The officer should include the following in the arrest/crime report:

- (a) Identification of all personnel firing CEDs
- (b) Identification of all witnesses
- (c) Medical care provided to the subject
- (d) Observations of the subject's physical and physiological actions
- (e) Any known or suspected drug use, intoxication, or other medical problems

303.6 MEDICAL TREATMENT

Consistent with local medical personnel protocols and absent extenuating circumstances, only appropriate medical personnel or officers trained in probe removal and handling should remove CED probes from a person's body. Used CED probes shall be treated as a sharps biohazard, similar to a used hypodermic needle, and handled appropriately. Universal precautions should be taken.

All persons who have been struck by CED probes, who have been subjected to the electric discharge of the device, or who sustained direct exposure of the laser to the eyes shall be medically assessed prior to booking. Additionally, any such individual who falls under any of the following categories should, as soon as practicable, be examined by paramedics or other qualified medical personnel:

- (a) The person is suspected of being under the influence of controlled substances and/or alcohol.
- (b) The person may be pregnant.
- (c) The person reasonably appears to be in need of medical attention.
- (d) The CED probes are lodged in a sensitive area (e.g., groin, female breast, head, face, neck).
- (e) The person requests medical treatment.

Any individual exhibiting signs of distress or who is exposed to multiple or prolonged applications shall be transported to a medical facility for examination or medically evaluated prior to booking. If any individual refuses medical attention, such a refusal should be witnessed by another officer and/or medical personnel and shall be fully documented in related reports. If an audio/video recording is made of the contact or an interview with the individual, any refusal should be included, if possible.

The transporting officer shall inform any person providing medical care or receiving custody that the individual has been subjected to the application of the CED (see the Medical Aid and Response Policy).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Conducted Energy Device

303.7 SUPERVISOR RESPONSIBILITIES

When possible, supervisors should respond to calls when they reasonably believe there is a likelihood the CED may be used. A supervisor should respond to all incidents where the CED was activated.

A supervisor should review each incident where a person has been exposed to a CED. The device's internal logs should be downloaded by a supervisor, Operations Commander, or designee and saved with the related arrest/crime report. The supervisor should arrange for photographs of probe sites to be taken and witnesses to be interviewed.

303.8 TRAINING

Personnel who are authorized to carry the CED shall be permitted to do so only after successfully completing the initial department-approved training. Any personnel who have not carried the CED as a part of their assignments for a period of six months or more shall be recertified by a qualified CED instructor prior to again carrying or using the device.

Personnel who have been issued CEDs will receive training on this policy, including the learning objectives as provided by POST, at least annually (Minn. Stat. § 626.8452, Subd. 3).

A reassessment of an officer's knowledge and/or practical skills may be required at any time, if deemed appropriate, by the Support Services Commander. All training and proficiency for CEDs will be documented in the officer's training files.

Command staff, supervisors, and investigators should receive CED training as appropriate for the investigations they conduct and review.

Officers who do not carry CEDs should receive training that is sufficient to familiarize them with the device and with working with officers who use the device.

The Support Services Commander is responsible for ensuring that all members who carry CEDs have received initial and annual proficiency training. Periodic audits should be used for verification.

Application of CEDs during training could result in injuries and should not be mandatory for certification.

The Support Services Commander should include the following training:

- (a) A review of this policy.
- (b) A review of the Use of Force Policy.
- (c) Performing weak-hand draws or cross-draws until proficient to reduce the possibility of unintentionally drawing and firing a firearm.
- (d) Target area considerations, to include techniques or options to reduce the unintentional application of probes to the head, neck, area of the heart, and groin.
- (e) Scenario-based training, including virtual reality training when available.
- (f) Handcuffing a subject during the application of the CED and transitioning to other force options.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Conducted Energy Device

- (g) De-escalation techniques.
- (h) Restraint techniques that do not impair respiration following the application of the CED.
- (i) Proper use of cover and concealment during deployment of the CED for purposes of officer safety.
- (j) Proper tactics and techniques related to multiple applications of CEDs.

Officer-Involved Shootings and Deaths

304.1 PURPOSE AND SCOPE

The purpose of this policy is to establish policy and procedures for the investigation of an incident in which a person is injured or dies as the result of an officer-involved shooting or dies as a result of another action of an officer.

In other incidents not covered by this policy, the Chief of Police may decide that the investigation will follow the process provided in this policy.

304.2 TYPES OF INVESTIGATIONS

Officer-involved shootings and deaths involve several separate investigations. The investigations may include:

- A criminal investigation of the suspect's actions.
- A criminal investigation of the involved officer's actions.
- An administrative investigation as to policy compliance by involved officers.
- A civil investigation to determine potential liability.

304.3 JURISDICTION

Jurisdiction is determined by the location of the shooting and the agency employing the involved officer(s). The following scenarios outline the jurisdictional responsibilities for investigating officer-involved shootings:

304.3.1 SOUTH SAINT PAUL POLICE DEPARTMENT OFFICER WITHIN THIS JURISDICTION

The South Saint Paul Police Department is responsible for the criminal investigation of the suspect's actions, the civil investigation and the administrative investigation. The criminal investigation of the officer-involved shooting will be conducted by an uninvolved outside law enforcement agency asked to conduct the investigation.

304.3.2 OUTSIDE AGENCY'S PEACE OFFICER WITHIN THIS JURISDICTION

The South Saint Paul Police Department is responsible for the criminal investigation of the suspect's actions. The criminal investigation of the officer-involved shooting will be conducted by this department or an uninvolved outside agency. The officer's employing agency will be responsible for any civil and/or administrative investigation(s).

304.3.3 SOUTH SAINT PAUL POLICE DEPARTMENT OFFICER IN ANOTHER JURISDICTION

The agency where the incident occurred has criminal jurisdiction and is responsible for the criminal investigation of the incident. That agency may relinquish its criminal investigation of the suspect(s) to another agency. The South Saint Paul Police Department will conduct timely civil and/or administrative investigations of its own personnel.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

304.3.4 POST ADMINISTRATIVE INVESTIGATIONS

The Minnesota POST Board may require an administrative investigation based on a complaint alleging a violation of a statute or rule that the board is empowered to enforce. An officer-involved shooting may result in such an allegation. Any such complaint assigned to this department shall be completed and a written summary submitted to the POST executive director within 30 days of the order for inquiry (Minn. Stat. § 214.10, Subd. 10).

304.3.5 COOPERATION WITH BUREAU OF CRIMINAL APPREHENSION INVESTIGATIONS

The Department will fully cooperate with and promptly respond to requests for information from the Bureau of Criminal Apprehension regarding an officer-involved death investigation (Minn. Stat. § 626.5534).

304.4 INVESTIGATION PROCESS

The following procedures are guidelines used in the investigation of an officer-involved shooting or death.

304.4.1 UNINVOLVED OFFICER RESPONSIBILITIES

Upon arrival at the scene of an officer-involved shooting or death, the first uninvolved SSP PD officer will be the officer-in-charge and will assume the responsibilities of a supervisor until properly relieved. This officer should, as appropriate:

- (a) Secure the scene and identify and eliminate hazards for all those involved.
- (b) Take reasonable steps to obtain emergency medical attention for injured individuals.
- (c) Request additional resources from the Department or other agencies.
- (d) Coordinate a perimeter or pursuit of suspects.
- (e) Check for injured persons and evacuate as needed.
- (f) Brief the supervisor upon arrival.

304.4.2 SUPERVISOR RESPONSIBILITIES

Upon arrival at the scene, the first uninvolved SSP PD supervisor should ensure completion of the duties as outlined above, plus:

- (a) Attempt to obtain a brief overview of the situation from any uninvolved officers.
 - 1. In the event that there are no uninvolved officers who can supply adequate overview, the supervisor should attempt to obtain a brief voluntary overview from one involved officer.
- (b) If necessary, the supervisor may administratively order any SSP PD officer to immediately provide public safety information necessary to secure the scene, identify injured parties and pursue suspects.
 - 1. Public safety information shall be limited to such things as outstanding suspect information, number and direction of any shots fired, perimeter of the incident scene, identity of known or potential witnesses and any other pertinent information.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

2. The initial on-scene supervisor should not attempt to order any involved officer to provide any information other than public safety information.
- (c) Provide all available information to the Sergeant and Dispatch. If feasible, sensitive information should be communicated over secure networks.
- (d) Take command of and secure the incident scene with additional SSP PD members until properly relieved by another supervisor or other assigned personnel or investigator.
- (e) As soon as practicable, ensure that involved officers are transported (separately, if feasible) to a suitable location for further direction.
 1. Each involved SSP PD officer should be given an administrative order not to discuss the incident with other involved officers or SSP PD members pending further direction from a supervisor.
 2. When an involved officer's weapon is taken or left at the scene for other than officer-safety reasons (e.g., evidence), ensure that he/she is provided with a comparable replacement weapon or transported by other officers.

304.4.3 NOTIFICATIONS

The following person(s) shall be notified as soon as practicable:

- Chief of Police
- Support Services Division Commander
- Operations Division Commander
- Outside agency investigators (if appropriate)
- Psychological/peer support personnel
- Medical Examiner (if necessary)
- Officer representative (if requested)

All outside inquiries about the incident shall be directed to the Police Chief, or if unavailable Command Staff.

304.4.4 INVOLVED OFFICERS

The following shall be considered for the involved officer:

- (a) Any request for legal or union representation will be accommodated.
 1. Involved SSP PD officers shall not be permitted to meet collectively or in a group with an attorney or any representative prior to providing a formal interview or report.
 2. Requests from involved non-SSP PD officers should be referred to their employing agency.
- (b) Discussions with licensed attorneys will be considered privileged as attorney-client communications.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

- (c) Discussions with agency representatives/employee groups will be privileged only as to the discussion of non-criminal information.
- (d) A licensed psychotherapist shall be provided by the Department to each involved SSP PD officer. A licensed psychotherapist may also be provided to any other affected SSP PD members, upon request.
 - 1. Interviews with a licensed psychotherapist will be considered privileged.
 - 2. An interview or session with a licensed psychotherapist may take place prior to the member providing a formal interview or report. However, the involved members shall not be permitted to consult or meet collectively or in a group with a licensed psychotherapist prior to providing a formal interview or report.
 - 3. A separate fitness-for-duty exam may also be required (see the Fitness for Duty Policy).
- (e) Communications between the involved officer and a peer support member, peer support counselors, and critical incident stress management team members are addressed in the Wellness Program Policy.

Care should be taken to preserve the integrity of any physical evidence present on the involved officer's equipment or clothing, such as blood or fingerprints, until investigators or lab personnel can properly retrieve it.

Each involved SSP PD officer shall be given reasonable paid administrative leave following an officer-involved shooting or death. It shall be the responsibility of the Sergeant to make schedule adjustments to accommodate such leave.

304.5 CRIMINAL INVESTIGATION

The County and City Attorney Offices's Office is responsible for the criminal investigation into the circumstances of any officer-involved shooting involving injury or death.

If available, investigative personnel from this department may be assigned to partner with investigators from outside agencies or the County and City Attorney Offices's Office to avoid duplicating efforts in related criminal investigations.

Once public safety issues have been addressed, criminal investigators should be given the opportunity to obtain a voluntary statement from involved officers and to complete their interviews.

The following shall be considered for the involved officer:

- (a) SSP PD supervisors and Support Services Commander personnel should not participate directly in any voluntary interview of SSP PD officers. This will not prohibit such personnel from monitoring interviews or providing the criminal investigators with topics for inquiry.
- (b) If requested, any involved officer will be afforded the opportunity to consult individually with a representative of the officer's choosing or an attorney prior to speaking with criminal investigators. However, in order to maintain the integrity of each involved officer's statement, involved officers shall not consult or meet with a representative or an attorney collectively or in groups prior to being interviewed.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

- (c) If any involved officer is physically, emotionally, or otherwise not in a position to provide a voluntary statement when interviewed by criminal investigators, consideration should be given to allowing a reasonable period for the officer to schedule an alternate time for the interview.
- (d) Any voluntary statement provided by an involved officer will be made available for inclusion in any related investigation, including administrative investigations. However, no administratively coerced statement will be provided to any criminal investigators unless the officer consents.

304.5.1 REPORTS BY INVOLVED SSP PD OFFICERS

In the event that suspects remain outstanding or subject to prosecution for related offenses, this department shall retain the authority to require involved SSP PD officers to provide sufficient information for related criminal reports to facilitate the apprehension and prosecution of those individuals.

While the involved SSP PD officer may write the report, it is generally recommended that such reports be completed by assigned investigators, who should interview all involved officers as victims/witnesses. Since the purpose of these reports will be to facilitate criminal prosecution, statements of involved officers should focus on evidence to establish the elements of criminal activities by suspects. Care should be taken not to duplicate information provided by involved officers in other reports.

Nothing in this section shall be construed to deprive an involved SSP PD officer of the right to consult with legal counsel prior to completing any such criminal report.

Reports related to the prosecution of criminal suspects will be processed according to normal procedures but should also be included for reference in the investigation of the officer-involved shooting or death.

304.5.2 WITNESS IDENTIFICATION AND INTERVIEWS

Because potential witnesses to an officer-involved shooting or death may become unavailable or the integrity of their statements compromised with the passage of time, a supervisor should take reasonable steps to promptly coordinate with criminal investigators to utilize available law enforcement personnel for the following:

- (a) Identification of all persons present at the scene and in the immediate area.
 - 1. When feasible, a recorded statement should be obtained from those persons who claim not to have witnessed the incident but who were present at the time it occurred.
 - 2. Any potential witness who is unwilling or unable to remain available for a formal interview should not be detained absent reasonable suspicion to detain or probable cause to arrest. Without detaining the individual for the sole purpose of identification, attempts to identify the witness prior to his/her departure should be made whenever feasible.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

- (b) Witnesses who are willing to provide a formal interview should be asked to meet at a suitable location where criminal investigators may obtain a recorded statement. Such witnesses, if willing, may be transported by a member of the Department.
 - 1. A written, verbal or recorded statement of consent should be obtained prior to transporting a witness. When the witness is a minor, consent should be obtained from the parent or guardian, if available, prior to transportation.
- (c) Promptly contacting the suspect's known family and associates to obtain any available and untainted background information about the suspect's activities and state of mind prior to the incident.

304.5.3 INVESTIGATIVE PERSONNEL

Once notified of an officer-involved shooting or death, it shall be the responsibility of the designated Investigations supervisor to assign appropriate investigative personnel to handle the investigation of related crimes. Department investigators will be assigned to work with investigators from the County and City Attorney Offices's Office and may be assigned to separately handle the investigation of any related crimes not being investigated by the County and City Attorney Offices's Office.

All related department reports, except administrative and/or privileged reports, will be forwarded to the designated Investigations supervisor for approval. Privileged reports shall be maintained exclusively by members who are authorized such access. Administrative reports will be forwarded to the appropriate Division Commander.

304.6 ADMINISTRATIVE INVESTIGATION

In addition to all other investigations associated with an officer-involved shooting or death, this department will conduct an internal administrative investigation of involved SSP PD officers to determine conformance with department policy. This investigation will be conducted under the supervision of the Support Services Commander and will be considered a confidential officer personnel file.

Interviews of members shall be subject to department policies and applicable laws (Personnel Complaints Policy; Minn. Stat. § 626.89).

- (a) Any officer involved in a shooting or death may be requested or administratively compelled to provide a blood sample for alcohol/drug screening in accordance with the drug and alcohol testing guidelines in the Alcohol and Drug Use Policy adopted under the authority of Minn. Stat. § 181.950 to Minn. Stat. § 181.957. Absent consent from the officer, such compelled samples and the results of any such testing shall not be disclosed to any criminal investigative agency.
- (b) If any officer has voluntarily elected to provide a statement to criminal investigators, the assigned administrative investigator should review that statement before proceeding with any further interview of that involved officer.
 - 1. If a further interview of the officer is deemed necessary to determine policy compliance, care should be taken to limit the inquiry to new areas with minimal, if any, duplication of questions addressed in the voluntary statement. The involved

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

officer shall be provided with a copy of his/her prior statement before proceeding with any subsequent interviews.

- (c) In the event that an involved officer has elected not to provide criminal investigators with a voluntary statement, the assigned administrative investigator shall conduct an administrative interview to determine all relevant information (Minn. Stat. § 626.89).
 - 1. Although this interview should not be unreasonably delayed, care should be taken to ensure that the officer's physical and psychological needs have been addressed before commencing the interview.
 - 2. The interview must be taken at the SSP PD or at a place agreed to by the interviewer and the involved officer.
 - 3. The interview must be of reasonable duration and provide the involved officer reasonable periods for rest and personal necessities. When practicable, the interview must be held during the involved officer's regularly scheduled work shift. If not, the involved officer must be compensated at his/her current pay rate.
 - 4. If requested, the officer shall have the opportunity to select an uninvolved representative or an attorney, or both, to be present during the interview. However, in order to maintain the integrity of each individual officer's statement, involved officers shall not consult or meet with a representative collectively or in groups prior to being interviewed.
 - 5. Administrative interviews shall be recorded electronically or otherwise by the investigator. The officer may also record the interview. A complete copy or transcript of the interview must be provided to the involved officer upon written request without charge or undue delay.
 - 6. The officer shall be informed of the nature of the investigation. If an officer refuses to answer questions, he/she should be given his/her Garrity rights and ordered to provide full and truthful answers to all questions. The officer shall be informed in writing or on the record that the interview will be for administrative purposes only and that the statement cannot be used criminally.
 - 7. The Support Services Commander shall compile all relevant information and reports necessary for the Department to determine compliance with applicable policies.
 - 8. Regardless of whether the use of force is an issue in the case, the completed administrative investigation shall be submitted to Command Staff, which will restrict its findings as to whether there was compliance with the Use of Force Policy.
 - 9. Any other indications of potential policy violations shall be determined in accordance with standard disciplinary procedures.

304.7 CIVIL LIABILITY RESPONSE

A member of this department may be assigned to work exclusively under the direction of the legal counsel for the Department to assist in the preparation of materials deemed necessary in anticipation of potential civil litigation.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

All materials generated in this capacity shall be considered attorney work product and may not be used for any other purpose. The civil liability response is not intended to interfere with any other investigation but shall be given reasonable access to all other investigations.

304.8 AUDIO AND VIDEO RECORDINGS

Any officer involved in a shooting or death may be permitted to review available Mobile Audio/Video (MAV), body-worn video, or other video or audio recordings prior to providing a recorded statement or completing reports.

Upon request, non-law enforcement witnesses who are able to verify their presence and their ability to contemporaneously perceive events at the scene of an incident may also be permitted to review available MAV, body-worn video, or other video or audio recordings with the approval of assigned investigators or a supervisor.

Any MAV, body-worn video, and other known video or audio recordings of an incident should not be publicly released during an ongoing investigation without consulting the prosecuting attorney or City Attorney's Office, as appropriate.

304.8.1 AUDIO AND VIDEO RECORDINGS OF USE OF FORCE INCIDENTS INVOLVING DEATHS OF INDIVIDUALS

When a person dies as a result of the use of force by an officer, the Department shall (Minn. Stat. § 13.825, Subd. 2; Minn. Stat. § 626.8473, Subd. 3):

- (a) Allow certain individuals as identified in Minn. Stat. § 13.825, upon request, to inspect all portable recording system data that documents the incident within five days of the request pursuant to the provisions of Minn. Stat. § 13.825.
- (b) Release all portable recording system data that documents the incident within 14 days of the incident pursuant to the provisions of Minn. Stat. § 13.825.

The Chief of Police should work with the Custodian of Records when redactions or denials are necessary (Minn. Stat. § 13.825, Subd. 2; Minn. Stat. § 626.8473, Subd. 3).

304.9 DEBRIEFING

Following an officer-involved shooting or death, the South Saint Paul Police Department should conduct both a Critical Incident Stress Debriefing and a tactical debriefing. See the Wellness Program Policy for guidance on Critical Incident Stress Debriefings.

304.9.1 CRITICAL INCIDENT/STRESS DEBRIEFING

A critical incident/stress debriefing should occur as soon as practicable. The Administration Division Commander is responsible for organizing the debriefing. Notes and recorded statements should not be taken because the sole purpose of the debriefing is to help mitigate the stress-related effects of a traumatic event (Minn. Stat. § 181.9732).

The debriefing is not part of any investigative process. Communications with critical incident stress management team members, as defined in Minn. Stat. § 181.9732, are confidential and shall not be disclosed except as provided in Minn. Stat. § 181.9732, Subd. 4 (Minn. Stat. § 181.9732).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer-Involved Shootings and Deaths

Members who witness a critical incident are prohibited from providing critical incident stress management services at a debriefing about the incident that they witnessed (Minn. Stat. § 181.9732).

Attendance at the debriefing shall only include those members of the Department directly involved in the incident, which can include support personnel (e.g., dispatchers, other non-sworn personnel). Family or other support personnel may attend with the concurrence of those involved in the incident. The debriefing shall be closed to the public and should be closed to all other members of the Department, including supervisory and Support Services Commander personnel.

304.9.2 TACTICAL DEBRIEFING

A tactical debriefing should take place to identify any training or areas of policy that need improvement. The Chief of Police should identify the appropriate participants. This debriefing should not be conducted until all involved members have provided recorded or formal statements to criminal and/or administrative investigators.

304.10 MEDIA RELATIONS

Any media release shall be prepared with input and concurrence from the supervisor and department representative responsible for each phase of the investigation. Releases will be available to the Sergeant, Investigation Division Commander and Police Chief in the event of inquiries from the media.

No involved SSP PD officer shall make any comment to the media unless he/she is authorized by the Chief of Police or a Division Commander.

Department members receiving inquiries regarding officer-involved shootings or deaths occurring in other jurisdictions shall refrain from public comment and will direct those inquiries to the agency having jurisdiction and primary responsibility for the investigation.

304.11 REPORTING

If an officer discharges a firearm in the course of duty, the Chief of Police shall notify the Commissioner of Public Safety within 30 days of the reason for and the circumstances surrounding the discharge of the firearm (Minn. Stat. § 626.553).

Firearms

305.1 PURPOSE AND SCOPE

This policy establishes procedures for the acquisition, use and documentation of training in the use of duty firearms. The Chief of Police or designee shall approve all duty firearms before they are acquired and utilized by any member of this department.

305.1.1 AUTHORIZATION TO CARRY FIREARMS

All licensed personnel shall successfully complete department training regarding the use of force, deadly force, and the use of firearms before being issued a firearm or being authorized to carry a firearm in the course of their duties (Minn. Stat. § 626.8452, Subd. 3; Minn. Stat. § 626.8463).

305.2 POLICY

The South Saint Paul Police Department will equip its members with firearms to address the risks posed to the public and department members by violent and sometimes well-armed persons. The Department will ensure firearms are appropriate, in good working order and that relevant training is provided as resources allow.

305.3 AUTHORIZED FIREARMS

No duty firearms will be carried that have not been thoroughly inspected by a member of the SSP PD Range Staff or Department Armorer during a regularly scheduled range date. Except in an emergency or as directed by a supervisor, no duty firearm shall be carried by a member who has not qualified with that make and model of weapon at an authorized department range.

All other weapons, including but not limited to, edged weapons, chemical or electronic weapons, impact weapons or any weapon prohibited or restricted by law or that is not covered elsewhere by department policy, may not be carried by personnel in the performance of their official duty without the express written authorization of the employee's Division Commander. This exclusion does not apply to the carrying of a single folding pocketknife that is not otherwise prohibited by law.

305.3.1 HANDGUNS

The authorized department-issued handgun is the Glock 9mm Model(s) 17, 19, 26 and 43.

305.3.2 AUTHORIZED SECONDARY FIREARMS

Officers desiring to carry a secondary firearm are subject to the following restrictions:

- (a) Must first receive approval from the Chief of Police or their designee before carrying the second firearm.
- (b) The firearm shall be in good working order and on the department's list of approved firearms.
- (c) Only one secondary firearm may be carried at a time.
- (d) The purchase of the firearm and ammunition shall be the responsibility of the officer.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Firearms

- (e) The firearm shall be carried out of sight at all times and in such a manner as to prevent unintentional cocking, discharge or loss of physical control.
- (f) The firearm shall be inspected by a member of the Department's Range Staff or Armorer prior to being carried and thereafter shall be subject to inspection whenever deemed necessary.
- (g) Ammunition shall be the same as department issue. If the caliber of the firearm is other than department issue, the Chief of Police or the authorized designee shall approve the ammunition.
- (h) Prior to carrying the secondary firearm, personnel shall qualify under range supervision and thereafter shall qualify in accordance with the department qualification schedule. Officers must demonstrate proficiency, safe handling, and that the firearm functions properly.
- (i) Personnel shall provide written notice of the make, model, color, serial number and caliber of a second firearm to the Range Staff.

305.3.3 PATROL RIFLES

The authorized department-issued patrol rifle is the Colt AR-15.

Members may deploy the patrol rifle in any circumstance where the member can articulate a reasonable expectation that the rifle may be needed. Examples of some general guidelines for deploying the patrol rifle may include, but are not limited to:

- (a) Situations where the member reasonably anticipates an armed encounter.
- (b) When a member is faced with a situation that may require accurate and effective fire at long range.
- (c) Situations where a member reasonably expects the need to meet or exceed a suspect's firepower.
- (d) When a member reasonably believes that there may be a need to fire on a barricaded person or a person with a hostage.
- (e) When a member reasonably believes that a suspect may be wearing body armor.
- (f) When authorized or requested by a supervisor.
- (g) When needed to euthanize an animal.

When not deployed, the patrol rifle shall be properly secured consistent with department training in a locking weapons rack in the patrol vehicle.

305.3.4 AMMUNITION

Officers shall carry only Department-authorized ammunition. Officers will generally be issued fresh duty ammunition in the specified quantity for all Department-issued firearms. Officers carrying personally owned authorized firearms of a caliber differing from Department-issued firearms shall be responsible for obtaining fresh duty ammunition in accordance with the above at their own expense.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Firearms

305.3.5 AUTHORIZED OFF-DUTY FIREARMS

The carrying of firearms by current license officers while off-duty is permitted by the Chief of Police but may be rescinded should circumstances dictate (e.g. administrative leave). License officers who choose to carry a firearm while off-duty, based upon their authority as a peace officer, will be required to meet the following guidelines;

- (a) The firearm shall be of good quality and workmanship.
- (b) The purchase of the firearm and ammunition shall be the responsibility of the officer.
- (c) The firearm shall be carried concealed at all times and in such a manner as to prevent unintentional cocking, discharge or loss of physical control.
- (d) It will be the responsibility of the officer to submit the firearm to a member of the Range Staff or Armorer for inspection prior to being carried. Prior to carrying any off-duty firearm, the officer shall demonstrate to the Range Staff that he/she is proficient in handling and firing the firearm and that it will be carried in a safe manner.
- (e) A complete description of the firearm shall be retained by the Operations Commander.
- (f) If any member desires to use more than one firearm while off-duty, he/she may do so, as long as the officer meets all the requirements set forth in this policy for each firearm used.
- (g) Officers shall only carry department-authorized ammunition.
- (h) When armed, whether on-duty or off-duty, officers shall carry their department identification and badge.

305.4 DUTY FIREARMS PROFICIENCY

All licensed personnel shall successfully complete Department training regarding the use of force, deadly force and the use of firearms before being issued a firearm or being authorized to carry a firearm in the course of their duties (Minn. Stat. § 626.8452 and Minn. Stat. § 626.8463).

An officer failing to demonstrate a minimum level of proficiency with any duty firearm he/she is authorized will receive remedial training as designed by the Department. Failure to show a minimum level of proficiency following the remedial training may result in the officer being prohibited from carrying a department firearm or off-duty firearm.

All licensed personnel shall participate in annual Department training regarding the use of force, deadly force and the use of firearms (Minn. Stat. § 626.8452 Subd. 3).

305.4.1 REPAIRS OR MODIFICATIONS

Each member shall be responsible for promptly reporting any damage or malfunction of an assigned firearm to a supervisor or the Operations Commander.

Firearms that are the property of the Department or personally owned firearms that are approved for department use may be repaired or modified only by a person who is department-approved and certified as an armorer or gunsmith in the repair of the specific firearm. Such modification or repair must be authorized in advance by the Operations Commander.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Firearms

Any repairs or modifications to the member's personally owned firearm shall be done at his/her expense and must be approved by the Operations Commander.

305.4.2 HOLSTERS

Only department-approved holsters shall be used and worn by members. Members assigned to uniformed patrol are required to use a retention level II or III holster. Members shall periodically inspect their holsters to make sure they are serviceable and provide the proper security and retention of the handgun.

305.5 SAFE HANDLING, INSPECTION AND STORAGE

Members shall maintain the highest level of safety when handling firearms and shall consider the following:

- (a) Members shall not unnecessarily display or handle any firearm.
- (b) Members shall be governed by all rules and regulations pertaining to the use of the range and shall obey all orders issued by the Operations Commander. Members shall not dry fire or practice quick draws except as instructed by the Operations Commander or other firearms training staff.
- (c) Generally, members shall not clean, repair, load or unload a firearm anywhere in the Department, except where clearing barrels are present.
- (d) Shotguns or rifles removed from vehicles or the equipment storage room shall be loaded and unloaded in the parking lot and outside of the vehicle, using clearing barrels.
- (e) Members shall not place or store any firearm or other weapon on department premises except where the place of storage is locked. No one shall carry firearms into the jail section or any part thereof when securing or processing an arrestee, but shall place all firearms in a secured location. Members providing access to the jail section to persons from outside agencies are responsible for ensuring firearms are not brought into the jail section.
- (f) Members shall not use any automatic firearm, heavy caliber rifle, gas or other type of chemical weapon or firearm from the armory, except with approval of a supervisor.
- (g) Any firearm authorized by the Department to be carried on- or off-duty that is determined by a member to be malfunctioning or in need of service or repair shall not be carried. It shall be promptly presented to the Department or a Operations Commander approved by the Department for inspection and repair. Any firearm deemed in need of repair or service by the Operations Commander will be immediately removed from service. If the firearm is the member's primary duty firearm, a replacement firearm will be issued to the member until the duty firearm is serviceable.

305.5.1 ALCOHOL AND DRUGS

Firearms shall not be carried by any member, either on- or off-duty, who has consumed an amount of an alcoholic beverage, taken any drugs or medication, or has taken any combination thereof that would tend to adversely affect the member's senses or judgment.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Firearms

305.5.2 STORAGE AT HOME

Members shall ensure that all firearms and ammunition are locked and secured while in their homes, vehicles or any other area under their control, and in a manner that will keep them inaccessible to children and others who should not have access. Members shall not permit department-issued firearms to be handled by anyone not authorized by the Department to do so. Members should be aware that negligent storage of a firearm could result in civil and criminal liability (Minn. Stat. § 609.666; Minn. Stat. § 609.378).

305.5.3 INSPECTION AND STORAGE

Shotguns and rifles shall be inspected at the beginning of the shift by the member to whom the weapon is issued. The member shall ensure that the firearm is carried in the proper condition and loaded with approved ammunition. Inspection of the shotgun and rifle shall be done while standing outside of the patrol vehicle. All firearms shall be pointed in a safe direction or into clearing barrels.

305.6 FIREARMS TRAINING AND QUALIFICATIONS

All members who carry a firearm while on-duty or off-duty are required to successfully complete training with their duty firearms. In addition to training, all members will qualify at least annually with their duty firearms (Minn. Stat. § 626.8452 Subd. 3). Training and qualifications must be on an approved range course.

At least annually, all members carrying a firearm should receive practical training designed to simulate field situations including low-light shooting.

The following guidelines will be observed on the department gun range:

- Must notify the on-duty supervisor or designee when the range is in use.
- Body armor required by all present when the range is in use.
- Eye and hearing protection must be worn by all when the range is in use.
- Personnel using the range must check in/out with supervisor on duty and advise of the firearms they are using.
- Clean (lead free) range ammunition only. (No dept issued ammunition)
- Approved handgun calibers only.
- Department issued firearms must be cleaned prior to check out
- Range must be cleaned of targets, brass and other items.
- Any issues or incidents must be reported to range officer or supervisor.
- AMMUNITION CONTAINING LEAD IS NOT ALLOWED TO BE USED ON THE SSP PD RANGE.

305.7 FIREARM DISCHARGE

Except during training or recreational use, any member who discharges a firearm intentionally or unintentionally, on- or off-duty, shall make a verbal report to their supervisor as soon as circumstances permit. If the discharge results in injury or death to another person, additional

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Firearms

statements and reports shall be made in accordance with the Officer-Involved Shootings and Deaths Policy. If a firearm was discharged as a use of force, the involved member shall adhere to the additional reporting requirements set forth in the Use of Force Policy.

In all other cases, written reports shall be made as follows:

- (a) If on-duty at the time of the incident, the member shall file a written report with their Division Commander or provide a recorded statement to investigators prior to the end of shift, unless otherwise directed.
- (b) If off-duty at the time of the incident, the member shall file a written report or provide a recorded statement no later than the end of the next regularly scheduled shift, unless otherwise directed by a supervisor.

305.7.1 WARNING AND OTHER SHOTS

Generally, shots fired for the purpose of summoning aid are discouraged and may not be discharged unless the member reasonably believes that they appear necessary, effective, and reasonably safe.

Warning shots shall not be used.

305.7.2 DESTRUCTION OF ANIMALS

Members are authorized to use firearms to stop an animal in circumstances where the animal reasonably appears to pose an imminent threat to human safety and alternative methods are not reasonably available or would likely be ineffective.

In circumstances where there is sufficient advance notice that a potentially dangerous animal may be encountered, department members should develop reasonable contingency plans for dealing with the animal (e.g., fire extinguisher, conducted energy device, oleoresin capsicum (OC) spray, animal control officer). Nothing in this policy shall prohibit any member from shooting a dangerous animal if circumstances reasonably dictate that a contingency plan has failed, becomes impractical, or if the animal reasonably appears to pose an imminent threat to human safety.

305.7.3 INJURED ANIMALS

With the approval of a supervisor or designee, a member may euthanize an animal that is so badly injured that human compassion requires its removal from further suffering and where other dispositions are impractical.

305.7.4 REPORTING FIREARMS DISCHARGE

The Chief of Police shall notify the Commissioner of Public Safety within 30 days of an on-duty firearm discharge, except when the discharge is in the course of training or destruction of animals (described in this policy). The notification shall contain information concerning the reason for and circumstances surrounding the discharge (Minn. Stat. § 626.553, Subd. 2).

305.8 RANGE STAFF DUTIES

The range will be under the exclusive control of the SSP PD Range Staff and Support Services Commander. All members attending will follow the directions of the Range Staff. The Range Staff

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Firearms

will maintain a roster of all members attending the range and will submit the roster to the Support Services Commander after each range date.

The range shall remain operational and accessible to Department members during hours established by the Department.

The Range Staff and Department Armorer have the responsibility of making periodic inspection, at least once a year, of all duty weapons carried by officers of this department to verify proper operation. The Range Staff and Armorer has the authority to deem any privately owned weapon unfit for service. The officer will be responsible for all repairs to his/her personal weapon; it will not be returned to service until inspected by the Operations Commander.

The Range Staff has the responsibility to ensure each officer on a yearly basis can demonstrate proficiency in the care and cleaning of the duty weapon.

The Range Staff shall complete and submit to the Support Services Commander documentation of the courses provided, including the qualifications of each instructor, a description of the training provided and a list of each officer who completes training. This list should be entered on a form that has been approved by the POST Board.

305.9 FLYING WHILE ARMED

The Transportation Security Administration (TSA) has imposed rules governing law enforcement officers flying armed on commercial aircraft. The following requirements apply to officers who intend to be armed while flying on a commercial air carrier or flights where screening is conducted (49 CFR 1544.219):

- (a) Officers wishing to fly while armed must be flying in an official capacity, not for vacation or pleasure, and must have a need to have the firearm accessible, as determined by the Department based on the law and published TSA rules.
- (b) Officers must carry their South Saint Paul Police Department identification card bearing the officer's name, a full-face photograph, identification number, the officer's signature, and the signature of the Chief of Police or the official seal of the Department and must present this identification to airline officials when requested. The officer should also carry the standard photo identification needed for passenger screening by airline and TSA officials (e.g., driver's license, passport).
- (c) The South Saint Paul Police Department must submit a National Law Enforcement Telecommunications System (NLETS) message prior to the officer's travel. If approved, TSA will send the South Saint Paul Police Department an NLETS message containing a unique alphanumeric identifier. The officer must present the message on the day of travel to airport personnel as authorization to travel while armed.
- (d) An official letter signed by the Chief of Police authorizing armed travel may also accompany the officer. The letter should outline the officer's need to fly armed, detail the itinerary, and include that the officer has completed the mandatory TSA training for a law enforcement officer flying while armed.
- (e) Officers must have completed the mandated TSA security training covering officers flying while armed. The training shall be given by the department-appointed instructor.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Firearms

- (f) It is the officer's responsibility to notify the air carrier in advance of the intended armed travel. This notification should be accomplished by early check-in at the carrier's check-in counter.
- (g) Any officer flying while armed should discreetly contact the flight crew prior to take-off and notify them of the officer's assigned seat.
- (h) Discretion must be used to avoid alarming passengers or crew by displaying a firearm. The officer must keep the firearm concealed on the officer's person at all times. Firearms are not permitted in carry-on luggage and may not be stored in an overhead compartment.
- (i) Officers should resolve any problems associated with flying armed through the flight captain, ground security manager, TSA representative, or other management representative of the air carrier.
- (j) Officers shall not consume alcoholic beverages while aboard an aircraft, or within eight hours prior to boarding an aircraft.

305.10 CARRYING FIREARMS OUT OF STATE

Qualified, active, full-time officers of this department are authorized to carry a concealed firearm in all other states subject to the following conditions (18 USC § 926B):

- (a) The officer shall carry the officer's South Saint Paul Police Department identification card whenever carrying such firearm.
- (b) The officer may not be the subject of any current disciplinary action.
- (c) The officer may not be under the influence of alcohol or any other intoxicating or hallucinatory drug.
- (d) The officer will remain subject to this and all other department policies (including qualifying and training).

Officers are cautioned that individual states may enact local regulations that permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property, or that prohibit or restrict the possession of firearms on any state or local government property, installation, building, base, or park. Federal authority may not shield an officer from arrest and prosecution in such locally restricted areas.

Active law enforcement officers from other states are subject to all requirements set forth in 18 USC § 926B.

Vehicle Pursuits

306.1 PURPOSE AND SCOPE

Vehicle pursuits expose innocent citizens, law enforcement officers and fleeing violators to the risk of serious injury or death. The primary purpose of this policy is to provide officers with guidance in balancing the safety of the public and themselves against law enforcement's duty to apprehend violators of the law. Another purpose of this policy is to minimize the potential for pursuit-related collisions. Vehicular pursuits require officers to exhibit a high degree of common sense and sound judgment. Officers must not forget that the immediate apprehension of a suspect is generally not more important than the safety of the public and pursuing officers (Minn. Stat. § 626.8458 Subd. 1).

306.1.1 PHILOSOPHY

Deciding whether to pursue a motor vehicle is a critical decision that must be made quickly and under difficult and unpredictable circumstances. In recognizing the risk to public safety created by vehicle pursuits, no officer or supervisor shall be criticized or disciplined for deciding not to engage in a vehicle pursuit due to the risk involved. This includes circumstances where Department policy would permit the initiation or continuation of the pursuit. It is recognized that vehicle pursuits are not always predictable and decisions made pursuant to this policy will be evaluated according to the totality of the circumstances reasonably available at the time of the pursuit (Minn. Stat. § 626.8458 Subd. 1).

Officers must remember that the most important factors to the successful conclusion of a pursuit are proper self-discipline and sound professional judgment. Officers conduct during the course of a pursuit must be objectively reasonable; that is, what a reasonable officer would do under the circumstances. An individual's unreasonable desire to apprehend a fleeing suspect at all costs has no place in professional law enforcement pursuit (Minn. Stat. § 626.8458 Subd. 2 (2)).

306.2 DEFINITIONS

Definitions related to this policy include:

Blocking or vehicle intercept/suppression - A slow-speed coordinated maneuver where two or more law enforcement vehicles simultaneously intercept and block the movement of a suspect vehicle, the driver of which may be unaware of the impending enforcement stop, with the goal of containment and preventing a pursuit. Blocking is not a moving or stationary road block.

Boxing-in - A tactic designed to stop a violator's vehicle by surrounding it with law enforcement vehicles and then slowing all vehicles to a stop.

Pursuit Intervention Technique (PIT) - A low-speed maneuver intended to terminate the pursuit by causing the violator's vehicle to spin out and come to a stop.

Ramming - The deliberate act of impacting a violator's vehicle with another vehicle to functionally damage or otherwise force the violator's vehicle to stop.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

Roadblocks - A tactic designed to stop a violator's vehicle by intentionally placing a vehicle or other immovable object in the path of the violator's vehicle.

Portable Tire Deflation Device - A device that extends across the roadway and is designed to puncture the tires of the pursued vehicle.

Vehicle pursuit - An event in which a peace officer attempts to apprehend a driver who ignores the signal to stop by increasing speed, extinguishing headlights or taillights, refusing to stop the vehicle, or using other means with intent to attempt to elude a peace officer (Minn. Stat. § 609.487).

306.3 OFFICER RESPONSIBILITIES

It is the policy of this department that a vehicle pursuit shall be conducted with at least one flashing red warning lamp visible from the front and a siren that is sounded when necessary to warn pedestrians or other drivers (Minn. Stat. § 169.17; Minn. Stat. § 169.68).

Operating an emergency vehicle in a pursuit with emergency lights and siren does not relieve the operator of an authorized emergency vehicle of the duty to drive with due regard for the safety of all persons, and does not protect the driver from the consequences of a reckless disregard for the safety of others (Minn. Stat. § 169.17).

306.3.1 WHEN TO INITIATE A PURSUIT

Officers are authorized to initiate a pursuit when it is reasonable to believe that a suspect is attempting to evade arrest or detention by fleeing in a vehicle that has been given a signal to stop by a peace officer.

The following factors individually and collectively shall be considered in deciding whether to initiate or continue a pursuit (Minn. Stat. § 626.8458 Subd. 2(2)):

- (a) Seriousness of the known or reasonably suspected crime and its relationship to community safety
- (b) The importance of protecting the public and balancing the known or reasonably suspected offense and the apparent need for immediate capture against the risks to officers, innocent motorists, and others
- (c) Apparent nature of the fleeing suspect (e.g., whether the suspect represents a serious threat to public safety)
- (d) The identity of the suspect has been verified and there is comparatively minimal risk in allowing the suspect to be apprehended at a later time
- (e) Safety of the public in the area of the pursuit, including the type of area, time of day, the amount of vehicular and pedestrian traffic (e.g., school zones), and the speed of the pursuit relative to these factors
- (f) The pursuing officer's familiarity with the area of the pursuit, the quality of radio communications between the pursuing units and the dispatcher/supervisor, and the driving capabilities of the pursuing officers under the conditions of the pursuit
- (g) Weather, traffic, and road conditions that unreasonably increase the danger of the pursuit when weighed against the risks resulting from the suspect's escape

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

- (h) Performance capabilities of the vehicles used in the pursuit in relation to the speeds and other conditions of the pursuit
- (i) Vehicle speeds
- (j) Other persons in or on the pursued vehicle (e.g., passengers, co-offenders, hostages)
- (k) Age of the suspect and occupants
- (l) Availability of other resources, such as aircraft assistance
- (m) The police unit is carrying passengers other than on-duty police officers. Pursuits should not be undertaken with a prisoner in the pursuit vehicle unless exigent circumstances exist, and then only after the need to apprehend the suspect is weighed against the safety of the prisoner in transport. A unit containing more than a single prisoner should not participate in a pursuit.

306.3.2 WHEN TO TERMINATE A PURSUIT

Pursuits should be discontinued whenever the totality of objective circumstances known or which reasonably ought to be known to the officer or supervisor during the pursuit indicates that the present risks of continuing the pursuit reasonably appear to outweigh the risks resulting from the suspect's escape.

The above factors on when to initiate a pursuit are expressly included herein and will apply equally to the decision to discontinue as well as the decision to initiate a pursuit. Officers and supervisors must objectively and continuously weigh the seriousness of the offense against the potential danger to innocent motorists, themselves, and the public when electing to continue a pursuit. In the context of this policy, the term "terminate" shall be construed to mean discontinue or to stop chasing the fleeing vehicle.

In addition to the factors listed above, the following factors should be considered when deciding whether to terminate a pursuit (Minn. Stat. § 626.8458 Subd. 2 (2)):

- (a) The distance between the pursuing officers and the fleeing vehicle is so great that further pursuit would be futile or require the pursuit to continue for an unreasonable time or distance.
- (b) The pursued vehicle's location is no longer definitely known.
- (c) The officer's pursuit vehicle sustains damage or a mechanical failure that renders it unsafe to drive.
- (d) The pursuit vehicle suffers an emergency equipment failure that causes the vehicle to no longer qualify for emergency operation use.
- (e) Extended pursuits of violators for misdemeanors not involving abuse or risk of serious harm (independent of the pursuit) are discouraged.
- (f) Hazards to uninvolved bystanders or motorists.
- (g) If the identity of the offender is known and it does not reasonably appear that the need for immediate capture outweighs the risks associated with continuing the pursuit,

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

officers should strongly consider discontinuing the pursuit and apprehending the offender at a later time.

- (h) When directed to terminate the pursuit by a supervisor.
- (i) When radio communications are broken or inadequate.
- (j) When the danger that the continued pursuit poses to the public, the officers, or the suspect is too great, balanced against the risk of allowing the suspect to remain at large.

306.3.3 SPEED LIMITS

The speed of a pursuit is a factor that should be evaluated on a continuing basis by the officer and supervisor. Evaluation of vehicle speeds shall take into consideration public safety, officer safety and the safety of the occupants of the fleeing vehicle.

Should high vehicle speeds be reached during a pursuit, officers and supervisors shall also consider these factors when determining the reasonableness of the speed of the pursuit:

- (a) Pursuit speeds have become unreasonably unsafe for the surrounding conditions.
- (b) Pursuit speeds have exceeded the driving ability of the officer.
- (c) Pursuit speeds are beyond the capabilities of the pursuit vehicle thus making its operation unsafe.

306.4 PURSUIT UNITS

Pursuit units should be limited to three vehicles (two units and a supervisor). However, the number of units involved will vary with the circumstances.

An officer or supervisor may request additional units to join a pursuit if, after assessing the factors outlined above, it appears that the number of officers involved would be insufficient to safely arrest the suspects. All other officers shall stay out of the pursuit but should remain alert to its progress and location. Any officer who drops out of a pursuit may then, if necessary, proceed to the termination point at legal speeds, following the appropriate rules of the road.

Distinctively marked patrol vehicles should replace unmarked vehicles involved in a pursuit whenever practicable.

306.4.1 MOTORCYCLE OFFICERS

A distinctively marked patrol vehicle equipped with emergency overhead lighting should replace a police motorcycle as primary and/or secondary pursuit unit as soon as practicable.

306.4.2 VEHICLES WITHOUT EMERGENCY EQUIPMENT

Vehicles not equipped with red light and siren are prohibited from initiating or joining in any pursuit. Officers in such vehicles may provide support to pursuing units as long as their vehicle is operated in compliance with all traffic laws.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

306.4.3 PRIMARY UNIT RESPONSIBILITIES

The initial pursuing officer will be designated as the primary pursuit unit and will be responsible for the conduct of the pursuit unless it is unable to remain reasonably close enough to the violator's vehicle. The primary responsibility of the officer initiating the pursuit is the apprehension of the suspects without unreasonable danger to the officer or other persons (Minn. Stat. § 626.8458 Subd. 2 (4)).

The primary unit should notify Dispatch, commencing with a request for priority radio traffic, that a vehicle pursuit has been initiated, and as soon as practicable provide information including but not limited to:

- (a) Reason for the pursuit.
- (b) Location and direction of travel.
- (c) Speed of the fleeing vehicle.
- (d) Description of the fleeing vehicle and license number, if known.
- (e) Number of occupants.
- (f) The identity or description of the known occupants.
- (g) Weather, road, and traffic conditions.
- (h) Identity of other agencies involved in the pursuit.
- (i) Information concerning the use of firearms, threat of force, injuries, hostages, or other unusual hazards.
- (j) Request for medical assistance for any person injured in the course of the pursuit (Minn. Stat. § 626.8458 Subd. 2 (6)).

Unless relieved by a supervisor or secondary unit, the officer in the primary unit shall be responsible for broadcasting the progress of the pursuit. Unless circumstances reasonably indicate otherwise, the primary unit should relinquish the responsibility of broadcasting the progress of the pursuit to a secondary unit or aircraft joining the pursuit to minimize distractions and allow the primary unit to concentrate foremost on safe pursuit tactics.

306.4.4 SECONDARY UNIT RESPONSIBILITIES

The second officer in the pursuit is responsible for the following:

- (a) Immediately notifying the dispatcher of entry into the pursuit
- (b) Remaining at a safe distance behind the primary unit unless directed to assume the role of primary officer, or if the primary unit is unable to continue the pursuit
- (c) Broadcasting the progress of the pursuit unless the situation indicates otherwise
- (d) Serve as backup to the primary unit once the subject has been stopped

306.4.5 PURSUIT DRIVING TACTICS

The decision to use or not use specific driving tactics requires the same assessment of considerations outlined in the factors to be considered concerning pursuit initiation and

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

termination. The following are tactics for units involved in the pursuit (Minn. Stat. § 626.8458 Subd. 2 (3)):

- (a) Officers, considering their driving skills and vehicle performance capabilities, will space themselves from other involved vehicles such that they are able to see and avoid hazards or react safely to maneuvers by the fleeing vehicle.
- (b) Officers may proceed past a red, or stop signal, or stop sign but only after slowing down and utilizing a flashing red lamp or siren as may be necessary for safe operation (Minn. Stat. § 169.03, Subd. 2).
- (c) As a general rule, officers should not pursue a vehicle driving the wrong way on a roadway, highway, or freeway (Minn. Stat. § 169.03). In the event the pursued vehicle does so, the following tactics should be considered:
 - 1. Request assistance from an available air unit.
 - 2. Maintain visual contact with the pursued vehicle by paralleling on the correct side of the roadway.
 - 3. Request other units to observe exits available to the suspects.
- (d) Notify the Minnesota State Patrol or other law enforcement agency if it appears the pursuit may enter their jurisdiction.
- (e) Officers involved in a pursuit should not attempt to pass other units unless the situation indicates otherwise or they are requested to do so by the primary unit, and a clear understanding of the maneuver process exists between the involved officers.

306.4.6 TACTICS/PROCEDURES FOR UNITS NOT INVOLVED IN THE PURSUIT

Officers are authorized to use emergency equipment at intersections along the pursuit path to clear intersections of vehicular and pedestrian traffic to protect the public. Officers should remain in their assigned area and should not become involved with the pursuit unless directed otherwise by a supervisor, if one is available.

The primary unit, secondary unit and supervisor should be the only units operating under emergency conditions (emergency lights and siren) unless other units are assigned to the pursuit.

306.4.7 PURSUIT TRAILING

In the event the initiating unit from this agency relinquishes control of the pursuit to another unit or jurisdiction, that initiating unit may, with permission of a supervisor, trail the pursuit to the termination point in order to provide necessary information and assistance for the arrest of the suspects.

The term "trail" means to follow the path of the pursuit at a safe speed while obeying all traffic laws and without activating emergency equipment. If the pursuit is at a slow rate of speed, the trailing unit will maintain sufficient distance from the pursuit units so as to clearly indicate an absence of participation in the pursuit.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

306.4.8 AIRCRAFT ASSISTANCE

When available, aircraft assistance should be requested. Once the air unit has established visual contact with the pursued vehicle, it should assume control over the pursuit. The primary and secondary ground units should consider whether the participation of an aircraft warrants their continued involvement in the pursuit (Minn. Stat. § 626.8458 Subd. 2 (4)).

The air unit should coordinate the activities of resources on the ground, report progress of the pursuit and provide officers and supervisors with details of upcoming traffic congestion, road hazards or other pertinent information to evaluate whether to continue the pursuit. If ground units are not within visual contact and the air unit determines that it is unsafe to continue the pursuit, the air unit should recommend terminating the pursuit.

306.5 SUPERVISORY CONTROL AND RESPONSIBILITIES

It is the policy of this department that available supervisory and management control will be exercised over all vehicle pursuits involving officers from this department (Minn. Stat. § 626.8458 Subd. 2 (4)).

The field supervisor of the officer initiating the pursuit, or if unavailable, the nearest field supervisor will be responsible for the following:

- (a) Upon becoming aware of a pursuit, immediately notify involved officers and Dispatch of supervisory presence and ascertain all reasonably available information to continuously assess the situation and risk factors associated with the pursuit in order to ensure that the pursuit is conducted within established department guidelines.
- (b) Engage in the pursuit, when appropriate, to provide on-scene supervision.
- (c) Exercise management and control of the pursuit even if not engaged in it.
- (d) Ensure that no more than the number of required law enforcement units needed are involved in the pursuit under the guidelines set forth in this policy.
- (e) Direct that the pursuit be terminated if, in the field supervisor's judgment, it is not justified to continue the pursuit under the guidelines of this policy.
- (f) Ensure that aircraft assistance is requested if available.
- (g) Ensure that the proper radio channel is being used.
- (h) Ensure the notification and/or coordination of outside agencies if the pursuit either leaves or is likely to leave the jurisdiction of this agency.
- (i) Control and manage SSP PD units when a pursuit enters another jurisdiction.
- (j) Prepare a post-pursuit critique and analysis of the pursuit for training purposes.

306.5.1 SERGEANT RESPONSIBILITIES

Upon becoming aware that a pursuit has been initiated, the Sergeant should monitor and continually assess the situation and ensure the pursuit is conducted within the guidelines and requirements of this policy. The Sergeant has the final responsibility for the coordination, control,

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

and termination of a vehicle pursuit and shall be in overall command (Minn. Stat. § 626.8458 Subd. 2 (4)).

The Sergeant shall review all pertinent reports for content and forward them to the Division Commander.

306.6 COMMUNICATIONS

If the pursuit is confined within the City limits, radio communications will be conducted on the primary channel unless instructed otherwise by a supervisor or communications dispatcher. If the pursuit leaves the jurisdiction of this department or such is imminent, involved units should, whenever available, switch radio communications to an emergency channel most accessible by participating agencies and units.

306.6.1 DISPATCH RESPONSIBILITIES

Upon notification that a pursuit has been initiated, Dispatch will be responsible for the following (Minn. Stat. § 626.8458 Subd. 2 (4)):

- (a) Coordinate pursuit communications of the involved units and personnel.
- (b) Notify and coordinate with other involved or affected agencies as practicable.
- (c) Ensure that a field supervisor is notified of the pursuit.
- (d) Assign an incident number and log all pursuit activities.
- (e) Broadcast pursuit updates as well as other pertinent information as necessary.
- (f) Notify the Sergeant as soon as practicable.

306.6.2 LOSS OF PURSUED VEHICLE

When the pursued vehicle is lost, the primary unit should broadcast pertinent information to assist other units in locating the vehicle. The primary unit will be responsible for coordinating any further search for either the pursued vehicle or suspects fleeing on foot.

306.7 INTER-JURISDICTIONAL CONSIDERATIONS

When a pursuit enters another agency's jurisdiction, the primary officer or supervisor, taking into consideration distance traveled, unfamiliarity with the area, and other pertinent facts, should determine whether to request the other agency to assume the pursuit. Unless entry into another jurisdiction is expected to be brief, it is generally recommended that the primary officer or supervisor ensure that notification is provided to the dispatcher and to each outside jurisdiction into which the pursuit is reasonably expected to enter, regardless of whether such jurisdiction is expected to assist (Minn. Stat. § 626.8458 Subd. 2 (5)).

If a pursuit from another agency enters the department's jurisdiction, Dispatch should update the on-duty supervisor.

306.7.1 ASSUMPTION OF PURSUIT BY ANOTHER AGENCY

South Saint Paul Police Department officers will discontinue the pursuit when another agency has assumed the pursuit unless continued assistance of the South Saint Paul Police Department is

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

requested by the agency assuming the pursuit. Upon discontinuing the pursuit, the primary unit may proceed upon request, with or at the direction of a supervisor, to the termination point to assist in the investigation.

The role and responsibilities of officers at the termination of a pursuit initiated by this department shall be coordinated with appropriate consideration of the units from the agency assuming the pursuit.

Notification of a pursuit in progress should not be construed as a request to join the pursuit. Requests to or from another agency to assume a pursuit should be specific. Because of communication limitations between local agencies, a request for another agency's assistance will mean that its personnel will assume responsibilities for the pursuit. For the same reasons, when a pursuit leaves another jurisdiction and a request for assistance is made to this department, the other agency should relinquish control.

306.7.2 PURSUITS EXTENDING INTO THIS JURISDICTION

The agency that initiates a pursuit shall be responsible for conducting the pursuit. Units from this department should not join a pursuit unless specifically requested to do so by the agency whose peace officers are in pursuit. The exception to this is when a single unit from the initiating agency is in pursuit. Under this circumstance, a unit from this department may join the pursuit until sufficient units from the initiating agency join the pursuit.

When a request is made for this department to assist or take over a pursuit from another agency that has entered this jurisdiction, the supervisor should consider these additional following factors:

- (a) Ability to maintain the pursuit.
- (b) Circumstances serious enough to continue the pursuit.
- (c) Adequate staffing to continue the pursuit.
- (d) The public's safety within this jurisdiction.
- (e) Safety of the pursuing officers.

As soon as practicable, a supervisor or the Sergeant should review a request for assistance from another agency. The Sergeant or supervisor, after consideration of the above factors, may decline to assist in or assume the other agency's pursuit.

Assistance to a pursuing outside agency by officers of this department will terminate at the City limits provided that the pursuing peace officers have sufficient assistance from other sources. Ongoing participation from this department may continue only until sufficient assistance is present.

In the event that a pursuit from another agency terminates within this jurisdiction, officers shall provide appropriate assistance to peace officers from the outside agency including, but not limited to, scene control, coordination and completion of supplemental reports and any other assistance requested or needed.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

306.8 PURSUIT INTERVENTION

Pursuit intervention is an attempt to terminate the ability of a suspect to continue to flee in a motor vehicle through tactical application of technology, portable tire deflation device, blocking, boxing, PIT (Pursuit Intervention Technique), vehicle suppression, ramming or roadblock procedures.

306.8.1 WHEN USE AUTHORIZED

Use of pursuit intervention tactics should be employed only after approval of a supervisor, if one is available. In deciding whether to use intervention tactics, officers/supervisors should balance the risks of allowing the pursuit to continue with the potential hazards arising from the use of each tactic to the public, the officers and persons in or on the pursued vehicle. With these risks in mind, the decision to use any intervention tactic should be reasonable in light of the circumstances apparent to the officer at the time of the decision (Minn. Stat. § 626.8458 Subd. 2).

It is imperative that officers act within legal bounds using good judgment and accepted practices.

306.8.2 USE OF FIREARMS

The use of firearms to disable a pursued vehicle is not generally an effective tactic and involves all the dangers associated with discharging firearms. Officers should not utilize firearms during an ongoing pursuit unless the conditions and circumstances meet the requirements authorizing the use of deadly force. Nothing in this section shall be construed to prohibit any officer from using a firearm to stop a suspect from using a vehicle as a deadly weapon.

306.8.3 INTERVENTION STANDARDS

Any pursuit intervention tactic, depending upon the conditions and circumstances under which it is used, may present dangers to the officers, the public or anyone in or on the vehicle being pursued. Certain applications of intervention tactics may be construed to be a use of force, including deadly force, and are subject to Department policies guiding such use. Officers who have not received Department-approved training in the application and use of any intervention tactic or equipment shall consider these facts and requirements prior to deciding how, when, where and if an intervention tactic should be employed.

- (a) Blocking or vehicle intercept/suppression should be considered in cases involving drivers who pose a threat to public safety when officers reasonably believe that attempting a conventional enforcement stop will likely result in the driver attempting to flee in the vehicle. Because of the potential risks involved, this technique should only be employed by officers after giving consideration to the following:
 - 1. The need to immediately stop the suspect vehicle or prevent it from leaving substantially outweighs the risks of injury or death to occupants of the suspect vehicle, officers or other members of the public.
 - 2. All other reasonable intervention techniques have failed or reasonably appear ineffective.
 - 3. Employing the blocking maneuver does not unreasonably increase the risk to officer safety.
 - 4. The target vehicle is stopped or traveling at a low speed.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

5. At no time should civilian vehicles be used to deploy this technique.
- (b) Only those officers trained in the use of the PIT will be authorized to use this procedure and only then with approval of a supervisor, if one is available, upon consideration of the circumstances and conditions presented at the time, including the potential for risk of injury to officers, the public and occupants of the pursued vehicle.
- (c) Ramming a fleeing vehicle should be done only after other reasonable tactical means at the officer's disposal have been exhausted. This tactic should be reserved for situations where there does not appear to be another reasonable alternative method. This policy is an administrative guide to direct officers in their decision-making process before ramming another vehicle. When ramming is used as a means to stop a fleeing vehicle, the following factors should be present:
 1. The suspect is an actual or suspected felon, who reasonably appears to represent a serious threat to the public if not apprehended.
 2. The suspect is driving with willful or wanton disregard for the safety of other persons or is driving in a reckless and life-endangering manner.
 3. If there does not reasonably appear to be a present or immediately foreseeable serious threat to the public, the use of ramming is not authorized.
- (d) As with all intervention techniques, pursuing officers should obtain supervisor approval, if one is available, before attempting to box a suspect vehicle during a pursuit. The use of such a technique must be carefully coordinated with all involved units, taking into consideration the circumstances and conditions apparent at the time, as well as the potential risk of injury to officers, the public and occupants of the pursued vehicle.
- (e) Portable tire deflation device should be deployed only when it is reasonably apparent that only the pursued vehicle will be affected by their use. Prior to the deployment of spike strips, the officer shall notify pursuing units and the supervisor of the intent and location. Officers should carefully consider the limitations of such devices as well as the potential risks to officers, the public and occupants of the pursued vehicle. If the pursued vehicle is a motorcycle, a vehicle transporting hazardous materials or a school bus transporting children officers and supervisors should weigh the potential consequences against the need to immediately stop the vehicle.
- (f) Because roadblocks involve a potential for serious injury or death to occupants of the pursued vehicle if the suspect does not stop, the intentional placement of roadblocks in the direct path of a pursued vehicle is generally discouraged and should not be deployed without prior approval of a supervisor, and only then under extraordinary conditions when all other reasonable intervention techniques have failed or reasonably appear ineffective and the need to immediately stop the pursued vehicle substantially outweighs the risks of injury or death to occupants of the pursued vehicle, officers or other members of the public.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

306.8.4 CAPTURE OF SUSPECTS

Proper self-discipline and sound professional judgment are the keys to a successful conclusion of a pursuit and apprehension of evading suspects. Officers shall use only that amount of force that reasonably appears necessary under the circumstances to properly perform their lawful duties.

Unless relieved by a supervisor, the primary officer should coordinate efforts to apprehend the suspect(s) following the pursuit. Officers should consider safety of the public and the involved officers when formulating plans to contain and capture the suspect.

306.8.5 VEHICLE SUPPRESSION

Active members of South Metro SWAT, while assigned to a SWAT operation, are authorized to use a SWAT vehicle, as well as agency vehicle, to conduct a vehicle suppression as described in the South Metro SWAT Operations Manual.

Active members of the Dakota County Drug Task Force while assigned to a Task Force operation, are authorized to conduct a vehicle suppression under the supervision of the Task Force.

306.9 REPORTING AND REVIEW REQUIREMENTS

All appropriate reports shall be completed to comply with appropriate local and state regulations. The Records Supervisor shall ensure the appropriate forms are filed with the Department of Public Safety within 30 days (Minn. Stat. § 626.5532):

- (a) The primary officer shall complete appropriate crime/arrest reports.
- (b) The primary officer or supervisor shall complete the appropriate pursuit report.
- (c) After first obtaining available information, the on-duty field supervisor shall promptly complete a Supervisor's Log or interoffice memorandum, briefly summarizing the pursuit to the Chief of Police or designee. This memo should minimally contain the following information (Minn. Stat. § 626.5532):
 - 1. Date and time of pursuit.
 - 2. Length of pursuit in distance and time.
 - 3. Involved units and officers.
 - 4. Initial reason and circumstances surrounding the pursuit.
 - 5. Starting and termination points.
 - 6. Alleged offense, charges filed or disposition: arrest, citation or other release.
 - 7. Arrestee information should be provided if applicable.
 - 8. Injuries and/or property damage.
 - 9. Medical treatment.
 - 10. The outcome of the pursuit.
 - 11. Name of supervisor handling or at the scene.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Pursuits

12. A preliminary determination that the pursuit appears to be in compliance with this policy or additional review and/or follow-up is warranted.
- (d) After receiving copies of reports, logs and other pertinent information, the Chief of Police or designee shall conduct or assign the completion of a post-pursuit review as appropriate to the circumstances.
- (e) Annually, the Chief of Police should direct a documented review and analysis of Department vehicle pursuits to minimally include policy suitability, policy compliance and training needs.

306.9.1 REGULAR AND PERIODIC PURSUIT TRAINING

In addition to initial and supplementary training on pursuits, all licensed non-exempt employees will participate, no less than annually, in regular and periodic training on this policy and the importance of vehicle safety and protecting the public at all times. Training will include a recognition of the need to balance the known offense and the need for immediate capture against the risks to officers and others.

The Support Services Commander shall ensure the frequency and content of emergency vehicle operations and vehicle pursuit training meets or exceeds that required by law (Minn. Stat. § 626.8458 Subd. 5).

306.9.2 POLICY REVIEW

Each licensed member of this department shall certify in writing that they have received, read and understand this policy initially and upon any amendments.

306.9.3 YEARLY CERTIFICATION

This policy shall be reviewed and certified to the state annually that it complies with requirements of any new or revised model policy adopted by the state (Minn. Stat. § 626.8458 Subd. 3).

306.9.4 PUBLIC DISCLOSURE

Copies of the current pursuit policy shall be made available to the public on request.

Officer Response to Calls

307.1 PURPOSE AND SCOPE

The State of Minnesota finds that emergency vehicle operations are an integral part of law enforcement's commitment to public safety. This policy provides for the safe and appropriate response to all emergency and nonemergency situations (Minn. Stat. § 626.8458, Subd. 1).

307.2 RESPONSE TO CALLS

307.2.1 RESPONSE TO EMERGENCY CALLS

Officers responding to an emergency call shall proceed immediately as appropriate. Officers responding to an emergency call shall sound the siren or display at least one lighted red light to the front of the vehicle. Whenever practicable, during an emergency call response the officer should continuously operate emergency lighting equipment and sound the siren (Minn. Stat. § 169.03 et seq.; Minn. Stat. § 169.17).

Responding with a red light, emergency lighting and/or siren does not relieve the operator of an authorized emergency vehicle or a law enforcement vehicle of the duty to drive with due regard for the safety of all persons and does not protect the driver from the consequences of his/her reckless disregard for the safety of others. The use of any other warning equipment without emergency lights and siren does not provide an exemption under Minnesota law (Minn. Stat. § 169.17).

Officers should only respond with a red light, emergency lights and/or siren when so dispatched or when circumstances reasonably indicate an emergency response is appropriate. Officers not responding with a red light, emergency lights and/or siren shall observe all traffic laws.

307.2.2 LIGHTING EXEMPTION OF LAW ENFORCEMENT VEHICLES

An officer may operate a vehicle without lights as otherwise required while performing law enforcement duties when the officer reasonably believes that operating the vehicle without lights is necessary to investigate a criminal violation or suspected criminal violation of state laws, rules or orders, or local laws, ordinances or regulations. The operation of a vehicle without lights must be consistent with the standards adopted by Minnesota Peace officer Standards and Training Board (POST) (Minn. Stat. § 169.541).

307.3 REQUESTING EMERGENCY ASSISTANCE

Requests for emergency assistance should be limited to those situations where the involved personnel reasonably believe that there is an imminent threat to the safety of officers, or assistance is needed to prevent imminent serious harm to a citizen. Where a situation has stabilized and emergency response is not required, the requesting officer shall promptly notify Dispatch.

If circumstances permit, the requesting officer should give the following information:

- The unit number
- The location

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer Response to Calls

- The reason for the request and type of emergency
- The number of units required

307.3.1 NUMBER OF UNITS PARTICIPATING

Normally, only those units reasonably necessary should respond to an emergency as an emergency call response. The Sergeant or the field supervisor should monitor all emergency responses and reduce or enhance the response as warranted.

307.4 EMERGENCY CALL RESPONSE

Emergency responses of more than one unit should include, if circumstances reasonably permit, coordination of the response of the second responding unit by Dispatch to avoid unanticipated intersecting of response routes.

The supervisor will make a determination regarding the appropriateness of the response of multiple officers and reduce or enhance the response as warranted.

307.5 RESPONSIBILITIES OF RESPONDING OFFICER(S)

Officers shall exercise sound judgment and care with due regard for life and property when responding to an emergency call. During a response to an emergency call officers may (Minn. Stat. § 169.03):

- (a) Proceed cautiously past a red or stop signal or stop sign but only after slowing down as may be necessary for safe operation.
- (b) Exceed any speed limits, provided this does not endanger life or property.
- (c) Disregard regulations governing direction of movement or turning in specified directions as authorized by law.
- (d) Disregard regulations governing parking or standing when using a warning lamp.

The decision to continue an emergency call response is at the discretion of the officer. If, in the officer's judgment, the roadway conditions or traffic congestion does not permit such a response without unreasonable risk, the officer may elect to respond to the call without the use of red lights and siren at the legal speed limit. In such an event, the officer should immediately notify other officers. An officer shall also discontinue an emergency call response when directed by a supervisor or as otherwise appropriate.

Upon determining that an emergency call response is appropriate, an officer shall immediately give the location from which he/she is responding.

When emergency vehicles are on the scene of an emergency and pose any hazard, or when the vehicle operators seek exemption to park, stop or stand contrary to any law or ordinance pursuant to Minn. Stat. § 169.541, adequate warning lights shall be operated whenever practicable.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Officer Response to Calls

307.6 SUPERVISORY RESPONSIBILITIES

Upon being notified that an emergency response has been initiated, the supervisor shall verify the following:

- (a) The proper response has been initiated.
- (b) No more than those units reasonably necessary under the circumstances are involved in the response.
- (c) Affected outside jurisdictions are being notified as practicable.

The supervisor shall, whenever practicable, monitor the response until it has been stabilized or terminated and assert control by directing units into or out of the response if necessary. If, in the supervisor's judgment, the circumstances require additional units to be assigned an emergency response, the supervisor may do so.

It is the supervisor's responsibility to terminate an emergency response that, in his/her judgment, is inappropriate due to the circumstances.

When making the decision to authorize an emergency call response, the supervisor should consider the following:

- The type of call or crime involved.
- The necessity of a timely response.
- Traffic and roadway conditions.
- The location of the responding units.

307.7 FAILURE OF EMERGENCY EQUIPMENT

If the emergency equipment on the vehicle should fail to operate, the officer must terminate the emergency call response and respond accordingly. The officer shall notify the supervisor of the equipment failure so that another unit may be assigned to the emergency response.

307.8 TRAINING

The Support Services Commander shall ensure the frequency and content of emergency vehicle operations training meets or exceeds that required by law (Minn. Stat. § 626.8458, Subd. 5; Minn. R. 6700.2702).

307.9 POLICY

It is the policy of this department to appropriately respond to emergency and nonemergency calls for service or requests for assistance, whether these are dispatched or self-initiated.

Canines

308.1 PURPOSE AND SCOPE

This policy establishes guidelines for the use of canines to augment law enforcement services in the community including, but not limited to locating individuals, contraband, apprehending criminal offenders and community outreach.

308.2 POLICY

It is the policy of the South Saint Paul Police Department that teams of handlers and canines meet and maintain the appropriate proficiency to effectively and reasonably carry out legitimate law enforcement objectives.

308.3 REQUESTS FOR CANINE TEAMS

Patrol Division members are encouraged to request the use of a canine.

308.3.1 OUTSIDE AGENCY REQUEST

All requests for canine assistance from outside agencies must be approved by the Sergeant and are subject to the following:

- (a) Canine teams shall not be used for any assignment that is not consistent with this policy.
- (b) The canine handler shall have the authority to decline a request for any specific assignment that he/she deems unsuitable.
- (c) Calling out off-duty canine teams is discouraged.
- (d) It shall be the responsibility of the canine handler to coordinate operations with agency personnel in order to minimize the risk of unintended injury.
- (e) It shall be the responsibility of the canine handler to complete all necessary reports or as directed.

308.3.2 PUBLIC DEMONSTRATIONS

All public requests for a canine team shall be reviewed by the canine handler prior to making any resource commitment. The canine handler is responsible for obtaining resources and coordinating involvement in the demonstration to include proper safety protocols. Canine handlers should exercise due care if demonstrating apprehension work.

308.4 APPREHENSION GUIDELINES

A canine may be used to locate and apprehend a suspect if the canine handler reasonably believes that the individual has committed, is committing, or is threatening to commit any serious offense and if any of the following conditions exist:

- (a) There is a reasonable belief the suspect poses an imminent threat of violence or serious harm to the public, any officer, or the handler.
- (b) The suspect is physically resisting or threatening to resist arrest and the use of a canine reasonably appears to be necessary to overcome such resistance.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Canines

- (c) The suspect is believed to be concealed in an area where entry by other than the canine would pose a threat to the safety of officers or the public.

It is recognized that situations may arise that do not fall within the provisions set forth in this policy. Such events require consideration of the totality of the circumstances and the use of an objective reasonableness standard applied to the decision to use a canine.

Absent a reasonable belief that a suspect has committed, is committing, or is threatening to commit a serious offense, mere flight from a pursuing officer without any of the above conditions, shall not serve as the basis for the use of a canine to apprehend a suspect.

Use of a canine to locate and apprehend a suspect wanted for a lesser criminal offense than those identified above requires approval from the Sergeant. Absent a change in circumstances that presents an imminent threat to officers, the canine, or the public, such canine use should be conducted on-leash or under conditions that minimize the likelihood the canine will bite or otherwise injure the individual.

In all applications, once the suspect has been located and no longer reasonably appears to present a threat or risk of escape, the handler should secure the canine as soon as it becomes reasonably practicable.

If the canine has apprehended the suspect with a secure bite, and the handler believes that the suspect no longer poses a threat, the handler should promptly command the canine to release the suspect.

308.4.1 PREPARATION FOR DEPLOYMENT

Prior to the use of a canine to search for or apprehend any suspect, the canine handler and/or the supervisor on-scene should carefully consider all pertinent information reasonably available at the time. The information should include but is not limited to:

- (a) The nature and seriousness of the suspected offense.
- (b) Whether violence or weapons were used or are anticipated.
- (c) The degree of resistance or threatened resistance, if any, the suspect has shown.
- (d) The suspect's known or perceived age.
- (e) The potential for injury to officers or the public caused by the suspect if the canine is not utilized.
- (f) Any potential danger to the public and/or other officers at the scene if the canine is released.
- (g) The potential for the suspect to escape or flee if the canine is not utilized.

As circumstances permit, the canine handler should make every reasonable effort to communicate and coordinate with other involved members to minimize the risk of unintended injury.

It is the canine handler's responsibility to evaluate each situation and determine whether the use of a canine is appropriate and reasonable. The canine handler shall have the authority to decline the use of the canine whenever he/she deems deployment is unsuitable.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Canines

A supervisor who is sufficiently apprised of the situation may prohibit deploying the canine.

Unless otherwise directed by a supervisor, assisting members should take direction from the handler in order to minimize interference with the canine.

308.4.2 WARNINGS AND ANNOUNCEMENTS

Unless it would increase the risk of injury or escape, a clearly audible warning announcing that a canine will be used if the suspect does not surrender should be made prior to releasing a canine. The handler should allow a reasonable time for a suspect to surrender and should quiet the canine momentarily to listen for any verbal response to the warning. If reasonably feasible, other members should be in a location opposite the warning to verify that the announcement could be heard. If available, warnings given in other languages should be used as necessary.

If a warning is not to be given, the canine handler, when reasonably practicable, should first advise the supervisor of his/her decision before releasing the canine. In the event of an apprehension, the handler shall document in any related report how the warning was given and, if none was given, the reasons why.

308.4.3 REPORTING DEPLOYMENTS, BITES, AND INJURIES

Handlers should document canine deployments in a canine use report. Whenever a canine deployment results in a bite or causes injury to an intended suspect, a supervisor should be promptly notified and the injuries documented in the canine use report. The injured person shall be promptly treated by Emergency Medical Services personnel and, if appropriate, transported to an appropriate medical facility for further treatment. The deployment and injuries should also be included in any related incident or arrest report.

Any unintended bite or injury caused by a canine, whether on- or off-duty, shall be promptly reported to the canine coordinator. Unintended bites or injuries caused by a canine should be documented in an administrative report, not in a canine use report.

If an individual alleges an injury, either visible or not visible, a supervisor shall be notified and both the individual's injured and uninjured areas shall be photographed as soon as reasonably practicable after first tending to the immediate needs of the injured party. Photographs shall be retained as evidence in accordance with current department evidence procedures. The photographs shall be retained until the criminal proceeding is completed and the time for any related civil proceeding has expired.

Canines used by law enforcement agencies are generally exempt from dangerous dog registration, impoundment, and reporting requirements (Minn. Stat. § 347.51, Subd. 4).

308.5 NON-APPREHENSION GUIDELINES

Properly trained canines may be used to track or search for non-criminals (e.g., lost children, individuals who may be disoriented or in need of medical attention). The canine handler is responsible for determining the canine's suitability for such assignments based on the conditions

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Canines

and the particular abilities of the canine. When the canine is deployed in a search or other non-apprehension operation the following guidelines apply.

- (a) Absent a change in circumstances that present an imminent threat to officers, the canine or the public, such applications should be conducted on-leash or under conditions that minimize the likelihood the canine will bite or otherwise injure the individual, if located.
- (b) Unless otherwise directed by a supervisor, assisting members should take direction from the handler in order to minimize interference with the canine.
- (c) Throughout the deployment, the handler should periodically give verbal assurances that the canine will not bite or hurt the individual and encourage the individual to make him/herself known.
- (d) Once the individual has been located, the handler should place the canine in a down-stay or otherwise secure it as soon as reasonably practicable.

308.5.1 ARTICLE DETECTION

A canine trained to find objects or property related to a person or crime may be used to locate or identify articles. A canine search should be conducted in a manner that minimizes the likelihood of unintended bites or injuries.

308.5.2 NARCOTICS DETECTION

A canine trained in narcotics detection may be used in accordance with current law and under certain circumstances, including:

- (a) The search of vehicles, buildings, bags, and other articles.
- (b) Assisting in the search for narcotics during a search warrant service.
- (c) Obtaining a search warrant by using the narcotics-detection trained canine in support of probable cause.

A narcotics-detection trained canine will not be used to search a person for narcotics unless the canine is trained to passively indicate the presence of narcotics.

308.6 HANDLER SELECTION

The minimum qualifications for the assignment of canine handler include:

- (a) An officer who is currently off probation.
- (b) Residing in an adequately fenced single-family residence (minimum 5-foot-high fence with locking gates).
- (c) A garage that can be secured and can accommodate a canine vehicle.
- (d) Living within 30 minutes travel time from the South Saint Paul City limits.
- (e) Agreeing to be assigned to the position for a minimum of three years.

308.7 CANINE COORDINATOR

The Operations Lieutenant, or designee, will serve as the canine coordinator.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Canines

The responsibilities of the coordinator include, but are not limited to:

- (a) Reviewing all canine use reports to ensure compliance with policy and to identify training issues and other needs of the program.
- (b) Maintaining liaison with the vendor kennel.
- (c) Maintaining liaison with command staff and functional supervisors.
- (d) Maintaining liaison with other agency canine coordinators.
- (e) Recommending and overseeing the procurement of equipment and services for the teams of handlers and canines.
- (f) Scheduling canine-related activities.
- (g) Ensuring the canine teams are scheduled for regular training to maximize their capabilities.

308.8 HANDLER RESPONSIBILITIES

The canine handler shall ultimately be responsible for the health and welfare of the canine and shall ensure that the canine receives proper nutrition, grooming, training, medical care, affection and living conditions.

The canine handler will be responsible for the following:

- (a) Except as required during appropriate deployment, the handler shall not expose the canine to any foreseeable and unreasonable risk of harm.
- (b) The handler shall maintain all department equipment under his/her control in a clean and serviceable condition.
- (c) When a handler is off-duty for an extended number of days the assigned canine vehicle should be stored at the South Saint Paul Police Department facility.
- (d) Handlers shall permit the canine coordinator to conduct spontaneous on-site inspections of affected areas of their homes as well as their canine vehicles to verify that conditions and equipment conform to this policy.
- (e) Any changes in the living status of the handler that may affect the lodging or environment of the canine shall be reported to the canine coordinator as soon as possible.
- (f) When off-duty the canine shall be in a kennel provided by the City at the home of the handler. When a canine is kenneled at the handler's home the gate shall be secured with a lock. When off-duty the canine may be let out of the kennel while under the direct control of the handler.
- (g) The canine should be permitted to socialize in the home with the handler's family for short periods of time and under the direct supervision of the handler.
- (h) Under no circumstances will the canine be lodged at another location unless approved by the canine coordinator or Sergeant.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Canines

- (i) When off-duty the handler shall not involve the canine in any law enforcement activity or official conduct unless approved in advance by the canine coordinator or Sergeant.
- (j) Whenever a canine handler is off-duty for an extended number of days it may be necessary to temporarily relocate the canine. In those situations the handler shall give reasonable notice to the canine coordinator so that appropriate arrangements can be made.

308.8.1 CANINE IN PUBLIC AREAS

The canine should be kept on a leash when in areas that allow access to the public. Exceptions to this rule would include specific law enforcement operations for which the canine is trained.

- (a) A canine shall not be left unattended in any area to which the public may have access.
- (b) When the canine vehicle is left unattended, all windows and doors shall be secured in such a manner as to prevent unauthorized access to the canine. The handler shall also ensure that the unattended vehicle remains inhabitable for the canine.

308.9 CANINE INJURY AND MEDICAL CARE

In the event that a canine is injured, or there is an indication that the canine is not in good physical condition, the injury or condition will be reported to the canine coordinator or Sergeant as soon as practicable and appropriately documented.

All medical attention shall be rendered by the designated canine veterinarian, except during an emergency where treatment should be obtained from the nearest available veterinarian. All records of medical treatment shall be maintained in the handler's personnel file.

308.10 TRAINING

Before assignment in the field each canine team shall be trained and certified to meet current nationally recognized standards or other recognized and approved certification standards. Cross-trained canine teams or those canine teams trained exclusively for the detection of narcotics and/or explosives also shall be trained and certified to meet current nationally recognized standards or other recognized and approved certification standards established for their particular skills.

The canine coordinator shall be responsible for scheduling periodic training for all department members in order to familiarize them with how to conduct themselves in the presence of department canines.

All canine training should be conducted while on-duty unless otherwise approved by the canine coordinator or Sergeant.

308.10.1 CONTINUED TRAINING

Each canine team shall thereafter be recertified to a current nationally recognized standard or other recognized and approved certification standards on an annual basis. Additional training considerations are as follows:

- (a) Canine teams should receive training as defined in the current contract with the South Saint Paul Police Department canine training provider.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Canines

- (b) Canine handlers are encouraged to engage in additional training with approval of the canine coordinator.
- (c) To ensure that all training is consistent, no handler, trainer, or outside vendor is authorized to train to a standard that is not reviewed and approved by the Department.

308.10.2 FAILURE TO SUCCESSFULLY COMPLETE TRAINING

Any canine team failing to graduate or obtain certification shall not be deployed in the field for tasks the team is not certified to perform until graduation or certification is achieved. When reasonably practicable, pending successful certification, the canine handler shall be temporarily reassigned to regular patrol duties.

308.10.3 TRAINING RECORDS

All canine training records shall be maintained in the canine handler's and the canine's training file.

308.10.4 TRAINING AIDS

Training aids are required to effectively train and maintain the skills of canines. Officers possessing, using or transporting controlled substances or explosives for canine training purposes must comply with federal and state requirements. Alternatively, the South Saint Paul Police Department may work with outside trainers with the applicable licenses or permits.

308.10.5 CONTROLLED SUBSTANCE TRAINING AIDS

Officers acting in the performance of their official duties may possess or transfer controlled substances for the purpose of narcotics-detection canine training in compliance with federal laws and if they comply with applicable state requirements (21 USC § 823(g)).

The Chief of Police or the authorized designee may authorize a member to seek a court order to allow controlled substances seized by the South Saint Paul Police Department to be possessed by the member or a narcotics-detection canine trainer who is working under the direction of this department for training purposes, provided the controlled substances are no longer needed as criminal evidence.

As an alternative, the Chief of Police or the authorized designee may request narcotics training aids from the Drug Enforcement Administration (DEA).

These procedures are not required if the canine handler uses commercially available synthetic substances that are not controlled narcotics.

308.10.6 CONTROLLED SUBSTANCE PROCEDURES

Due to the responsibilities and liabilities involved with possessing readily usable amounts of controlled substances and the ever-present danger of the canine's accidental ingestion of these controlled substances, the following procedures shall be strictly followed:

- (a) All controlled substance training samples shall be weighed and tested prior to dispensing to the individual canine handler or trainer.
- (b) The weight and test results shall be recorded and maintained by this department.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Canines

- (c) Any person possessing controlled substance training samples pursuant to court order or DEA registration shall maintain custody and control of the controlled substances and shall keep records regarding any loss of, or damage to, those controlled substances.
- (d) All controlled substance training samples will be inspected, weighed, and tested quarterly. The results of the quarterly testing shall be recorded and maintained by the canine coordinator with a copy forwarded to the dispensing agency.
- (e) All controlled substance training samples will be stored in locked, airtight, and watertight cases at all times, except during training. The locked cases shall be secured in the trunk of the canine handler's assigned patrol vehicle during transport and stored in an appropriate locked container. There are no exceptions to this procedure.
- (f) The canine coordinator shall periodically inspect every controlled substance training sample for damage or tampering and take any appropriate action.
- (g) Any unusable controlled substance training samples shall be returned to the Evidence Room or to the dispensing agency.
- (h) All controlled substance training samples shall be returned to the dispensing agency upon the conclusion of the training or upon demand by the dispensing agency.

Domestic Abuse

309.1 PURPOSE AND SCOPE

The purpose of this policy is to provide the guidelines necessary to deter, prevent, and reduce domestic abuse through vigorous enforcement and to address domestic abuse as a serious crime against society. The policy specifically addresses the commitment of this department to take enforcement action when appropriate, to provide assistance to victims and to guide officers in the investigation of domestic abuse.

309.1.1 DEFINITIONS

Definitions related to this policy include:

Court order - All forms of orders related to domestic abuse, that have been issued by a court of this state or another, whether civil or criminal, regardless of whether service has been made.

Domestic abuse - Commission of any of the following if committed against a family or household member by another family or household member (Minn. Stat. § 518B.01, Subd. 2):

- (a) Actual or fear of imminent physical harm, bodily injury, or assault
- (b) Threats of violence with intent to terrorize as specified by Minn. Stat. § 609.713, Subd.1.
- (c) Criminal sexual conduct (Minn. Stat. § 609.342 to Minn. Stat. § 609.3451)
- (d) Interference with an emergency call as specified by Minn. Stat. § 609.78, Subd.2.

309.2 POLICY

The South Saint Paul Police Department's response to incidents of domestic abuse and violations of related court orders shall stress enforcement of the law to protect the victim and shall communicate the philosophy that domestic abuse is criminal behavior. It is also the policy of this department to facilitate victims' and offenders' access to appropriate civil remedies and community resources whenever feasible.

309.3 OFFICER SAFETY

The investigation of domestic abuse cases often places officers in emotionally charged and sometimes highly dangerous environments. No provision of this policy is intended to supersede the responsibility of all officers to exercise due caution and reasonable care in providing for the safety of any officers and parties involved.

309.4 INVESTIGATIONS

The following guidelines should be followed by officers when investigating domestic abuse cases:

- (a) Calls of reported, threatened, imminent, or ongoing domestic abuse and the violation of any court order are of extreme importance and should be considered among the highest response priorities. This includes incomplete 9-1-1 calls.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Domestic Abuse

- (b) When practicable, officers should obtain and document statements from the victim, the suspect and any witnesses, including children, in or around the household or location of occurrence.
- (c) Officers should list the full name and date of birth (and school if available) of each child who was present in the household at the time of the offense. The names of other children who may not have been in the house at that particular time should also be obtained for follow-up.
- (d) When practicable and legally permitted, video or audio record all significant statements and observations.
- (e) All injuries should be photographed, regardless of severity, taking care to preserve the victim's personal privacy. Where practicable, photographs should be taken by a person of the same sex. Victims whose injuries are not visible at the time of the incident should be asked to contact the Investigations in the event that the injuries later become visible.
- (f) Officers should request that the victim complete and sign an authorization for release of medical records related to the incident when applicable.
- (g) If the suspect is no longer at the scene, officers should make reasonable efforts to locate the suspect to further the investigation, provide the suspect with an opportunity to make a statement and make an arrest or seek an arrest warrant if appropriate.
- (h) Seize any firearms or other dangerous weapons in the home, if appropriate and legally permitted, for safekeeping or as evidence.
- (i) When completing an incident or arrest report for violation of a court order, officers should include specific information that establishes that the offender has been served, including the date the offender was served, the name of the agency that served the order and the provision of the order that the subject is alleged to have violated. When reasonably available, the arresting officer should attach a copy of the order to the incident or arrest report.
- (j) Officers should take appropriate enforcement action when there is probable cause to believe an offense has occurred. Factors that should not be used as sole justification for declining to take enforcement action include:
 - 1. Marital status of suspect and victim.
 - 2. Whether the suspect lives on the premises with the victim.
 - 3. Claims by the suspect that the victim provoked or perpetuated the violence.
 - 4. The potential financial or child custody consequences of arrest.
 - 5. The physical or emotional state of either party.
 - 6. Use of drugs or alcohol by either party.
 - 7. Denial that the abuse occurred where evidence indicates otherwise.
 - 8. A request by the victim not to arrest the suspect.
 - 9. Location of the incident (public/private).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Domestic Abuse

10. Speculation that the complainant may not follow through with the prosecution.
11. The racial, cultural, social, professional position or sexual orientation of the victim or suspect.

309.4.1 IF A SUSPECT IS ARRESTED

If a suspect is arrested, officers should:

- (a) Advise the victim that there is no guarantee the suspect will remain in custody.
- (b) Provide the victim's contact information to the jail staff to enable notification of the victim upon the suspect's release from jail (Minn. Stat. § 629.72 Subd. 6).
- (c) Advise the victim whether any type of court order will be in effect when the suspect is released from jail.

309.4.2 IF NO ARREST IS MADE

If no arrest is made, the officer should:

- (a) Advise the parties of any options, including but not limited to:
 1. Voluntary separation of the parties.
 2. Appropriate resource referrals (e.g., counselors, friends, relatives, shelter homes, victim witness unit).
- (b) Document the resolution in a report.

309.5 VICTIM ASSISTANCE

Because victims may be traumatized or confused, officers should be aware that a victim's behavior and actions may be affected.

- (a) Victims should be provided with the department's domestic abuse information handout, even if the incident may not rise to the level of a crime.
- (b) Victims should be alerted to any available victim advocates, shelters, and community resources.
- (c) When an involved person requests law enforcement assistance while removing essential items of personal property, officers should stand by for a reasonable amount of time.
- (d) If the victim has sustained injury or complains of pain, officers should seek medical assistance as soon as practicable.
- (e) Officers should ask the victim whether he/she has a safe place to stay and assist in arranging transportation to an alternate shelter if the victim expresses a concern for his/her safety or if the officer determines that a need exists.
- (f) Officers should make reasonable efforts to ensure that any children or dependent adults who are under the supervision of the suspect or victim are being properly cared for.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Domestic Abuse

- (g) If appropriate, officers should seek or assist the victim in obtaining an emergency order.

309.6 DISPATCH ASSISTANCE

All calls of domestic abuse, including incomplete 9-1-1 calls, should be dispatched as soon as practicable.

Dispatchers are not required to verify the validity of a court order before responding to a request for assistance. Officers should request that dispatchers check whether any of the involved persons are subject to the terms of a court order.

309.7 FOREIGN COURT ORDERS

Various types of orders may be issued in domestic abuse cases. Any foreign court order properly issued by a court of another state, Indian tribe or territory shall be enforced by officers as if it were the order of a court in this state. An order should be considered properly issued when it reasonably appears that the issuing court has jurisdiction over the parties and reasonable notice and opportunity to respond was given to the party against whom the order was issued (18 USC § 2265). An otherwise valid out-of-state court order shall be enforced, regardless of whether the order has been properly registered with this state.

309.7.1 CANADIAN ORDERS FOR PROTECTION

An order for protection issued by Canada or a Canadian province shall be enforced as if it were the order of a court in this state and afforded the same consideration as foreign court orders with respect to proper issuance and registration (Minn. Stat. § 518F.03).

309.8 VERIFICATION OF COURT ORDERS

Determining the validity of a court order, particularly an order from another jurisdiction, can be challenging. Therefore, in determining whether there is probable cause to make an arrest for a violation of any court order, officers should carefully review the actual order when available, and, where appropriate and practicable:

- (a) Ask the subject of the order about his/her notice or receipt of the order, his/her knowledge of its terms and efforts to respond to the order.
- (b) Check available records or databases that may show the status or conditions of the order.
- (c) Contact the issuing court to verify the validity of the order.
- (d) Contact a law enforcement official from the jurisdiction where the order was issued to verify information.

Officers should document in an appropriate report their efforts to verify the validity of an order, regardless of whether an arrest is made. Officers should contact a supervisor for clarification when needed.

309.9 LEGAL MANDATES AND RELEVANT LAWS

Minnesota law provides for the following:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Domestic Abuse

309.9.1 STANDARDS FOR ARRESTS

Officers investigating a domestic abuse report should consider the following:

- (a) An officer has the authority to arrest a person without a warrant, including at the person's residence, if the peace officer has probable cause to believe that the person has, within the preceding 72 hours, exclusive of the day probable cause was established, assaulted, threatened with a dangerous weapon, or placed in fear of immediate bodily harm any person covered by the "family or household member" definition, even if the assault did not rise to the level of a felony or did not take place in the presence of the peace officer (Minn. Stat. § 629.34; Minn. Stat. § 629.341).
- (b) Officers should generally not make dual arrests but may make an arrest of a primary aggressor. Where there are allegations that each party assaulted the other, the officer shall determine whether there is sufficient evidence to conclude that one of the parties was the primary aggressor based on the following criteria and the officer's judgment (Minn. Stat. § 629.342, Subd. 2):
 - 1. Comparative extent of any injuries inflicted
 - 2. Fear of physical injury because of past or present threats
 - 3. Actions taken in self-defense or to protect oneself
 - 4. History of domestic abuse perpetrated by one party against the other
 - 5. Existence or previous existence of an order for protection
- (c) An officer shall not issue a citation in lieu of arrest and detention to an individual charged with any of the following offenses (Minn. Stat. § 629.72):
 - 1. Stalking
 - 2. Domestic abuse
 - 3. Violation of an order for protection
 - 4. Violation of a domestic abuse no contact order
- (d) The Sergeant will determine whether a person arrested on a charge of stalking any person, domestic abuse, violation of an order for protection, violation of a domestic abuse no contact order, or violation of a court-ordered transfer of firearms will be held in custody or be issued a citation in lieu of continued detention and released after booking. The person shall be held in custody whenever the Sergeant determines that it reasonably appears the release of the person (Minn. Stat. § 629.72):
 - 1. Poses a threat to the alleged victim or another family or household member.
 - 2. Poses a threat to public safety.
 - 3. Involves a substantial likelihood that the arrested person will fail to appear at subsequent proceedings.
- (e) Officers shall arrest and take into custody, without a warrant, a person whom the peace officer has probable cause to believe has violated a court order issued pursuant to Minn. Stat. § 518B.01 or Minn. Stat. § 629.75. Such an arrest shall be made even if the violation of the order did not take place in the presence of the peace officer, if the

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Domestic Abuse

officer can verify the existence of the order. If the person is not released on citation in lieu of continuing detention, the person shall be held in custody for these violations for at least 36 hours unless released by a court (Minn. Stat. § 518B.01; Minn. Stat. § 629.75).

- (f) An arrest for a violation of an order of protection may be made regardless of whether the excluded party was invited back to the residence (Minn. Stat. § 518B.01, Subd. 18).
- (g) Following an arrest, an officer should contact the local domestic abuse program by phone as soon as possible and provide the name and address of the victim and a brief factual account of events associated with the action.
- (h) An officer shall arrest and take into custody a person whom the officer has probable cause to believe has violated a harassment restraining order, pursuant to Minn. Stat. § 609.748, if the officer can verify the existence of the order.
- (i) Officers are authorized to make an arrest without a warrant when there is probable cause to believe the person has violated the provisions of any other no contact or restraining order issued by a court, even if the offense did not rise to the level of a felony (Minn. Stat. § 629.34). While conducting a domestic abuse investigation officers shall attempt to verify whether there has been a court order issued.
- (j) Officers should consider whether other offenses have been committed that may not qualify as a domestic abuse including, but not limited to, burglary, felony assault, other threats of violence, kidnapping, false imprisonment, witness tampering, trespassing, criminal damage to property, disorderly conduct, or assault.

309.9.2 REPORTS AND RECORDS

- (a) Officers should include information related to the following in a report, as applicable (Minn. Stat. § 629.341):
 - 1. Names, addresses, and telephone numbers of all involved persons
 - 2. Condition of clothing
 - 3. Description of the scene, including any property damage
 - 4. Evidence of physical injury, including strangulation
 - 5. Presence of elderly victims or persons with disabilities
 - 6. Facts related to any person who may have been a primary aggressor
 - 7. Excited utterances of the victim and the suspect
 - 8. Demeanor of the victim and the suspect
 - 9. Medical records, including the victim's statements to paramedics, nurses, and doctors
 - 10. Detailed statements of interviews of witnesses, including children, who may have been present, noting any language barriers
 - 11. A detailed explanation of the reasons for the officer's decision not to arrest or seek an arrest warrant

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Domestic Abuse

12. Evidence of any prior domestic abuse or related convictions, including dates
 13. Any existing orders for protection, harassment restraining order, or no contact orders
 14. Identifying information of a specific court order violated, including county of origin, the file number, and the provision allegedly violated
- (b) Domestic abuse reports should be forwarded to the appropriate prosecutor for review and consideration of criminal charges, even when no arrest is made or warrant requested.
- (c) If a child was present at the scene of a domestic abuse incident or was the victim of domestic abuse, the officer should determine whether the child has been subjected to physical abuse, sexual abuse, or neglect, and comply with the mandatory reporting requirements of Minn. Stat. § 260E.06 et seq.
1. The officer shall also attempt to verify whether there has been an order for protection issued under Minn. Stat. § 260C.201 and take appropriate action.
- (d) Fees will not be charged for the release of reports related to domestic abuse, as directed in Minn. Stat. § 13.82.

309.9.3 SERVICE OF COURT ORDERS

Officers, when reasonably safe and in a position to do so, shall serve copies or short forms of court orders as directed in Minn. Stat. § 518B.01.

309.9.4 COURT-ORDERED FIREARM SURRENDERS

Although not always required, this department generally will accept firearms surrendered by a court order from an abusing party or defendant. A decision to refuse a surrendered firearm should be approved by a supervisor.

Firearms will normally be surrendered at the South Saint Paul Police Department; however, when encountering someone in the field who wishes to surrender a firearm, officers should make reasonable efforts to accommodate the request.

However, if at the time of conviction that the court further finds (by preponderance of the evidence) that the defendant poses an imminent risk of causing substantial bodily harm, the court SHALL order LE to take immediate possession of all firearms in defendant's possession

Surrendered firearms should be collected and submitted to the Evidence Room in accordance with the Property and Evidence Policy.

Search and Seizure

310.1 PURPOSE AND SCOPE

Both the federal and state Constitutions provide every individual with the right to be free from unreasonable searches and seizures. This policy provides general guidelines for South Saint Paul Police Department personnel to consider when dealing with search and seizure issues.

310.2 POLICY

It is the policy of the South Saint Paul Police Department to respect the fundamental privacy rights of individuals. Members of this department will conduct searches in strict observance of the constitutional rights of persons being searched. All seizures by this department will comply with relevant federal and state law governing the seizure of persons and property.

The Department will provide relevant and current training to officers as guidance for the application of current law, local community standards and prosecutorial considerations regarding specific search and seizure situations, as appropriate.

310.3 SEARCHES

The U.S. Constitution generally provides that a valid warrant is required in order for a search to be valid. There are, however, several exceptions that permit a warrantless search.

Examples of law enforcement activities that are exceptions to the general warrant requirement include, but are not limited to, searches pursuant to the following:

- Valid consent
- Incident to a lawful arrest
- Legitimate community caretaking interests
- Vehicle searches under certain circumstances
- Exigent circumstances

Certain other activities are recognized by federal and state courts and by certain statutes as legitimate law enforcement activities that also do not require a warrant. Such activities may include seizure and examination of abandoned property, and observations of activities and property located on open public areas.

Because case law regarding search and seizure is constantly changing and subject to interpretation by the courts, each member of this department is expected to act in each situation according to current training and his/her familiarity with clearly established rights as determined by case law.

Whenever practicable, officers are encouraged to contact a supervisor to resolve questions regarding search and seizure issues prior to electing a course of action.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Search and Seizure

310.4 SEARCH PROTOCOL

Although conditions will vary and officer safety and other exigencies must be considered in every search situation, the following guidelines should be followed whenever circumstances reasonably permit:

- (a) Members of this department will strive to conduct searches with dignity and courtesy.
- (b) Officers should explain to the person being searched the reason for the search and how the search will be conducted.
- (c) Searches should be carried out with due regard and respect for private property interests and in a manner that minimizes damage. Property should be left in a condition as close as reasonably possible to its pre-search condition.
- (d) In order to minimize the need for forcible entry, an attempt should be made to obtain keys, combinations or access codes when a search of locked property is anticipated.
- (e) When the person to be searched is of the opposite sex as the searching officer, a reasonable effort should be made to summon an officer of the same sex as the subject to conduct the search. When it is not practicable to summon an officer of the same sex as the subject, the following guidelines should be followed:
 1. Another officer or a supervisor should witness the search.
 2. The officer should not search areas of the body covered by tight-fitting clothing, sheer clothing or clothing that could not reasonably conceal a weapon.

310.5 DOCUMENTATION

Officers are responsible to document any search and to ensure that any required reports are sufficient including, at minimum, documentation of the following:

- Reason for the search
- Any efforts used to minimize the intrusiveness of any search (e.g., asking for consent or keys)
- What, if any, injuries or damage occurred
- All steps taken to secure property
- The results of the search, including a description of any property or contraband seized
- If the person searched is the opposite sex, any efforts to summon an officer of the same sex as the person being searched and the identification of any witness officer

Supervisors shall review reports to ensure the reports are accurate, that actions are properly documented and that current legal requirements and department policy have been met.

Temporary Custody of Juveniles

311.1 PURPOSE AND SCOPE

This policy provides guidelines consistent with the Juvenile Justice and Delinquency Prevention Act for juveniles taken into temporary custody by members of the South Saint Paul Police Department (34 USC § 11133; Minn. Stat. § 260B.176; Minn. Stat. § 260C.176).

This policy does not apply to secure detention facilities, shelter care facilities, or the juvenile portion of an adult facility authorized to hold juveniles, but rather applies to the temporary custody of a juvenile before a juvenile is released, delivered to a court, or delivered to any of these other facilities (Minn. Stat. § 260B.176, Subd. 3; Minn. Stat. § 260C.176, Subd. 3).

311.1.1 DEFINITIONS

Definitions related to this policy include:

Custodian or Guardian - A person who is under a legal obligation or who is in fact providing care and support for a minor (Minn. Stat. § 260B.007, Subd. 13; Minn. Stat. § 260C.007, Subd. 10).

Juvenile non-offender - An abused, neglected, dependent, or alien juvenile who may be legally held for his/her own safety or welfare. This includes those held as runaways (Minn. Stat. § 260C.175), truancy violators (Minn. Stat. § 260C.143), and juveniles 15 years old or younger in custody related to their engaging in prostitution or related activities (Minn. Stat. § 260B.007 Subd. 6(c)). This also includes any juvenile who may have initially been contacted for an offense that would not subject an adult to arrest (e.g., fine-only offense) but was taken into custody for his/her protection or for purposes of reuniting the juvenile with a parent, guardian, or other responsible person.

Juvenile offender - A juvenile 17 years of age or younger who is alleged to have committed an offense that would subject an adult to arrest (a non-status offense). It also includes possession of a handgun in violation of Minn. Stat. § 624.713 (28 CFR 31.303). This does not include a juvenile petty offender under Minn. Stat. § 260B.007.

Non-secure custody - When a juvenile is held in the presence of an officer or other custody employee at all times and is not placed in a locked room, cell, or behind any locked doors. Juveniles in non-secure custody may be handcuffed but not to a stationary or secure object. Personal supervision, through direct visual monitoring, and audio two-way communication is maintained. Monitoring through electronic devices, such as video, does not replace direct visual observation.

Secure custody - When a juvenile offender is held in a locked room, a set of rooms, or a cell. Secure custody also includes being physically secured to a stationary object.

Examples of secure custody include:

- (a) A juvenile left alone in an unlocked room within the secure perimeter of the adult temporary holding area.
- (b) A juvenile handcuffed to a rail.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

- (c) A juvenile placed in a room that contains doors with delayed egress devices that have a delay of more than 30 seconds.
- (d) A juvenile being processed in a secure booking area when a non-secure booking area is available.
- (e) A juvenile left alone in a secure booking area after being photographed and fingerprinted.
- (f) A juvenile placed in a cell within the adult temporary holding area whether or not the cell door is locked.
- (g) A juvenile placed in a room that is capable of being locked or contains a fixed object designed for cuffing or restricting movement.

Sight and sound separation - Located or arranged to prevent physical, visual, or auditory contact.

Status offender - A juvenile suspected of committing a criminal violation of the law that would not be a criminal violation but for the age of the offender. Examples may include underage possession of tobacco or curfew violation. A juvenile in custody on a court order or warrant based upon a status offense is also a status offender. Juvenile petty offenders taken into custody should be considered a status offender for purposes of this policy (Minn. Stat. § 260B.007; Minn. Stat. § 260B.143).

311.2 POLICY

The South Saint Paul Police Department is committed to releasing juveniles from temporary custody as soon as reasonably practicable and keeping juveniles safe while they are in temporary custody at the South Saint Paul Police Department. Juveniles should be held in temporary custody only for as long as reasonably necessary for processing, transfer, or release.

311.3 JUVENILES WHO SHOULD NOT BE HELD

Juveniles who exhibit any of the following conditions should not be held at the South Saint Paul Police Department:

- (a) Unconscious
- (b) Seriously injured
- (c) A known suicide risk or obviously severely emotionally disturbed
- (d) Significantly intoxicated
- (e) Extremely violent or continuously violent

Officers taking custody of a juvenile who exhibits any of the above conditions should take reasonable steps to provide medical attention or mental health assistance and notify a supervisor of the situation.

These juveniles should not be held at the South Saint Paul Police Department unless they have been evaluated by a qualified medical and/or mental health professional.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

If the officer taking custody of the juvenile believes the juvenile may be a suicide risk, the juvenile shall be under continuous direct supervision until evaluation, release, or a transfer is completed.

311.3.1 SUICIDE PREVENTION OF JUVENILES IN CUSTODY

The arresting officer should be alert to potential symptoms based upon exhibited behavior that may indicate the juvenile is a suicide risk. These symptoms may include depression, refusal to communicate, verbally threatening to kill him/herself, or any unusual behavior that may indicate the juvenile may harm him/herself while in custody.

311.4 CUSTODY OF JUVENILES

Officers should take custody of a juvenile and temporarily hold the juvenile at the South Saint Paul Police Department when there is no other lawful and practicable alternative to temporary custody. Refer to the Child Abuse Policy for additional information regarding detaining a juvenile that is suspected of being a victim.

No juvenile should be held in temporary custody at the South Saint Paul Police Department without authorization of the arresting officer's supervisor or the Sergeant.

Any juvenile taken into custody shall be released to the care of the juvenile's parent or other responsible adult, or transferred to a juvenile custody facility or to other authority as soon as practicable, and in no event shall a juvenile be held beyond six hours from the time of his/her entry into the South Saint Paul Police Department (34 USC § 11133).

311.4.1 CUSTODY OF JUVENILE NON-OFFENDERS

Non-offenders taken into protective custody in compliance with the Child Abuse Policy should generally not be held at the South Saint Paul Police Department. Custodial arrangements should be made for non-offenders as soon as reasonably possible (Minn. Stat. § 260B.175; Minn. Stat. § 260C.143; Minn. Stat. § 260C.176). Juvenile non-offenders may not be held in secure custody (34 USC § 11133).

Juveniles detained for truancy violations may be (Minn. Stat. § 260C.143):

- (a) Transported to the juvenile's home and released to a parent or guardian.
- (b) Transported to the juvenile's school of enrollment and delivered to the school superintendent or a teacher.
- (c) Transported to a child truancy center under Minn. Stat. § 260A.04, Subd. 3.

311.4.2 CUSTODY OF JUVENILE STATUS OFFENDERS

Status offenders should generally be released by citation or with a warning rather than taken into temporary custody. However officers may take custody of a status offender if requested to do so by a parent or legal guardian in order to facilitate reunification (e.g., transported home or to the station to await a parent). Juvenile status offenders may not be held in secure custody (34 USC § 11133).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

311.4.3 CUSTODY OF JUVENILE OFFENDERS

Juvenile offenders should be held in non-secure custody while at the South Saint Paul Police Department unless another form of custody is authorized by this policy or is necessary due to exigent circumstances.

Generally juvenile offenders may be taken into custody under the authority of Minn. Stat. § 260B.175 when a court order authorizes the custody, when the juvenile has committed an offense that would warrant the arrest of an adult, or when it is reasonably believed that the child has violated the terms of probation, parole, or other field supervision.

An officer who takes a juvenile offender of any age or gender into custody or could take the juvenile into custody under Minn. Stat. § 260B.175 is authorized to perform a protective pat-down search of the juvenile offender in order to protect the officer's safety (Minn. Stat. § 260B.175, Subd. 4).

The parent, guardian, or custodian of the juvenile shall be notified as soon as possible when a juvenile offender is taken into custody. Juvenile offenders shall be released to the custody of a parent, guardian, custodian, or other suitable person unless there is reason to believe that the juvenile would (Minn. Stat. § 260B.176):

- (a) Endanger themselves or others.
- (b) Not return for a court hearing.
- (c) Run away from or otherwise not remain in the care or control of their parent, guardian, or custodian.
- (d) Face immediate endangerment to the juvenile's health or welfare.

If a juvenile offender is not released to a parent, guardian, custodian, or other suitable person, the officer taking the juvenile offender into custody shall communicate with or deliver the juvenile to a secure detention facility to determine whether the juvenile should be released or detained. The officer shall also notify the court as soon as possible of the detention of the juvenile and the reasons for detention (Minn. Stat. § 260B.176).

311.4.4 SCHOOL NOTIFICATION

Minnesota law requires that the Chief of Police or the authorized designee notify the superintendent or chief administrative officer of a juvenile's school of an incident occurring within our jurisdiction if (Minn. Stat. § 260B.171, Subd. 5):

- (a) There is probable cause to believe a juvenile has committed an offense that would be a crime if committed as an adult, where the victim is a student or staff member and the notice is reasonably necessary for the protection of the victim.
- (b) There is probable cause to believe a juvenile has committed certain serious crimes regardless of whether the victim is a student or staff member.
- (c) The juvenile is taken into protective custody and methamphetamine manufacture or storage is involved (see the Child Abuse Policy for guidelines) (see also, Minn. Stat. § 260C.171)

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

However, the department is not required to notify the school if it is determined that notice would jeopardize an ongoing investigation.

311.5 ADVISEMENTS

When a juvenile is taken into custody on a warrant, the juvenile and his/her parent, guardian, or custodian, if present, shall immediately be informed of the existence of the warrant for immediate custody and, as soon as practicable, of the reasons why the juvenile is being taken into custody (Minnesota Rules of Juvenile Delinquency Procedure 4.03, Subd. 10).

If it is determined that a juvenile taken into custody is going to be placed into a secure detention facility or a shelter care facility, the officer shall advise both the juvenile and the juvenile's parent, guardian, or custodian as soon as possible (Minn. Stat. § 260B.176, Subd. 3; Minn. Stat. § 260C.176, Subd. 3):

- (a) Of the reasons for custody and the reasons for placement.
- (b) Of the location of the facility unless there is reason to believe that disclosure would place the juvenile's health and welfare in immediate endangerment. If so, the disclosure shall not be made (Minn. Stat. § 260B.176, Subd. 5).
- (c) That the juvenile's parent, guardian, or custodian and attorney or guardian ad litem may make an initial visit to the facility at any time. Subsequent visits may also be made on a reasonable basis.
- (d) That the juvenile may telephone parents and an attorney or guardian ad litem immediately after being admitted to the facility and thereafter on a reasonable basis.
- (e) That the juvenile may not be detained for acts under Minn. Stat. § 260B.007, Subd. 6 for longer than 36 hours excluding weekends and holidays unless a petition has been filed pursuant to Minn. Stat. § 260B.178.
- (f) That the juvenile may not be detained under Minn. Stat. § 260C.175, Subd. 1, clause (1) or (2), item (ii) longer than 72 hours at a shelter care facility excluding weekends and holidays unless a petition has been filed pursuant to Minn. Stat. § 260C.178.
- (g) That the juvenile may not be detained for acts under Minn. Stat. § 260B.007, Subd. 6 for longer than 24 hours in an adult jail or municipal lockup excluding weekends and holidays or longer than six hours if the adult jail or municipal lockup is a standard metropolitan statistical area, unless a petition has been filed pursuant to Minn. Stat. § 260B.178 and a motion made to refer the juvenile for adult prosecution.
- (h) Of the date, time, and place of the detention hearing, if this information is available.
- (i) That the juvenile and the juvenile's parent, guardian, or custodian have the right to be present and to be represented by counsel, at the detention hearing and that if they cannot afford counsel it will be appointed at public expense.

311.6 JUVENILE CUSTODY LOGS

Any time a juvenile is held in custody at the Department the custody shall be promptly and properly documented in the juvenile custody log, including:

- (a) Identifying information about the juvenile being held.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

- (b) Date and time of arrival and release from the South Saint Paul Police Department.
- (c) Sergeant notification and approval to temporarily hold the juvenile.
- (d) Any charges for which the juvenile is being held and classification of the juvenile as a juvenile offender, status offender, or non-offender.
- (e) Any changes in status.
- (f) Time of all welfare checks.
- (g) Any medical and other screening requested and completed.
- (h) Circumstances that justify any secure custody.
- (i) Any other information that may be required by other authorities, such as compliance inspectors or a local juvenile court authority.

The Sergeant shall initial the log to approve the custody, including any secure custody and shall also initial the log when the juvenile is released.

311.7 NO-CONTACT REQUIREMENTS

Sight and sound separation shall be maintained between all juveniles and adults while in custody at the Department (34 USC § 11133). There should also be sight and sound separation between non-offenders and juvenile or status offenders.

In situations where brief or accidental contact may occur (e.g., during the brief time a juvenile is being fingerprinted and/or photographed in booking), a member of the South Saint Paul Police Department shall maintain a constant, immediate presence with the juvenile or the adult to minimize any contact. If inadvertent or accidental contact does occur, reasonable efforts shall be taken to end the contact.

311.8 TEMPORARY CUSTODY REQUIREMENTS

Members and supervisors assigned to monitor or process any juvenile at the South Saint Paul Police Department shall ensure the following:

- (a) The Sergeant should be notified if it is anticipated that a juvenile may need to remain at the South Saint Paul Police Department more than four hours. This will enable the Sergeant to ensure no juvenile is held at the South Saint Paul Police Department more than six hours.
- (b) A staff member of the same sex shall supervise personal hygiene activities and care, such as changing clothing or using the restroom, without direct observation to allow for privacy.
- (c) Personal visual checks and significant incidents/activities shall be noted on the log.
- (d) There shall be no viewing devices, such as peep holes or mirrors, of which the juvenile is not aware. Therefore an employee should inform a juvenile under his/her care that the juvenile will be monitored at all times unless he/she is using the toilet. This does not apply to surreptitious and legally obtained recorded interrogations.
- (e) Juveniles shall have reasonable access to toilets and wash basins.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

- (f) Food should be provided if a juvenile has not eaten within the past four hours or is otherwise in need of nourishment, including any special diet required for the health of the juvenile.
- (g) Juveniles shall have reasonable access to a drinking fountain or water.
- (h) Juveniles shall have reasonable opportunities to stand and stretch, particularly if handcuffed or restrained in any way.
- (i) Juveniles should have privacy during family, guardian, and/or lawyer visits.
- (j) Juveniles should be permitted to remain in their personal clothing unless the clothing is taken as evidence or is otherwise unsuitable or inadequate for continued wear while in custody.
- (k) Blankets should be provided as reasonably necessary.
- (l) Adequate shelter, heat, light, and ventilation should be provided without compromising security or enabling escape.
- (m) Juveniles shall have adequate furnishings, including suitable chairs or benches.
- (n) Juveniles shall have the right to the same number of telephone calls as an adult in custody.
- (o) No discipline may be administered to any juvenile nor may juveniles be subjected to corporal or unusual punishment, humiliation, or mental abuse.

311.9 USE OF RESTRAINT DEVICES

Juvenile offenders may be handcuffed in accordance with the Handcuffing and Restraints Policy. A juvenile offender may be handcuffed at the South Saint Paul Police Department when the juvenile presents a heightened risk. However non-offenders and status offenders should not be handcuffed unless they are combative or threatening.

Restraints shall only be used after less restrictive measures have failed and with the approval of the Sergeant if available. Restraints shall only be used so long as it reasonably appears necessary for the juvenile's protection or the protection of others.

Juveniles in restraints shall be kept away from other unrestrained juveniles or monitored in such a way as to protect the juvenile from abuse.

311.10 PERSONAL PROPERTY

The officer taking custody of a juvenile offender or status offender at the South Saint Paul Police Department shall ensure a thorough search of the juvenile's property is made and all property is removed from the juvenile, especially those items that could compromise safety, such as pens, pencils, and belts.

The personal property of a juvenile should be placed in a property bag. The property should be inventoried in the juvenile's presence and sealed into the bag. The property should be kept in a monitored or secure location until the juvenile is released from the custody of the South Saint Paul Police Department.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

311.11 SECURE CUSTODY

Only juvenile offenders 14 years of age or older may be placed in secure custody (Minn. Stat. § 260B.181). Sergeant approval is required before placing a juvenile offender in secure custody.

Secure custody should only be used for juvenile offenders when there is a reasonable belief that the juvenile is a serious risk of harm to him/herself or others.

Members of this department should not use secure custody for convenience when non-secure custody is or later becomes a reasonable option.

When reasonably practicable, handcuffing one hand of a juvenile offender to a fixed object while otherwise maintaining the juvenile in non-secure custody should be considered as the method of secure custody rather than the use of a locked enclosure. An employee must be present at all times to ensure the juvenile's safety while secured to a stationary object.

Generally, juveniles should not be secured to a stationary object for more than 60 minutes. Supervisor approval is required to secure a juvenile to a stationary object for longer than 60 minutes and every 30 minutes thereafter. Supervisor approval should be documented.

311.11.1 LOCKED ENCLOSURES

A thorough inspection of the area shall be conducted before placing a juvenile into the enclosure. A second inspection shall be conducted after removing the juvenile. Any damage noted to the room should be photographed and documented in the crime report.

The following requirements shall apply to a juvenile offender who is held inside a locked enclosure:

- (a) The juvenile shall constantly be monitored by an audio/video system during the entire custody.
- (b) Juveniles shall have constant auditory access to department members.
- (c) Initial placement into and removal from a locked enclosure shall be logged.
- (d) Random personal visual checks of the juvenile by a staff member shall occur no less than every 15 minutes.
 - 1. All checks shall be logged.
 - 2. The check should involve questioning the juvenile as to his/her well-being (sleeping juveniles or apparently sleeping juveniles should be awakened).
 - 3. Requests or concerns of the juvenile should be logged.
- (e) Males and females shall not be placed in the same locked room.
- (f) Juvenile offenders should be separated according to severity of the crime (e.g., felony or misdemeanor).
- (g) Restrained juveniles shall not be mixed in a cell or room with unrestrained juveniles.

311.12 SUICIDE ATTEMPT, DEATH, OR SERIOUS INJURY OF A JUVENILE

The Sergeant will ensure procedures are in place to address the suicide attempt, death, or serious injury of any juvenile held at the South Saint Paul Police Department. The procedures will address:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Juveniles

- (a) Immediate notification of the on-duty supervisor, Chief of Police and Investigation Division Supervisor.
- (b) Notification of the parent, guardian, or person standing in loco parentis of the juvenile.
- (c) Notification of the appropriate prosecutor.
- (d) Notification of the City attorney.
- (e) Evidence preservation.

311.13 INTERVIEWING OR INTERROGATING JUVENILE SUSPECTS

No interview or interrogation of a juvenile should occur unless the juvenile has the apparent capacity to consent and does consent to an interview or interrogation. If feasible, an attempt should be made to contact the juvenile's legal guardian advising them of the potential interview.

311.14 RESTRICTION ON PHOTOGRAPHING

Photographing of juveniles taken into custody will only occur with the consent of the juvenile court, except when the photograph is taken related to a violation of driving while impaired or is taken pursuant to the laws of arrest (Minn. Stat. § 260B.171, Subd. 5; Minn. Stat. § 260B.175; Minn. Stat. § 169A.20).

Adult Abuse

312.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the investigation and reporting of suspected abuse of certain adults who may be more vulnerable than others. This policy also addresses mandatory notification for South Saint Paul Police Department members as required by law (Minn. Stat. § 626.557).

312.1.1 DEFINITIONS

Definitions related to this policy include (Minn. Stat. § 626.5572):

Adult abuse - Any offense or attempted offense involving violence or neglect of an adult victim when committed by a person responsible for the adult's care, or any other act that would mandate reporting or notification to a social service agency or law enforcement.

312.2 POLICY

The South Saint Paul Police Department will investigate all reported incidents of alleged adult abuse and ensure proper reporting and notification as required by law.

312.3 MANDATORY NOTIFICATION

Members of the South Saint Paul Police Department shall notify the entity responsible for receiving such reports when they have reason to believe that a vulnerable adult is being or has been maltreated, or has sustained a physical injury which is not reasonably explained. Members shall also report suspected negligent care by a service or health care provider that resulted in injury or harm requiring the care of a physician (Minn. Stat. § 626.557).

For purposes of notification, a vulnerable adult is a person age 18 or older who has physical, mental or emotional disabilities that make it difficult for the person to care for or to protect him/herself from maltreatment. It also refers to adults who reside at a facility, or receive care at a facility or through home care (Minn. Stat. § 626.5572).

Maltreatment includes abuse, neglect and financial exploitation. Abuse can be physical, emotional or sexual. Financial exploitation may include any instance where vulnerable adults' money, assets or property are not used for their benefit or are stolen or kept from them (see Minn. Stat. § 626.5572 for full definitions).

312.3.1 NOTIFICATION PROCEDURE

Notification should be made as soon as possible, but in all cases within 24 hours (Minn. Stat. § 626.557; Minn. Stat. § 626.5572). To the extent possible, the following should be included in the notification:

- (a) The identity of the vulnerable adult and any caregiver
- (b) The nature and extent of the suspected maltreatment
- (c) Any evidence of previous maltreatment

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Adult Abuse

- (d) The name and addresses of the person initiating the report or other witnesses
- (e) The time, date, and location of the incident
- (f) Any other information that might be helpful in investigating the suspected maltreatment

If notification of maltreatment is first made to the South Saint Paul Police Department, the member receiving the notification shall complete and forward the intake form to the entity responsible for receiving such reports.

312.4 QUALIFIED INVESTIGATORS

Qualified investigators should be available to investigate cases of adult abuse. These investigators should:

- (a) Conduct interviews in appropriate interview facilities.
- (b) Be familiar with forensic interview techniques specific to adult abuse investigations.
- (c) Present all cases of alleged adult abuse to the prosecutor for review.
- (d) Coordinate with other enforcement agencies, social service agencies and facility administrators as needed.
- (e) Provide referrals to therapy services, victim advocates, guardians and support for the victim and family as appropriate.
- (f) Participate in or coordinate with multidisciplinary investigative teams as applicable (Minn. Stat. § 626.5571).

312.5 INVESTIGATIONS AND REPORTING

All reported or suspected cases of adult abuse require investigation and a report, even if the allegations appear unfounded or unsubstantiated. Investigations should be initiated immediately or as soon as possible thereafter. (Minn. Stat. § 626.557).

Investigations and reports related to suspected cases of adult abuse should address, as applicable:

- (a) The overall basis for the contact. This should be done by the investigating officer in all circumstances where a suspected adult abuse victim is contacted.
- (b) Any relevant statements the victim may have made and to whom he/she made the statements.
- (c) If a person is taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.
- (d) Documentation of any visible injuries or any injuries identified by the victim. This should include photographs of such injuries, if practicable.
- (e) Whether the victim was transported for medical treatment or a medical examination.
- (f) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other potential victims or witnesses who may reside in the residence.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Adult Abuse

- (g) Identification of any prior related reports or allegations of abuse, including other jurisdictions, as reasonably known.
- (h) Previous addresses of the victim and suspect.
- (i) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim's environment.

Any unexplained death of an adult who was in the care of a guardian or caretaker should be considered as potential adult abuse and investigated similarly.

Assigned members shall initiate an investigation of vulnerable adult abuse as soon as possible, but in all cases within 24 hours when there is reason to believe a crime has been committed (Minn. Stat. § 626.557).

312.6 PROTECTIVE CUSTODY

Before taking an adult abuse victim into protective custody when facts indicate the adult may not be able to care for him/herself, the officer should make reasonable attempts to contact an appropriate protective services agency. Generally, removal of an adult abuse victim from his/her family, guardian or other responsible adult should be left to the welfare authorities when they are present or have become involved in an investigation.

Generally, members of this department should remove an adult abuse victim from his/her family or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the victim. Prior to taking an adult abuse victim into protective custody, the officer should take reasonable steps to deliver the adult to another qualified legal guardian, unless it reasonably appears that the release would endanger the victim or result in abduction. If this is not a reasonable option, the officer shall ensure that the adult is delivered to an appropriate protective services agency or medical facility.

Whenever practicable, the officer should inform a supervisor of the circumstances prior to taking an adult abuse victim into protective custody. If prior notification is not practicable, officers should contact a supervisor promptly after taking the adult into protective custody.

When adult abuse victims are under state control, have a state-appointed guardian or there are other legal holdings for guardianship, it may be necessary or reasonable to seek a court order on behalf of the adult victim to either remove the adult from a dangerous environment (protective custody) or restrain a person from contact with the adult.

312.7 INTERVIEWS

312.7.1 PRELIMINARY INTERVIEWS

Absent extenuating circumstances or impracticality, officers should audio record the preliminary interview with a suspected adult abuse victim. Officers should avoid multiple interviews with the victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating officers should defer interviews until a person who is specially trained in such interviews is available.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Adult Abuse

312.7.2 DETAINING VICTIMS FOR INTERVIEWS

An officer should not detain an adult involuntarily who is suspected of being a victim of abuse solely for the purpose of an interview or physical exam without his/her consent or the consent of a guardian unless one of the following applies:

- (a) Exigent circumstances exist, such as:
 - 1. A reasonable belief that medical issues of the adult need to be addressed immediately.
 - 2. A reasonable belief that the adult is or will be in danger of harm if the interview or physical exam is not immediately completed.
 - 3. The alleged offender is a family member or guardian and there is reason to believe the adult may be in continued danger.
- (b) A court order or warrant has been issued.

312.8 MEDICAL EXAMINATIONS

When an adult abuse investigation requires a medical examination, the investigating officer should obtain consent for such examination from the victim, guardian, agency or entity having legal custody of the adult. The officer should also arrange for the adult's transportation to the appropriate medical facility.

In cases where the alleged offender is a family member, guardian, agency or entity having legal custody and is refusing to give consent for the medical examination, officers should notify a supervisor before proceeding. If exigent circumstances do not exist or if state law does not provide for officers to take the adult for a medical examination, the supervisor should consider other government agencies or services that may obtain a court order for such an examination.

312.9 DRUG-ENDANGERED VICTIMS

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of an adult abuse victim who has been exposed to the manufacturing, trafficking or use of narcotics.

312.9.1 SUPERVISOR RESPONSIBILITIES

The Investigations supervisor should:

- (a) Work with professionals from the appropriate agencies, including the applicable adult protective services agency, other law enforcement agencies, medical service providers and local prosecutors, to develop community-specific procedures for responding to situations where there are adult abuse victims endangered by exposure to methamphetamine labs or the manufacture and trafficking of other drugs.
- (b) Activate any available interagency response when an officer notifies the Investigations supervisor that he/she has responded to a drug lab or other narcotics crime scene where an adult abuse victim is present or where evidence indicates that an adult abuse victim lives.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Adult Abuse

- (c) Develop a report format or checklist for use when officers respond to drug labs or other narcotics crime scenes. The checklist will help officers document the environmental, medical, social and other conditions that may affect the adult.

312.9.2 OFFICER RESPONSIBILITIES

Officers responding to a drug lab or other narcotics crime scene where an adult abuse victim is present or where there is evidence that an adult abuse victim lives should:

- (a) Document the environmental, medical, social and other conditions of the adult, using photography as appropriate and the checklist or form developed for this purpose.
- (b) Notify the Investigations supervisor so an interagency response can begin.

312.10 STATE MANDATES AND OTHER RELEVANT LAWS

Minnesota requires or permits the following:

312.10.1 RECORDS SECTION RESPONSIBILITIES

The Records Section is responsible for:

- (a) Providing a copy of the adult abuse report to the applicable entity in the county responsible for receiving such reports as required by law.
- (b) Retaining the original adult abuse report with the initial case file.

312.10.2 RELEASE OF REPORTS

Information related to incidents of adult abuse or suspected adult abuse shall be confidential and may only be disclosed pursuant to state law and the Records Maintenance and Release Policy (Minn. Stat. § 626.557).

312.11 TRAINING

The Department should provide training on best practices in adult abuse investigations to members tasked with investigating these cases. The training should include:

- (a) Participating in multidisciplinary investigations, as appropriate.
- (b) Conducting interviews.
- (c) Availability of therapy services for adults and families.
- (d) Availability of specialized forensic medical exams.
- (e) Cultural competence (including interpretive services) related to adult abuse investigations.
- (f) Availability of victim advocates or other support.

Discriminatory Harassment

313.1 PURPOSE AND SCOPE

This policy is intended to prevent department members from being subjected to discriminatory harassment, including sexual harassment and retaliation. Nothing in this policy is intended to create a legal or employment right or duty that is not created by law.

313.2 POLICY

The South Saint Paul Police Department is an equal opportunity employer and is committed to creating and maintaining a work environment that is free of all forms of discriminatory harassment, including sexual harassment and retaliation. The Department will not tolerate, discrimination against employees in hiring, promotion, discharge, compensation, fringe benefits, and other privileges of employment. The Department will take preventive and corrective action to address any behavior that violates this policy or the rights it is designed to protect.

The non-discrimination policies of the Department may be more comprehensive than state or federal law. Conduct that violates this policy may not violate state or federal law but still could subject a member to discipline.

313.3 DEFINITIONS

Definitions related to this policy include:

313.3.1 DISCRIMINATION

The Department prohibits all forms of discrimination, including any employment-related action by a member that adversely affects an applicant or member and is based on actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law.

Discriminatory harassment, including sexual harassment, is verbal or physical conduct that demeans or shows hostility or aversion toward an individual based upon that individual's protected class. It has the effect of interfering with an individual's work performance or creating a hostile or abusive work environment.

Conduct that may, under certain circumstances, constitute discriminatory harassment can include making derogatory comments; making crude and offensive statements or remarks; making slurs or off-color jokes; stereotyping; engaging in threatening acts; making indecent gestures, pictures, cartoons, posters, or material; making inappropriate physical contact; or using written material or department equipment and/or systems to transmit or receive offensive material, statements, or pictures. Such conduct is contrary to department policy and to a work environment that is free of discrimination.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Discriminatory Harassment

313.3.2 SEXUAL HARASSMENT

The Department prohibits all forms of discrimination and discriminatory harassment, including sexual harassment. It is unlawful to harass an applicant or a member because of that person's sex.

Sexual harassment includes but is not limited to unwelcome sexual advances, requests for sexual favors, or other verbal, visual, or physical conduct of a sexual nature when:

- (a) Submission to such conduct is made either explicitly or implicitly a term or condition of employment, position, or compensation.
- (b) Submission to, or rejection of, such conduct is used as the basis for any employment decisions affecting the member.
- (c) Such conduct has the purpose or effect of substantially interfering with a member's work performance or creating an intimidating, hostile, or offensive work environment.

313.3.3 ADDITIONAL CONSIDERATIONS

Discrimination and discriminatory harassment do not include actions that are in accordance with established rules, principles, or standards including:

- (a) Acts or omission of acts based solely upon bona fide occupational qualifications under the Equal Employment Opportunity Commission (EEOC) and the Minnesota Department of Human Rights.
- (b) Bona fide requests or demands by a supervisor that the member improve the member's work quality or output, that the member report to the job site on time, that the member comply with City or department rules or regulations, or any other appropriate work-related communication between supervisor and member.

313.3.4 RETALIATION

Retaliation is treating a person differently or engaging in acts of reprisal or intimidation against the person because the person has engaged in protected activity, filed a charge of discrimination, participated in an investigation, or opposed a discriminatory practice. Retaliation will not be tolerated.

313.4 RESPONSIBILITIES

This policy applies to all department personnel. All members shall follow the intent of these guidelines in a manner that reflects department policy, professional standards, and the best interest of the Department and its mission.

Members are encouraged to promptly report any discriminatory, retaliatory, or harassing conduct or known violations of this policy to a supervisor. Any member who is not comfortable with reporting violations of this policy to the member's immediate supervisor may bypass the chain of command and make the report to a higher-ranking supervisor or manager. Complaints may also be filed with the Chief of Police, the Director of Human Services, or the City Administrator.

Any member who believes, in good faith, that the member has been discriminated against, harassed, or subjected to retaliation, or who has observed harassment, discrimination, or

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Discriminatory Harassment

retaliation, is encouraged to promptly report such conduct in accordance with the procedures set forth in this policy.

Supervisors and managers receiving information regarding alleged violations of this policy shall determine if there is any basis for the allegation and shall proceed with resolution as stated below.

313.4.1 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors and managers shall include but are not limited to:

- (a) Continually monitoring the work environment and striving to ensure that it is free from all types of unlawful discrimination, including harassment or retaliation.
- (b) Taking prompt, appropriate action within their work units to avoid and minimize the incidence of any form of discrimination, harassment, or retaliation.
- (c) Ensuring that their subordinates understand their responsibilities under this policy.
- (d) Ensuring that members who make complaints or who oppose any unlawful employment practices are protected from retaliation and that such matters are kept confidential to the extent possible.
- (e) Making a timely determination regarding the substance of any allegation based upon all available facts.
- (f) Notifying the Chief of Police or the Director of Human Services in writing of the circumstances surrounding any reported allegations or observed acts of discrimination, harassment, or retaliation no later than the next business day.

313.4.2 SUPERVISOR'S ROLE

Supervisors and managers shall be aware of the following:

- (a) Behavior of supervisors and managers should represent the values of the Department and professional standards.
- (b) False or mistaken accusations of discrimination, harassment, or retaliation can have negative effects on the careers of innocent members.

Nothing in this section shall be construed to prevent supervisors or managers from discharging supervisory or management responsibilities, such as determining duty assignments, evaluating or counseling members, or issuing discipline in a manner that is consistent with established procedures.

313.5 INVESTIGATION OF COMPLAINTS

Various methods of resolution exist. During the pendency of any such investigation, the supervisor of the involved members should take prompt and reasonable steps to mitigate or eliminate any continuing abusive or hostile work environment. It is the policy of the Department that all complaints of discrimination, retaliation, or harassment shall be fully documented, and promptly and thoroughly investigated.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Discriminatory Harassment

313.5.1 SUPERVISOR RESOLUTION

Members who believe they are experiencing discrimination, harassment, or retaliation should be encouraged to inform the individual that the behavior is unwelcome, offensive, unprofessional, or inappropriate. However, if the member feels uncomfortable or threatened or has difficulty expressing the member's concern, or if this does not resolve the concern, assistance should be sought from a supervisor or manager who is a rank higher than the alleged transgressor.

313.5.2 FORMAL INVESTIGATION

If the complaint cannot be satisfactorily resolved through the process described above, a formal investigation will be conducted.

The person assigned to investigate the complaint will have full authority to investigate all aspects of the complaint. Investigative authority includes access to records and the cooperation of any members involved. No influence will be used to suppress any complaint and no member will be subject to retaliation or reprisal for filing a complaint, encouraging others to file a complaint, or for offering testimony or evidence in an investigation.

Formal investigation of the complaint will be confidential to the extent possible and will include but is not limited to details of the specific incident, frequency and dates of occurrences, and names of any witnesses. Witnesses will be advised regarding the prohibition against retaliation, and that a disciplinary process, up to and including termination, may result if retaliation occurs.

Members who believe they have been discriminated against, harassed, or retaliated against because of their protected status are encouraged to follow the chain of command but may also file a complaint directly with the Chief of Police, the Director of Human Services or the City Administrator.

313.5.3 ALTERNATIVE COMPLAINT PROCESS

No provision of this policy shall be construed to prevent any member from seeking legal redress outside the Department. Members who believe that they have been harassed, discriminated against, or retaliated against are entitled to bring complaints of employment discrimination to federal, state, and/or local agencies responsible for investigating such allegations. Specific time limitations apply to the filing of such charges. Members are advised that proceeding with complaints under the provisions of this policy does not in any way affect those filing requirements.

313.6 DOCUMENTATION OF COMPLAINTS

All complaints or allegations shall be thoroughly documented on the appropriate forms and in a manner designated by the Chief of Police. The outcome of all reports shall be:

- (a) Approved by the Chief of Police, the City Administrator, or the Director of Human Services, depending on the ranks of the involved parties.
- (b) Maintained in accordance with the established records retention schedule.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Discriminatory Harassment

313.6.1 NOTIFICATION OF DISPOSITION

The complainant and/or victim will be notified in writing of the disposition of the investigation and the actions taken to remedy or address the circumstances giving rise to the complaint.

313.7 TRAINING

All new members shall be provided with a copy of this policy as part of their orientation. The policy shall be reviewed with each new member. The member shall certify by signing the prescribed form that the member has been advised of this policy, is aware of and understands its contents, and agrees to abide by its provisions during the member's term with the Department.

All members shall receive annual training on the requirements of this policy and shall certify by signing the prescribed form that they have reviewed the policy, understand its contents, and agree that they will continue to abide by its provisions.

Child Abuse

314.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the investigation of suspected child abuse. This policy also addresses when South Saint Paul Police Department members are required to notify the county social services agency of suspected child abuse.

314.1.1 DEFINITIONS

Definitions related to this policy include:

Child - Unless otherwise specified by a cited statute, a child is any person under the age of 18 years.

Child abuse (also known as maltreatment of minors) - Any offense or attempted offense involving violence or neglect with a child victim when committed by a person responsible for the child's care or any other act that would mandate notification to a social service agency (Minn. Stat. § 260E.03; Minn. Stat. § 260E.06).

314.2 POLICY

The South Saint Paul Police Department will investigate all reported incidents of alleged criminal child abuse and ensure the county social services agency is notified as required by law.

314.3 MANDATORY NOTIFICATION

Members of the South Saint Paul Police Department shall notify the county social services agency when they have reason to believe any of the following may have occurred or when someone reports any of the following (Minn. Stat. § 260E.06):

- (a) A child is being neglected or has been neglected within the preceding three years.
- (b) A child is being physically abused or has been physically abused within the preceding three years by a person responsible for the child's care.
- (c) A child is being sexually abused, threatened with sexual abuse, or has been sexually abused within the preceding three years by a person responsible for the child's care, by a person who has a significant relationship to the child, or by a person in a position of authority.
- (d) A woman is pregnant and has used a controlled substance for a non-medical purpose during the pregnancy, including but not limited to tetrahydrocannabinol (marijuana), or has consumed alcoholic beverages during the pregnancy in any way that is habitual or excessive (Minn. Stat. § 260E.03, subd. 15; Minn. Stat. § 260E.31).

Notification is mandatory for any acts of neglect, physical abuse, and sexual abuse that constitute a crime, whether or not the suspect had any relationship to or responsibility for the child (Minn. Stat. § 260E.12).

For purposes of notification, physical abuse includes injuries, mental injuries, or injuries that cannot be reasonably explained (e.g., punching, kicking, burning). Sexual abuse includes criminal

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Child Abuse

sexual conduct and prostitution offenses. Neglect includes failure to supply a child with necessary clothing, shelter, or medical care. See Minn. Stat. § 260E.03 for full definitions of physical abuse, sexual abuse, and neglect.

314.3.1 NOTIFICATION PROCEDURE

Notification should occur as follows (Minn. Stat. § 260E.09):

- (a) The member tasked with the investigation shall call the county social services agency and report the alleged abuse as soon as possible but always within 24 hours. The time of the call and the name of the person should be documented.
- (b) Notification, when possible, should include:
 - 1. The child's current location and whether the child is in immediate danger.
 - 2. A description of when and where the incident occurred and what happened to the child.
 - 3. A description of the injuries or present condition of the child.
 - 4. The names and addresses of the child, parents, or caregivers.
 - 5. Whether there were any witnesses to the incident and their names.
 - 6. Any additional information about the child, family, or caregivers that may be helpful.
 - 7. Whether the incident occurred in a licensed facility or a school and what actions the facility employees may have taken.
 - 8. Whether there are immediate family, relative, or community resources that would offer protection or support to the child.
- (c) Forms that may be required by the county social services agency or other written notification shall be completed and faxed or delivered to the county social services agency as soon as possible but always within 72 hours, exclusive of weekends and holidays.
- (d) Approved investigation reports should be forwarded to the county social services agency as soon as practical.
- (e) When the child abuse occurred at a facility or by a person from a facility that requires a state license or a profession that requires a state license (e.g., foster homes, group homes, day care, educator), notification shall also be made to the agency responsible for licensing the facility or person (Minn. Stat. § 260E.11).

314.4 QUALIFIED INVESTIGATORS

Qualified investigators should be available for child abuse investigations. These investigators should:

- (a) Conduct interviews in child-appropriate interview facilities.
- (b) Be familiar with forensic interview techniques specific to child abuse investigations.
- (c) Present all cases of alleged child abuse to the prosecutor for review.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Child Abuse

- (d) Coordinate with other enforcement agencies, social service agencies, and school administrators as needed.
- (e) Provide referrals to therapy services, victim advocates, guardians, and support for the child and family as appropriate.
- (f) Participate in or coordinate with multidisciplinary investigative teams as applicable.

314.5 INVESTIGATIONS AND REPORTING

In all reported or suspected cases of child abuse, a report will be written. Officers shall write a report even if the allegations appear unfounded or unsubstantiated.

Investigations and reports related to suspected cases of child abuse should address, as applicable:

- (a) The overall basis for the contact. This should be done by the investigating officer in all circumstances where a suspected child abuse victim was contacted.
- (b) The exigent circumstances that existed if officers interviewed the child victim without the presence of a parent or guardian.
- (c) Any relevant statements the child may have made and to whom he/she made the statements.
- (d) If a child was taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.
- (e) Documentation of any visible injuries or any injuries identified by the child. This should include photographs of such injuries, if practicable.
- (f) Whether the child victim was transported for medical treatment or a medical examination.
- (g) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other children who may reside in the residence.
- (h) Identification of any prior related reports or allegations of child abuse, including other jurisdictions, as reasonably known.
- (i) Previous addresses of the victim and suspect.
- (j) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim's environment.

All cases of the unexplained death of a child should be investigated as thoroughly as if it had been a case of suspected child abuse (e.g., a sudden or unexplained death of an infant).

314.6 PROTECTIVE CUSTODY

Before taking any child into protective custody, the officer should make reasonable attempts to contact the county social services agency. Generally, removal of a child from his/her family,

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Child Abuse

guardian or other responsible adult should be left to the child welfare authorities when they are present or have become involved in an investigation.

Generally, members of this department should remove a child from his/her parent or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the child. Prior to taking a child into protective custody, the officer should take reasonable steps to deliver the child to another qualified parent or legal guardian, unless it reasonably appears that the release would endanger the child or result in abduction. If this is not a reasonable option, the officer shall ensure that the child is delivered to the county social services agency.

Whenever practicable, the officer should inform a supervisor of the circumstances prior to taking a child into protective custody. If prior notification is not practicable, officers should contact a supervisor promptly after taking a child into protective custody.

Children may only be removed from a parent or guardian in the following situations (Minn. Stat. § 260C.175):

- (a) When a court has issued an order for removal.
- (b) When a child is found in surroundings or conditions that pose an imminent threat to the child's health or welfare or that a peace officer reasonably believes pose an imminent threat to the child's health or welfare.
- (c) If an Indian child is a resident of a reservation or is domiciled on a reservation but temporarily located off the reservation, taking the child into custody under this clause shall be consistent with the Indian Child Welfare Act (25 USC § 1922).

314.6.1 NOTICE TO PARENT OR CUSTODIAN AND CHILD

Whenever an officer takes a child into protective custody, the officer shall notify the parent or custodian and the child (age 10 years or older) that they may request that the child be placed with a relative instead of in a shelter care facility. The officer also shall give the parent or custodian a list, published by the Minnesota Department of Human Services, of names, addresses, and telephone numbers of social services agencies that offer child welfare services. When placement with a relative is requested, the officer will coordinate with the responsible social services agency to ensure the child's safety and well-being in compliance with Minn. Stat. § 260C.181 (Minn. Stat. § 260C.175).

If the parent or custodian was not present when the child was removed from the residence, the list shall be left with an adult who is on the premises or left in a conspicuous place on the premises if no adult is present. If the officer has reason to believe the parent or custodian is not able to read and understand English, the officer must provide a list that is written in the language of the parent or custodian (Minn. Stat. § 260C.175; Minn. Stat. § 260C.181).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Child Abuse

314.6.2 SAFE PLACE FOR NEWBORNS

A person may leave an unharmed newborn less than seven days old with the staff of a hospital, urgent care facility or ambulance service without being subject to prosecution (Minn. Stat. § 609.3785). The responsible social service agency is charged with addressing these matters but may contact law enforcement if child abuse is suspected (Minn. Stat. § 145.902; Minn. Stat. § 609.3785).

314.7 INTERVIEWS

314.7.1 PRELIMINARY INTERVIEWS

Absent extenuating circumstances or impracticality, officers should record the preliminary interview with suspected child abuse victims. Officers should avoid multiple interviews with a child victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating officers should defer interviews until a person who is specially trained in such interviews is available. Generally, child victims should not be interviewed in the home or location where the alleged abuse occurred.

314.7.2 DETAINING ABUSE VICTIMS FOR INTERVIEW

An officer should not detain a child involuntarily who is suspected of being a victim of child abuse solely for the purpose of an interview or physical exam without the consent of a parent or guardian unless one of the following applies:

(a) Exigent circumstances exist, such as:

1. A reasonable belief that medical issues of the child need to be addressed immediately.
2. A reasonable belief that the child is or will be in danger of harm if the interview or physical exam is not immediately completed.
3. The alleged offender is the custodial parent or guardian and there is reason to believe the child may be in continued danger.

(b) A court order or warrant has been issued.

314.7.3 NOTIFICATION TO PARENTS

Generally, officers should cooperate with parents and guardians and seek consent prior to conducting interviews of children. However, when reasonably necessary, state law grants officers the authority to interview a child who is the alleged victim of abuse or neglect, and any other children who currently reside or have resided with the alleged victim, without parental consent (Minn. Stat. § 260E.22, Subd. 1).

The interview may take place at school or at any facility or other place where the alleged victim or other children might be found, or the child may be transported to, and the interview conducted at, a place that is appropriate for the interview and has been designated by the local welfare agency or law enforcement agency. When it is possible and substantial child endangerment or sexual

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Child Abuse

abuse is alleged, the interview may take place outside the presence of the alleged offender and prior to any interviews of the alleged offender (Minn. Stat. § 260E.22).

The officer shall notify the parent, legal custodian, or guardian that the interview occurred as soon as reasonably practicable after the interview, unless the juvenile court has determined that reasonable cause exists to withhold the information (Minn. Stat. § 260E.22).

314.7.4 INTERVIEWS AT SCHOOL

If officers assigned to investigate a report of maltreatment determine that an interview should take place on school property, written notification of the intent to interview the child on school property must be received by school officials prior to the interview. The notification shall include the name of the child to be interviewed, the purpose of the interview, and a reference to the statutory authority to conduct an interview on school property (Minn. Stat. § 260E.22, Subd. 7).

The investigating officer shall determine who may attend the interview, although school officials may set reasonable conditions as to the time, place, and manner of the interview (Minn. Stat. § 260E.22, Subd. 7).

314.7.5 DOCUMENTING AND RECORDING INTERVIEWS

Any statement made by an alleged child abuse victim during the course of a criminal investigation shall be documented. The documentation of the interview must contain, at a minimum (Minn. Stat. § 260E.23):

- (a) The date, time, place, and duration of the interview.
- (b) The identity of the persons present at the interview.
- (c) A summary of the information obtained during the interview if it was not audio recorded.

Members should follow the written guidelines of the county attorney's office regarding recording interviews of a child abuse victim.

314.8 MEDICAL EXAMINATIONS

If the child has been the victim of abuse that requires a medical examination, the investigating officer should obtain consent for such examination from the appropriate parent, guardian or agency having legal custody of the child. The officer should also arrange for the child's transportation to the appropriate medical facility.

In cases where the alleged offender is the custodial parent or guardian and is refusing consent for the medical examination, officers should notify a supervisor before proceeding. If exigent circumstances do not exist or if state law does not provide for officers to take the child for a medical examination, the notified supervisor should consider obtaining a court order for such an examination.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Child Abuse

314.9 DRUG-ENDANGERED CHILDREN

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of children exposed to the manufacturing, trafficking or use of narcotics.

314.9.1 SUPERVISOR RESPONSIBILITIES

The Investigations supervisor should:

- (a) Work with professionals from the appropriate agencies, including the county social services agency, other law enforcement agencies, medical service providers and local prosecutors to develop community specific procedures for responding to situations where there are children endangered by exposure to methamphetamine labs or the manufacture and trafficking of other drugs.
- (b) Activate any available interagency response when an officer notifies the Investigations supervisor that the officer has responded to a drug lab or other narcotics crime scene where a child is present or where evidence indicates that a child lives there.

314.9.2 OFFICER RESPONSIBILITIES

Officers responding to a drug lab or other narcotics crime scene where a child is present or where there is evidence that a child lives should:

- (a) Document the environmental, medical, social and other conditions of the child using photography as appropriate and the checklist or form developed for this purpose.
- (b) Notify the Investigations supervisor so an interagency response can begin.

314.9.3 SCHOOL NOTIFICATION

If a juvenile is taken into protective custody after being found in an area where methamphetamine was being manufactured or attempted to be manufactured, or where any chemical substances, paraphernalia or waste products related to methamphetamine are stored, the officer who took the juvenile into custody shall notify the chief administrative officer of the juvenile's school (Minn. Stat. § 260C.171, Subd. 6).

314.10 STATE MANDATES AND OTHER RELEVANT LAWS

Minnesota requires or permits the following:

314.10.1 RELEASE OF REPORTS

Information related to incidents of child abuse or suspected child abuse shall be confidential and may only be disclosed pursuant to state law and the Records Maintenance and Release Policy (Minn. Stat. § 260E.35).

314.10.2 MULTIDISCIPLINARY INVESTIGATIVE TEAMS

Child mortality review panels, local review teams, and the commissioner of children, youth, and families shall have access to not public data regarding the death or near death of a child. This

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Child Abuse

department shall cooperate fully with any such team and investigation (Minn. Stat. § 260E.39, Subd. 5).

314.10.3 COORDINATION WITH SOCIAL SERVICES

In every case of child abuse that would require notification to a local county social services agency, the investigating officer shall coordinate the planning and execution of the investigation and assessment efforts to avoid a duplication of fact-finding efforts and multiple interviews. The investigating officer shall prepare a report separate from the social services agency (Minn. Stat. § 260E.12; Minn. Stat. § 260E.14, Subd. 5).

Members may disclose the status of an individual as a predatory offender to a child protection worker who is conducting an investigation or a family assessment under Chapter 260E (Minn. Stat. § 243.166; Minn. Stat. § 260E.03).

314.10.4 NOTIFICATION PROCESS

The Patrol Supervisor is responsible for ensuring the mandatory notifications to the county social service agency are carried out. This should be achieved, in part, by establishing and reviewing related procedures and through ongoing training (Minn. Stat. § 260E.01 et seq.).

314.10.5 COURT-ORDERED FIREARM SURRENDERS

Although not required, this department generally will accept firearms surrendered by a court order from an abusing party or defendant. A decision to refuse a surrendered firearm should be approved by a supervisor.

Firearms will normally be surrendered at the South Saint Paul Police Department; however, when encountering someone in the field who wishes to surrender a firearm, officers should make reasonable efforts to accommodate the request.

Surrendered firearms should be collected and submitted to the Evidence Room in accordance with the Property and Evidence Policy.

314.11 TRAINING

The Training Unit should provide training on best practices in child abuse investigations to members tasked with investigating these cases. The training should include:

- (a) Participating in multidisciplinary investigations, as appropriate.
- (b) Conducting forensic interviews.
- (c) Availability of therapy services for children and families.
- (d) Availability of specialized forensic medical exams.
- (e) Cultural competence (including interpretive services) related to child abuse investigations.
- (f) Availability of victim advocate or guardian ad litem support.

Missing Persons

315.1 PURPOSE AND SCOPE

This policy provides guidance for handling missing person investigations.

315.1.1 DEFINITIONS

Definitions related to this policy include:

Endangered - A person the Department has confirmed is missing and there is sufficient evidence to indicate that the person is at risk of physical injury or death. Examples include (Minn. Stat. § 299C.52):

- (a) The person is missing because of a confirmed abduction or under circumstances that indicate the person's disappearance was not voluntary.
- (b) The person is missing under known dangerous circumstances.
- (c) The person is missing for more than 30 days.
- (d) The person is under the age of 21 and at least one other factor is applicable.
- (e) There is evidence that the person is in need of medical attention or prescription medication such that it will have a serious adverse effect on the person's health if the person does not receive the needed care or medication.
- (f) The person does not have a pattern of running away or disappearing.
- (g) The person is mentally impaired.
- (h) There is evidence that a non-custodial parent may have abducted the person.
- (i) The person has been the subject of past threats or acts of violence.
- (j) There is evidence that the person is lost in the wilderness, backcountry, or outdoors where survival is precarious and immediate and effective investigation and search-and-rescue efforts are critical.
- (k) Any other factor the Department deems to indicate the person may be at risk of physical injury or death, including a determination by another law enforcement agency that the person is missing and endangered.

Missing person - Any person who is reported missing to law enforcement when that person's location is unknown. This includes any person under the age of 18 or who is certified or known to be mentally incompetent (Minn. Stat. § 299C.52).

Missing person networks - Databases or computer networks that are available to law enforcement and are suitable for obtaining information related to missing person investigations. This includes the National Crime Information Center (NCIC), the National Missing and Unidentified Persons System (NamUs), the Minnesota Justice Information Services (MNJIS), the Minnesota Missing and Unidentified Persons Clearinghouse, and the Minnesota Crime Alert Network.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

315.2 POLICY

The South Saint Paul Police Department does not consider any report of a missing person to be routine and assumes that the missing person is in need of immediate assistance until an investigation reveals otherwise. Priority shall be given to missing person cases over property-related cases. Members will initiate an investigation into all reports of missing persons, regardless of the length of time the person has been missing.

315.3 REQUIRED FORMS AND BIOLOGICAL SAMPLE COLLECTION KITS

The Investigations supervisor shall ensure the following forms and kits are developed and available:

- Missing person report form
- Missing person investigation checklist that provides investigation guidelines and resources that could be helpful in the early hours of a missing person investigation
- Missing person school notification form
- Medical records release form
- Biological sample collection kits

315.4 ACCEPTANCE OF REPORTS

Any member encountering a person who wishes to report a missing person or runaway shall render assistance without delay. This can be accomplished by accepting the report via telephone or in person and initiating the investigation. Those members who do not take such reports or who are unable to give immediate assistance shall promptly dispatch or alert a member who can take the report.

A report shall be accepted in all cases and regardless of where the person was last seen, where the person resides or any question of jurisdiction (Minn. Stat. § 299C.53, Subd.1(a)).

315.5 INITIAL INVESTIGATION

Officers or other members conducting the initial investigation of a missing person should take the following investigative actions as applicable:

- (a) Respond to a dispatched call as soon as practicable. Obtain a detailed description of the missing person, as well as a description of any related vehicle and/or abductor.
- (b) Interview the reporting party and any witnesses to determine whether the person qualifies as a missing person and, if so, whether the person may be endangered (Minn. Stat. § 299C.53, Subd. 1(b)). Interviews should be conducted separately, if practicable.
- (c) Consult with the Bureau of Criminal Apprehension (BCA) if the person is determined to be an endangered missing person (Minn. Stat. § 299C.53, Subd. 1(b)).
- (d) Canvass the last known area where the missing person was seen, if known. A search of the location where the incident took place, if known, should also be conducted and a search warrant obtained if necessary.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

- (e) Determine when, where and by whom the missing person was last seen. Interview the person who last had contact with the missing person.
- (f) Notify a supervisor immediately if there is evidence that a missing person is either endangered or may qualify for a public alert, or both (see the Public Alerts Policy).
- (g) Broadcast an "Attempt to Locate" (ATL) or similar alert if the person is under 18 years of age or there is evidence that the missing person is endangered. The alert should be broadcast as soon as practicable but in no event more than one hour after determining the missing person is under 18 years of age or may be endangered.
- (h) Relay known details to all on-duty personnel as well as other local or surrounding law enforcement agencies using local and state databases.
- (i) Ensure that entries are made into the appropriate missing person networks:
 - 1. Immediately, when the missing person is endangered (Minn. Stat. § 299C.53, Subd. 1(b)).
 - 2. In all other cases, as soon as practicable, but not later than two hours from the time of the initial report (34 USC § 41308).
- (j) Complete the appropriate report forms accurately and completely and initiate a search as applicable according to the facts.
- (k) Collect and/or review:
 - 1. A photograph and fingerprint card of the missing person, if available (Minn. Stat. § 299C.54, Subd. 2).
 - 2. A voluntarily provided biological sample of the missing person, if available (e.g., toothbrush, hairbrush).
 - 3. Any documents that may assist in the investigation, such as court orders regarding custody.
 - 4. Any other evidence that may assist in the investigation, including personal electronic devices (e.g., cell phones, computers).
- (l) When circumstances permit and if appropriate, attempt to determine the missing person's location through their telecommunications carrier.
- (m) Contact the appropriate agency if the report relates to a missing person report previously made to another agency and that agency is actively investigating the report. When this is not practicable, the information should be documented in an appropriate report for transmission to the appropriate agency. If the information relates to an endangered missing person, the member should notify a supervisor and proceed with reasonable steps to locate the missing person.
- (n) Implement multi-jurisdictional coordination/mutual aid plan as appropriate such as when:
 - 1. The primary agency has limited resources.
 - 2. The investigation crosses jurisdictional lines.
 - 3. Jurisdictions have pre-established task forces or investigative teams.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

315.5.1 CRIME SCENE INVESTIGATION AND MANAGEMENT

If a crime scene is identified, it should be secured and a command post or operation base located at a reasonable distance from the crime scene. Staff and assign the responsibilities for command post supervisor, media specialist, search coordinator, investigative coordinator, communication officer and support unit coordinator. Provide two liaison officers (one at the command post and one at the crime scene). The role of the liaison at the home will include facilitating support and advocacy for the family.

The investigation of the scene and the crime should consider various elements, including:

- (a) Establishing the ability to “trap and trace” all incoming calls. Consider setting up a separate telephone line or cellular telephone for department use and follow-up on all leads.
- (b) Compiling a list of known sex offenders in the region.
- (c) In cases of infant abduction, investigating claims of home births made in the area.
- (d) In cases involving children, obtaining child protective agency records for reports of child abuse.
- (e) Reviewing records for previous incidents related to the missing person and prior law enforcement activity in the area, including prowlers, indecent exposure, attempted abductions, etc.
- (f) Obtaining the missing person's medical and dental records, fingerprints and a biological sample when practicable or within 30 days.
- (g) Creating a missing person profile with detailed information obtained from records and interviews with family and friends, describing the missing person's health, relationships, personality, problems, life experiences, plans, equipment, etc.
- (h) Interviewing delivery personnel, employees of gas, water, electric and cable companies, taxi drivers, post office personnel, sanitation workers, etc.
- (i) Determining if outside help is needed and the merits of utilizing local, state and federal resources related to specialized investigative needs, including:
 - 1. Investigative resources (e.g., search and rescue).
 - 2. Interpretive resources.
 - 3. Telephone services, such as traps, traces and triangulation.
 - 4. Media assistance from local and national sources.
- (j) Using secure electronic communication information, such as the missing person's cellular telephone number, e-mail address and information from social networking sites.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

- (k) Appointing an officer to communicate with the family/reporting party or their designee. The officer will be the primary point of contact for the family/reporting party or their designee, and should provide contact information and the family information packet (if available) to the family/reporting party or their designee.
- (l) Providing general information to the family/reporting party or their designee about the handling of the missing person case or about any intended efforts, only to the extent that disclosure would not adversely affect the department's ability to locate or protect the missing person or to apprehend or criminally prosecute any person in connection to the case.

315.6 REPORT PROCEDURES AND ROUTING

Members should complete all missing person reports and forms promptly and advise the appropriate supervisor as soon as a missing person report is ready for review.

315.6.1 SUPERVISOR RESPONSIBILITIES

The responsibilities of the supervisor shall include, but are not limited to:

- (a) Reviewing and approving missing person reports upon receipt.
 - 1. The reports should be promptly sent to the Records Section.
- (b) Ensuring resources are deployed as appropriate.
- (c) Initiating a command post as needed.
- (d) Ensuring applicable notifications and public alerts are made and documented.
- (e) Ensuring that records have been entered into the appropriate missing persons networks.
- (f) Taking reasonable steps to identify and address any jurisdictional issues to ensure cooperation among agencies.
 - 1. If the case falls within the jurisdiction of another agency, the supervisor should facilitate transfer of the case to the agency of jurisdiction.

315.6.2 RECORDS SECTION RESPONSIBILITIES

The responsibilities of the Records Section receiving member shall include, but are not limited to:

- (a) As soon as reasonable under the circumstances, notifying and forwarding a copy of the report to the agency of jurisdiction for the missing person's residence in cases where the missing person is a resident of another jurisdiction.
- (b) Notifying and forwarding a copy of the report to the agency of jurisdiction where the missing person was last seen.
- (c) Notifying and forwarding a copy of the report to the agency of jurisdiction for the missing person's intended or possible destination, if known.
- (d) Forwarding a copy of the report to the Investigations.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

- (e) Coordinating with the NCIC Terminal Contractor for Minnesota to have the missing person record in the NCIC computer networks updated with additional information obtained from missing person investigations (34 USC § 41308).

315.7 INVESTIGATIONS FOLLOW-UP

In addition to completing or continuing any actions listed above, the investigator assigned to a missing person investigation:

- (a) Should ensure that the missing person's school is notified within 10 days if the missing person is a juvenile.
 - 1. The notice shall be in writing and should also include a photograph.
 - 2. The investigator should meet with school officials as appropriate to stress the importance of including the notice in the child's student file, along with the investigator's contact information if the school receives a call requesting the transfer of the missing child's files to another school.
- (b) Should recontact the reporting party and/or other witnesses within 30 days of the initial report and within 30 days thereafter to keep them informed, as appropriate, and to determine if any additional information has become available.
- (c) Shall review the case file to determine whether any additional information received on the missing person indicates that the person is endangered, and shall update applicable state or federal databases accordingly (Minn. Stat. § 299C.535(b); Minn. Stat. § 299C.535(c)).
- (d) Shall attempt to obtain the following, if not previously obtained, if the person remains missing after 30 days (Minn. Stat. § 299C.535(a)):
 - 1. Biological samples from family members and, if possible, from the missing person
 - 2. Dental information and X-rays
 - 3. Additional photographs and video that may aid the investigation or identification
 - 4. Fingerprints
 - 5. Any other specific identifying information
- (e) Should consider contacting other agencies involved in the case to determine if any additional information is available.
- (f) Shall verify and update the Minnesota Justice Information Services (MNJIS), the Minnesota Missing and Unidentified Persons Clearinghouse, NCIC and any other applicable missing person networks within 30 days of the original entry into the networks and every 30 days thereafter until the missing person is located (34 USC § 41308).
- (g) Should continue to make reasonable efforts to locate the missing person and document these efforts at least every 30 days.
- (h) Should consider taking certain actions if a person is missing after a prolonged period, generally exceeding 45 days. Those actions include:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

1. Developing a profile of the possible abductor.
 2. Using a truth verification device for parents, spouse, and other key individuals.
 3. Reviewing all reports and transcripts of interviews, revisiting the crime scene, reviewing all photographs and videotapes, reinterviewing key individuals and reexamining all physical evidence collected.
 4. Reviewing all potential witness/suspect information obtained in the initial investigation and considering background checks on anyone of interest identified in the investigation.
 5. Periodically checking pertinent sources of information about the missing person for any activity, such as telephone, bank, Internet or credit card activity.
 6. Developing a timeline and other visual exhibits.
 7. Critiquing the results of the ongoing investigation with appropriate investigative resources.
 8. Arranging for periodic media coverage.
 9. Considering the use of rewards and crime-stoppers programs.
 10. Maintaining contact with the family and/or the reporting party or designee, as appropriate.
- (i) Shall maintain a close liaison with state and local child welfare systems and the National Center for Missing and Exploited Children (NCMEC) if the missing person is under the age of 21 and shall promptly notify NCMEC when the person is missing from a foster care family home or childcare institution (34 USC § 41308).
 - (j) Should make appropriate inquiry with the Medical Examiner.
 - (k) Should obtain and forward medical and dental records, photos, X-rays, and biological samples, as applicable.
 - (l) Shall attempt to obtain the most recent photograph for persons under 18 years of age if it has not been obtained previously, forward the photograph to BCA (Minn. Stat. § 299C.54), and enter the photograph into applicable missing person networks (34 USC § 41308).
 - (m) In the case of an endangered missing person or a person who has been missing for an extended time, should consult with a supervisor regarding seeking federal assistance from the FBI and the U.S. Marshals Service (28 USC § 566).

315.8 WHEN A MISSING PERSON IS FOUND

When any person reported missing is found, the assigned investigator shall document the location of the missing person in the appropriate report, notify the reporting party and other involved agencies and refer the case for additional investigation if warranted.

The Records Supervisor shall ensure that, upon receipt of information that a missing person has been located, the following occurs:

- (a) Notification is made to BCA.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

- (b) A missing child's school is notified.
- (c) Entries are made in the applicable missing person networks (Minn. Stat. § 299C.53, Subd. 2).
- (d) When a child is endangered, the fact that the child has been found shall be reported within 24 hours to BCA.
- (e) Notification shall be made to any other law enforcement agency that took the initial report or participated in the investigation.

315.8.1 PERSONS FOUND ALIVE

Additional responsibilities related to missing persons who are found alive include:

- (a) Verifying that the located person is the reported missing person.
- (b) If appropriate, arranging for a comprehensive physical examination of the victim.
- (c) Conducting a careful interview of the person, documenting the results of the interview and involving all appropriate agencies.
- (d) Notifying the family/reporting party that the missing person has been located. In adult cases, if the located adult permits the disclosure of his/her whereabouts and contact information, the family/reporting party may be given this information.
- (e) Depending on the circumstances of the disappearance, considering the need for reunification assistance, intervention, counseling or other services for either the missing person or family/reporting party.
- (f) Performing a constructive post-case critique. Reassessing the procedures used and updating the Department policy and procedures as appropriate.

315.8.2 UNIDENTIFIED PERSONS

Members investigating a case of an unidentified person who is deceased or a living person who cannot assist in identifying themselves should:

- (a) Obtain a complete description of the person.
- (b) Enter the unidentified person's description into the NCIC Unidentified Person File and the NamUs database.
- (c) Use available resources, such as those related to missing persons, to identify the person.

315.8.3 DECEASED PERSONS

If a deceased person has been identified as a missing person, the Investigations shall attempt to locate family members and inform them of the death and the location of the deceased missing person's remains. All efforts to locate and notify family members shall be recorded in appropriate reports and properly retained (Minn. Stat. § 390.25, Subd. 2).

Additional investigation responsibilities include the following:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

- (a) Secure the crime scene if this department has jurisdiction.
- (b) Contact the coroner, medical examiner or forensic anthropologist to arrange for body recovery and examination.
- (c) Collect and preserve any evidence at the scene.
- (d) Depending on the circumstances, consider the need for intervention, counseling or other services for the family/reporting party.
- (e) Cancel alerts and remove the case from NCIC and other information systems; remove posters and other publications from circulation.
- (f) Perform a constructive post-case critique. Reassess the procedures used and update the department policy and procedures as appropriate.

315.9 CASE CLOSURE

The Investigations supervisor may authorize the closure of a missing person case after considering the following:

- (a) Closure is appropriate when the missing person is confirmed returned or evidence matches an unidentified person or body.
- (b) If the missing person is a resident of South Saint Paul or this department is the lead agency, the case should be kept under active investigation for as long as the person may still be alive. Exhaustion of leads in the investigation should not be a reason for closing a case.
- (c) If this department is not the lead agency, the case can be made inactive if all investigative leads have been exhausted, the lead agency has been notified and entries are made in the applicable missing person networks, as appropriate.
- (d) A missing person case should not be closed or reclassified because the person would have reached a certain age or adulthood or because the person is now the subject of a criminal or civil warrant.

315.10 TRAINING

Subject to available resources, the Support Services Commander should ensure that members of this department whose duties include missing person investigations and reports receive training that includes:

- (a) The initial investigation:
 - 1. Assessments and interviews
 - 2. Use of current resources, such as Mobile Audio Video (MAV)
 - 3. Confirming missing status and custody status of minors
 - 4. Evaluating the need for a heightened response
 - 5. Identifying the zone of safety based on chronological age and developmental stage
- (b) Briefing of department members at the scene.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Missing Persons

- (c) Identifying NCIC Missing Person File categories (e.g., disability, endangered, involuntary, juvenile and catastrophe).
- (d) Verifying the accuracy of all descriptive information.
- (e) Initiating a neighborhood investigation.
- (f) Investigating any relevant recent family dynamics.
- (g) Addressing conflicting information.
- (h) Key investigative and coordination steps.
- (i) Managing a missing person case.
- (j) Additional resources and specialized services.
- (k) Update procedures for case information and descriptions.
- (l) Preserving scenes.
- (m) Internet and technology issues (e.g., Internet use, cell phone use).
- (n) Media relations.

Public Alerts

316.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for alerting the public to important information and soliciting public aid when appropriate.

316.2 POLICY

Public alerts may be employed using the Emergency Alert System (EAS), local radio, television and press organizations and other groups to notify the public of incidents, or enlist the aid of the public, when the exchange of information may enhance the safety of the community. Various types of alerts may be available based upon each situation and the alert system's individual criteria.

316.3 RESPONSIBILITIES

316.3.1 EMPLOYEE RESPONSIBILITIES

Employees of the South Saint Paul Police Department should notify their supervisor, Sergeant or Investigations Supervisor as soon as practicable upon learning of a situation where public notification, a warning or enlisting the help of the media and public could assist in locating a missing person, apprehending a dangerous person or gathering information.

316.3.2 SUPERVISOR RESPONSIBILITIES

A supervisor apprised of the need for a public alert is responsible to make the appropriate notifications based upon the circumstances of each situation. The supervisor shall promptly notify the Chief of Police, the appropriate Division Commander and the Police Chief when any public alert is generated.

The supervisor in charge of the investigation to which the alert relates is responsible for the following:

- (a) Updating alerts
- (b) Canceling alerts
- (c) Ensuring all appropriate reports are completed
- (d) Preparing an after-action evaluation of the investigation to be forwarded to the Division Commander

316.4 AMBER ALERTS

America's Missing: Broadcast Emergency Response (AMBER) Alert™ is the recruitment of public assistance to locate an abducted child via a widespread media alert. Utilizing the assistance of local radio, television and press affiliates, the public will be notified of the circumstances of a child's abduction and how it can assist law enforcement in the child's recovery. The goal of the AMBER Alert program is the safe return of an abducted child by establishing an effective partnership between the community, the media and law enforcement through the Minnesota Crime Alert Network (Minn. Stat. § 299A.61 Subd. 1).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Public Alerts

316.4.1 CRITERIA

Any non-familial case in which an individual is abducted and the public can assist will trigger the activation of either the AMBER Alert and/or the Minnesota Crime Alert Network (MCAN) to inform the public and request its assistance in locating the individual.

The criteria for issuance of an Amber Alert are as follows:

- (a) A child 17 years of age or younger was abducted and there is reason to believe the victim is in imminent danger of serious bodily injury or death.
- (b) There is information available to disseminate to the general public that could assist with the safe recovery of the victim and/or the apprehension of the suspect.

An AMBER Alert should not be requested if there is no information to distribute.

316.4.2 PROCEDURE

The supervisor shall review the AMBER Alert checklist provided by the Bureau of Criminal Apprehension (BCA) to determine whether the abduction meets the AMBER Alert criteria.

As soon as possible, Records Section personnel shall enter the child's name and other critical data into the National Crime Information Center (NCIC), with appropriate flags.

If the AMBER Alert criteria is met, the supervisor, Sergeant or Investigations supervisor will notify the Operations Center at the BCA. The BCA will determine whether an AMBER Alert will be issued and, if so, will activate the Minnesota Emergency Alert System (EAS) through the Minnesota Department of Public Safety (DPS) Division of Homeland Security and Emergency Management (HSEM).

BCA will manage press notifications through the EAS.

As additional information becomes available, the BCA shall be apprised and they will disseminate the information, as appropriate.

When the child is found, or the alert should be cancelled for other reasons, the Investigations supervisor shall immediately notify BCA with the pertinent information.

316.5 MINNESOTA CRIME ALERT NETWORK (MCAN)

MCAN is a statewide communications network that enables law enforcement agencies to quickly alert the public (Minn. Stat. § 299A.61). In cases where the AMBER Alert criteria are not met, the supervisor shall issue a missing person alert through MCAN to notify the public and request information on the case (Minn. Stat. § 299C.53). Law enforcement agencies, businesses, schools, and community members participate in the network.

316.5.1 CRITERIA

MCAN is available for disseminating information regarding the commission of crimes, including information on missing and endangered children or vulnerable adults, or attempts to reduce theft and other crime.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Public Alerts

316.5.2 PROCEDURE

If a supervisor determines that an MCAN alert should be requested, the supervisor should contact the BCA Operations Center and provide the requested information (Minn. Stat. § 299C.53).

The Police Chief should prepare a press release that includes all available information that might strengthen the assistance by the public or other law enforcement agencies. It should be updated with additional information as it becomes available and useful. All media releases should be coordinated with the BCA. In the event of a confirmed child abduction, whether or not an AMBER Alert or MCAN alert is activated, procedures designed to inform the media should be followed. Initial information to release may include but is not limited to:

- (a) The nature of the crime that has occurred.
- (b) The victim's identity, age, and description, if relevant.
- (c) Photograph if available.
- (d) The suspect's identity, age, and description, if known.
- (e) Pertinent vehicle description.
- (f) Detail regarding location of incident, direction of travel, and potential destinations, if known.
- (g) Whether there is reason to believe the suspect has a relationship to the victim.
- (h) Name and phone number of the Police Chief or other authorized individual to handle media liaison.
- (i) A telephone number for the public to call with leads or information.

As additional information pertinent to the case becomes available, it shall be forwarded to the BCA.

316.6 BLUE ALERTS

Blue Alerts are used to provide a statewide system for the rapid dissemination of information regarding a violent criminal who has seriously injured or killed a local, state or federal law enforcement officer.

316.6.1 CRITERIA

The following criteria should be utilized to determine if a request to activate a Blue Alert will be made:

- (a) A law enforcement officer has been killed, seriously injured or is missing while in the line of duty under circumstances evidencing concern for the officer's safety.
- (b) The investigating law enforcement agency has determined that:
 - 1. The suspect poses a serious risk to the public or other law enforcement personnel.
 - 2. Dissemination of available information to the public may help avert further harm or assist in the apprehension of the suspect.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Public Alerts

- (c) A description of the offender, the offender's vehicle (including license plate or partial license plate) is available for broadcast.

316.6.2 PROCEDURE

The on-duty supervisor should ensure that contact is made with the Minnesota Bureau of Criminal Apprehension (BCA) to request activation of a Blue Alert. The on-duty supervisor should also ensure that any changes to information (e.g., vehicle information, broadcast area) are communicated to BCA in a timely manner.

Victim and Witness Assistance

317.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that crime victims and witnesses receive appropriate assistance, that they are provided with information from government and private resources, and that the agency meets all related legal mandates.

317.2 POLICY

The South Saint Paul Police Department is committed to providing guidance and assistance to the victims and witnesses of crime. The employees of the South Saint Paul Police Department will show compassion and understanding for victims and witnesses and will make reasonable efforts to provide the support and information identified in this policy.

317.3 CRIME VICTIM LIAISON

The Chief of Police should appoint a member of the Department to serve as the crime victim liaison. The crime victim liaison will be the point of contact for individuals requiring further assistance or information from the South Saint Paul Police Department regarding benefits from crime victim resources. This person shall also be responsible for maintaining compliance with all legal mandates related to crime victims and/or witnesses.

317.3.1 SPECIFIC VICTIM LIAISON DUTIES

The crime victim liaison shall assist the Minnesota Crime Victims Reimbursement Board in performing its duties and ensure that the Records Section forwards copies of requested reports to the board or other authorized organizations within 10 days of receipt, in compliance with the Records Maintenance and Release Policy. These reports include those maintained as confidential or not open to inspection under Minn. Stat. § 260B.171 or Minn. Stat. § 260C.171 (Minn. Stat. § 611A.66).

The crime victim liaison will also (Minn. Stat. § 611A.27):

- (a) Serve for a sexual assault victim or a sexual assault victim's written designee as the liaison between the South Saint Paul Police Department and a forensic laboratory.
- (b) Facilitate requests for information made by a sexual assault victim or written designee.
- (c) Provide an appropriate response to a victim's request for investigative data within 30 days.
- (d) Develop a procedure allowing a sexual assault victim to request that the sexual assault examination kit be submitted to a forensic laboratory if the victim had not previously authorized such submission.

The crime victim liaison or the authorized designee, in consultation with the Investigation Division Division Commander, should establish procedures for receiving requests for assistance in applying for U visa or T visa status, and make those procedures available to victims. The procedures should provide for responses to these requests to be made in compliance with

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Victim and Witness Assistance

applicable law and as set forth in the Immigration Violations Policy and applicable law (Minn. Stat. § 611A.95).

317.4 CRIME VICTIMS

Officers should provide all victims with the applicable victim information handouts.

Officers should never guarantee a victim's safety from future harm but may make practical safety suggestions to victims who express fear of future harm or retaliation. Officers should never guarantee that a person qualifies as a victim for the purpose of compensation or restitution but may direct him/her to the proper written department material or available victim resources.

317.5 VICTIM INFORMATION

The Administration Supervisor shall ensure that victim information handouts are available and current. These should include as appropriate:

- (a) Shelters and other community resources for victims, including domestic abuse and sexual assault victims.
- (b) Assurance that sexual assault victims will not incur out-of-pocket expenses for forensic medical exams, and information about evidence collection, storage, and preservation in sexual assault cases (34 USC § 10449; 34 USC § 20109).
- (c) An advisement that a person who was arrested may be released on bond or some other form of release and that the victim should not rely upon an arrest as a guarantee of safety.
- (d) A clear explanation of relevant court orders and how they can be obtained.
- (e) Information regarding available compensation for qualifying victims of crime.
- (f) VINE® information (Victim Information and Notification Everyday), including the telephone number and whether this free service is available to allow victims to check on an offender's custody status and to register for automatic notification when a person is released from jail.
- (g) Notice regarding U visa and T visa application processes.
- (h) Resources available for victims of identity theft.
- (i) A place for the officer's name, badge number, and any applicable case or incident number.
- (j) Notices and information regarding the rights of crime victims, domestic abuse victims, and offender release as detailed in the following:
 - 1. Safe at Home address confidentiality program (Minn. Stat. § 5B.03)
 - 2. Offender release notification (Minn. Stat. § 244.052; Minn. Stat. § 244.053; Minn. Stat. § 611A.06; Minn. Stat. § 629.73)
 - 3. Tenancy issues (Minn. Stat. § 504B.205; Minn. Stat. § 504B.206)
 - 4. Victim and specific domestic abuse victim information/Minnesota CHOICE (Minn. Stat. § 611A.02 et seq.; Minn. Stat. § 629.341; Minn. Stat. § 629.72)

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Victim and Witness Assistance

- (k) A notice that a decision to arrest is the officer's and the decision to prosecute lies with the prosecutor, even when a victim requests no arrest or prosecution.
- (l) Contact information for the Office of Justice Programs and the Emergency Fund and Crime Victims Reimbursement (Minn. Stat. § 611A.66).

317.6 WITNESSES

Officers should never guarantee a witness' safety from future harm or that his/her identity will always remain confidential. Officers may make practical safety suggestions to witnesses who express fear of future harm or retaliation.

Officers should investigate allegations of witness intimidation and take enforcement action when lawful and reasonable.

Standards of Conduct

318.1 PURPOSE AND SCOPE

This policy establishes standards of conduct that are consistent with the values and mission of the South Saint Paul Police Department and are expected of all department members. The standards contained in this policy are not intended to be an exhaustive list of requirements and prohibitions but they do identify many of the important matters concerning conduct. In addition to the provisions of this policy, members are subject to all other provisions contained in this manual, as well as any additional guidance on conduct that may be disseminated by this department or a member's supervisors.

318.1.1 STANDARDS OF CONDUCT FOR PEACE OFFICERS

The South Saint Paul Police Department adopts the Professional Conduct of Peace Officers model policy established and published by the Minnesota Board of Peace Officer Standards and Training Board (POST) (Minn. Stat. § 626.8457). This model policy applies to all peace officers of this department.

[See attachment: MN POST Professional Conduct of Peace Officers Model Policy.pdf](#)

The provisions of this policy are in addition to collective bargaining agreements or any other applicable law.

The Department shall report to POST any data regarding the investigation and disposition of cases involving alleged misconduct of officers (Minn. Stat. § 626.8457, Subd. 3).

318.2 POLICY

The continued employment or appointment of every member of the South Saint Paul Police Department shall be based on conduct that reasonably conforms to the guidelines set forth herein. Failure to meet the guidelines set forth in this policy, whether on- or off-duty, may be cause for disciplinary action.

318.3 DIRECTIVES AND ORDERS

Members shall comply with lawful directives and orders from any department supervisor or person in a position of authority, absent a reasonable and bona fide justification.

318.3.1 UNLAWFUL OR CONFLICTING ORDERS

Supervisors shall not knowingly issue orders or directives that, if carried out, would result in a violation of any law or department policy. Supervisors should not issue orders that conflict with any previous order without making reasonable clarification that the new order is intended to countermand the earlier order.

No member is required to obey any order that appears to be in direct conflict with any federal law, state law or local ordinance. Following a known unlawful order is not a defense and does not relieve the member from criminal or civil prosecution or administrative discipline. If the legality of an order is in doubt, the affected member shall ask the issuing supervisor to clarify the order or

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Standards of Conduct

shall confer with a higher authority. The responsibility for refusal to obey rests with the member, who shall subsequently be required to justify the refusal.

Unless it would jeopardize the safety of any individual, members who are presented with a lawful order that is in conflict with a previous lawful order, department policy or other directive shall respectfully inform the issuing supervisor of the conflict. The issuing supervisor is responsible for either resolving the conflict or clarifying that the lawful order is intended to countermand the previous lawful order or directive, in which case the member is obliged to comply. Members who are compelled to follow a conflicting lawful order after having given the issuing supervisor the opportunity to correct the conflict, will not be held accountable for disobedience of the lawful order or directive that was initially issued.

The person countermanding the original order shall notify, in writing, the person issuing the original order, indicating the action taken and the reason.

318.3.2 SUPERVISOR RESPONSIBILITIES

Supervisors and managers are required to follow all policies and procedures and may be subject to discipline for:

- (a) Failure to be reasonably aware of the performance of their subordinates or to provide appropriate guidance and control.
- (b) Failure to promptly and fully report any known misconduct of a member to his/her immediate supervisor or to document such misconduct appropriately or as required by policy.
- (c) Directing a subordinate to violate a policy or directive, acquiesce to such a violation, or are indifferent to any such violation by a subordinate.
- (d) The unequal or disparate exercise of authority on the part of a supervisor toward any member for malicious or other improper purpose.

318.4 GENERAL STANDARDS

Members shall conduct themselves, whether on- or off-duty, in accordance with the United States and Minnesota constitutions and all applicable laws, ordinances, and rules enacted or established pursuant to legal authority.

Members shall familiarize themselves with policies and procedures and are responsible for compliance with each. Members should seek clarification and guidance from supervisors in the event of any perceived ambiguity or uncertainty.

Discipline may be initiated for any good cause. It is not mandatory that a specific policy or rule violation be cited to sustain discipline. This policy is not intended to cover every possible type of misconduct.

318.5 CAUSES FOR DISCIPLINE

The following are illustrative of causes for disciplinary action. This list is not intended to cover every possible type of misconduct and does not preclude the recommendation of disciplinary action

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Standards of Conduct

for violation of other rules, standards, ethics, and specific action or inaction that is detrimental to efficient department service.

318.5.1 LAWS, RULES AND ORDERS

- (a) Violation of, or ordering or instructing a subordinate to violate any policy, procedure, rule, order, directive, requirement or failure to follow instructions contained in department or City manuals.
- (b) Disobedience of any legal directive or order issued by any department member of a higher rank.
- (c) Violation of federal, state, local or administrative laws, rules or regulations.

318.5.2 ETHICS

- (a) Using or disclosing one's status as a member of the South Saint Paul Police Department in any way that could reasonably be perceived as an attempt to gain influence or authority for nondepartment business or activity.
- (b) The wrongful or unlawful exercise of authority on the part of any member for malicious purpose, personal gain, willful deceit or any other improper purpose.
- (c) The receipt or acceptance of a reward, fee or gift from any person for service incident to the performance of the member's duties (lawful subpoena fees and authorized work permits excepted).
- (d) Acceptance of fees, gifts or money contrary to the rules of this department and/or laws of the state.
- (e) Offer or acceptance of a bribe or gratuity.
- (f) Misappropriation or misuse of public funds, property, personnel or services.
- (g) Any other failure to abide by the standards of ethical conduct.

318.5.3 DISCRIMINATION, OPPRESSION, OR FAVORITISM

Unless required by law or policy, discriminating against, oppressing, or providing favoritism to any person because of actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, economic status, cultural group, veteran status, marital status, and any other classification or status protected by law, or intentionally denying or impeding another in the exercise or enjoyment of any right, privilege, power, or immunity, knowing the conduct is unlawful.

318.5.4 RELATIONSHIPS

- (a) Unwelcome solicitation of a personal or sexual relationship while on-duty or through the use of one's official capacity.
- (b) Engaging in on-duty sexual activity including but not limited to sexual intercourse, excessive displays of public affection, or other sexual contact.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Standards of Conduct

- (c) Establishing or maintaining an inappropriate personal or financial relationship, as a result of an investigation, with a known victim, witness, suspect, or defendant while a case is being investigated or prosecuted, or as a direct result of any official contact.
- (d) Associating with or joining a criminal gang, organized crime, and/or criminal syndicate when the member knows or reasonably should know of the criminal nature of the organization. This includes any organization involved in a definable criminal activity or enterprise, except as specifically directed and authorized by this department.
- (e) Associating on a personal, rather than official, basis with persons who demonstrate recurring involvement in serious violations of state or federal laws after the member knows, or reasonably should know, of such criminal activities, except as specifically directed and authorized by this department.
- (f) Supporting or participating in the activities of a hate or extremist group (Minn. Stat. § 626.8436).

318.5.5 ATTENDANCE

- (a) Leaving the job to which the member is assigned during duty hours without reasonable excuse and proper permission and approval.
- (b) Unexcused or unauthorized absence or tardiness.
- (c) Excessive absenteeism or abuse of leave privileges.
- (d) Failure to report to work or to the place of assignment at the time specified and fully prepared to perform duties without reasonable excuse.

318.5.6 UNAUTHORIZED ACCESS, DISCLOSURE, OR USE

- (a) Unauthorized and inappropriate intentional release of confidential or protected information, materials, data, forms, or reports obtained as a result of the member's position with this department.
- (b) Disclosing to any unauthorized person any active investigation information.
- (c) The use of any information, photograph, video, or other recording obtained or accessed as a result of employment or appointment to this department for personal or financial gain or without the express authorization of the Chief of Police or the authorized designee.
- (d) Loaning, selling, allowing unauthorized use, giving away, or appropriating any department property for personal use, personal gain, or any other improper or unauthorized use or purpose.
- (e) Using department resources in association with any portion of an independent civil action. These resources include but are not limited to personnel, vehicles, equipment, and nonsubpoenaed records.

318.5.7 EFFICIENCY

- (a) Neglect of duty.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Standards of Conduct

- (b) Unsatisfactory work performance including but not limited to failure, incompetence, inefficiency, or delay in performing and/or carrying out proper orders, work assignments, or the instructions of supervisors without a reasonable and bona fide excuse.
- (c) Concealing, attempting to conceal, removing, or destroying defective or incompetent work.
- (d) Unauthorized sleeping during on-duty time or assignments.
- (e) Failure to notify the Department within 24 hours of any change in residence address or contact numbers.
- (f) Failure to notify the Department of Human Resources of changes in relevant personal information (e.g., information associated with benefits determination) in a timely fashion.

318.5.8 PERFORMANCE

- (a) Failure to disclose or misrepresenting material facts, or making any false or misleading statement on any application, examination form, or other official document, report or form, or during the course of any workrelated investigation.
- (b) The falsification of any work-related records, making misleading entries or statements with the intent to deceive or the willful and unauthorized removal, alteration, destruction and/or mutilation of any department record, public record, book, paper or document.
- (c) Failure to participate in, or giving false or misleading statements, or misrepresenting or omitting material information to a supervisor or other person in a position of authority, in connection with any investigation or in the reporting of any department--related business.
- (d) Being untruthful or knowingly making false, misleading or malicious statements that are reasonably calculated to harm the reputation, authority or official standing of this department or its members.
- (e) Disparaging remarks or conduct concerning duly constituted authority to the extent that such conduct disrupts the efficiency of this department or subverts the good order, efficiency and discipline of this department or that would tend to discredit any of its members.
- (f) Unlawful gambling or unlawful betting at any time or any place. Legal gambling or betting under any of the following conditions:
 - 1. While on department premises.
 - 2. At any work site, while on duty or while in uniform, or while using any department equipment or system.
 - 3. Gambling activity undertaken as part of an officer's official duties and with the express knowledge and permission of a direct supervisor is exempt from this prohibition.
- (g) Improper political activity including:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Standards of Conduct

1. Unauthorized attendance while on duty at official legislative or political sessions.
 2. Solicitations, speeches or distribution of campaign literature for or against any political candidate or position while on duty or on department property except as expressly authorized by City policy, the collective bargaining agreement, or the Chief of Police.
- (h) Engaging in political activities during assigned working hours except as expressly authorized by City policy, the collective bargaining agreement, or the Chief of Police.
- (i) Any act on or off duty that brings discredit to this department.

318.5.9 CONDUCT

- (a) Failure of any member to promptly and fully report activities on his/her part or the part of any other member where such activities resulted in contact with any other law enforcement agency or that may result in criminal prosecution or discipline under this policy.
- (b) Unreasonable and unwarranted force to a person encountered or a person under arrest.
- (c) Exceeding lawful peace officer powers by unreasonable, unlawful or excessive conduct.
- (d) Unauthorized or unlawful fighting, threatening or attempting to inflict unlawful bodily harm on another.
- (e) Engaging in horseplay that reasonably could result in injury or property damage.
- (f) Discourteous, disrespectful or discriminatory treatment of any member of the public or any member of this department or the City.
- (g) Use of obscene, indecent, profane or derogatory language while on duty or in uniform.
- (h) Criminal, dishonest, or disgraceful conduct, whether on- or off-duty, that adversely affects the member's relationship with this department.
- (i) Unauthorized possession of, loss of, or damage to department property or the property of others, or endangering it through carelessness or maliciousness.
- (j) Attempted or actual theft of department property; misappropriation or misuse of public funds, property, personnel or the services or property of others; unauthorized removal or possession of department property or the property of another person.
- (k) Activity that is incompatible with a member's conditions of employment or appointment as established by law or that violates a provision of any collective bargaining agreement or contract to include fraud in securing the appointment or hire.
- (l) Initiating any civil action for recovery of any damages or injuries incurred in the course and scope of employment or appointment without first notifying the Chief of Police of such action.
- (m) Any other on or off duty conduct which any member knows or reasonably should know is unbecoming a member of this department, is contrary to good order, efficiency or morale, or tends to reflect unfavorably upon this department or its members.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Standards of Conduct

318.5.10 SAFETY

- (a) Failure to observe or violating department safety standards or safe working practices.
- (b) Failure to maintain current licenses or certifications required for the assignment or position (e.g., driver's license, first aid).
- (c) Failure to maintain good physical condition sufficient to adequately and safely perform law enforcement duties.
- (d) Unsafe firearm or other dangerous weapon handling to include loading or unloading firearms in an unsafe manner, either on- or off-duty.
- (e) Carrying, while on the premises of the work place, any firearm or other lethal weapon that is not authorized by the member's appointing authority.
- (f) Unsafe or improper driving habits or actions in the course of employment or appointment.
- (g) Any personal action contributing to a preventable traffic collision.
- (h) Concealing or knowingly failing to report any on-the-job or work-related accident or injury as soon as practicable but within 24 hours.

318.5.11 INTOXICANTS

- (a) Reporting for work or being at work while intoxicated or when the member's ability to perform assigned duties is impaired due to the use of alcohol, medication or drugs, whether legal, prescribed or illegal.
- (b) Possession or use of alcohol at any work site or while on-duty, except as authorized in the performance of an official assignment. A member who is authorized to consume alcohol is not permitted to do so to such a degree that it may impair on-duty performance.
- (c) Unauthorized possession, use of, or attempting to bring a controlled substance, illegal drug or non-prescribed medication to any work site.

Hate or Prejudice Crimes

319.1 PURPOSE AND SCOPE

The South Saint Paul Police Department recognizes and places a high priority on the rights of all individuals guaranteed under the constitution and the laws of this state. When such rights are infringed upon by violence, threats or other harassment, this department will utilize all available resources to see that justice is served under the law. This policy has been developed to meet or exceed the provisions of the Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act, and provides members of this department with guidelines for identifying and investigating incidents and crimes that may be motivated by hatred or other bias.

319.1.1 FEDERAL JURISDICTION

The federal government also has the power to investigate and prosecute bias-motivated violence by providing the U.S. Department of Justice with jurisdiction over crimes of violence where the perpetrator has selected the victim because of the person's actual or perceived race, color, religion, national origin, gender, sexual orientation, gender identity or disability (18 USC § 245).

319.2 DEFINITIONS

Hate or Prejudice Crime - Conduct that would constitute a crime and was committed because of the victim's or another's actual or perceived race, color, religion, national origin, ethnicity, gender, sexual orientation, gender identity or expression, or disability (see generally Minn. Stat. § 611A.79, Subd. 1).

319.3 PREVENTING AND PREPARING FOR LIKELY HATE OR PREJUDICE CRIMES

While it is recognized that not all crime can be prevented, this department is committed to taking a proactive approach to preventing and preparing for likely hate or prejudice crimes by among other things:

- (a) Officers should make an affirmative effort to establish contact with persons and groups within the community who are likely targets of hate crimes to form and cooperate with prevention and response networks.
- (b) Providing victim assistance and follow-up as outlined below, including community follow-up.
- (c) Educating community and civic groups relating to hate crime laws.

319.4 PROCEDURE FOR INVESTIGATING HATE OR PREJUDICE CRIMES

Whenever any member of this department receives a report of a suspected hate or prejudice crime or other activity that reasonably appears to involve a potential hate or prejudice crime, the following should occur:

- (a) Officers will be promptly assigned to contact the victim, witness or reporting party to investigate the matter further as circumstances may dictate.
- (b) A supervisor should be notified of the circumstances as soon as practicable.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Hate or Prejudice Crimes

- (c) Once “in progress” aspects of any such situation have been stabilized (e.g., treatment of victims or apprehension of present suspects), the assigned officers will take all reasonable steps to preserve available evidence that may tend to establish that a hate or prejudice crime was involved.
- (d) The assigned officers will interview available witnesses, victims and others to determine what circumstances, if any, indicate that the situation may involve a hate or prejudice crime.
- (e) Depending on the situation, the assigned officers or supervisor may request additional assistance from investigators or other resources to further the investigation.
- (f) The assigned officers will include all available evidence indicating the likelihood of a hate or prejudice crime in the relevant report(s). All related reports will be clearly marked as “Hate or Prejudice Crimes” and, absent prior approval of a supervisor, will be completed and submitted by the assigned officers before the end of the shift.
- (g) The assigned officers will provide the victim(s) of any suspected hate or prejudice crime with the brochure on hate and prejudice crimes authorized by the Department. Such brochures will also be available to members of the public upon request. The assigned officers should also make reasonable efforts to assist the victim(s) by providing available information on local assistance programs and organizations as required by the Victim Assistance Policy.
- (h) The assigned officers and supervisor should take reasonable steps to ensure that any such situation does not escalate further and provide information to the victim regarding legal aid, e.g., a possible Temporary Restraining Order through the courts, prosecuting attorney or City Attorney.

319.5 INVESTIGATIONS RESPONSIBILITIES

If a case is assigned to the Investigations, the assigned investigator will be responsible for following up on the reported hate or prejudice crime as follows:

- (a) Coordinating further investigation with the prosecuting attorney and other appropriate law enforcement agencies, as appropriate.
- (b) Maintaining contact with the victim(s) and other involved individuals as needed.
- (c) Maintaining statistical data and tracking of suspected hate or prejudice crimes as indicated or required by state law.

319.5.1 STATE HATE CRIME REPORTING

This department shall report hate or prejudice crime offenses in the form and manner and at regular intervals as prescribed by rules adopted by the Department of Public Safety. This shall be conducted by the Records Supervisor (Minn. Stat § 626.5531 Subd. 1). Reports are required to include:

- (a) The date of the offense.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Hate or Prejudice Crimes

- (b) The location of the offense.
- (c) Whether the target of the incident was a person, private property or public property.
- (d) The crime committed.
- (e) The type of bias and information about the offender and the victim that is relevant to that bias.
- (f) Any organized group involved in the incident.
- (g) The disposition of the case.
- (h) Whether the determination that the offense was motivated by bias was based on the officer's reasonable belief or on the victim's allegation.
- (i) Any additional information the superintendent deems necessary for the acquisition of accurate and relevant data.

319.5.2 FEDERAL HATE CRIME REPORTING

The Records Supervisor should include hate crime data reporting within the National Incident-Based Reporting System (NIBRS), Uniform Crime Report (UCR) and Summary Reporting System (SRS) reports pursuant to Records Section procedures and in compliance with (28 USC § 534 (a)).

319.6 TRAINING

All members of this department will receive training on hate and prejudice crime recognition and investigation and will attend periodic training that incorporates a hate and prejudice crime training component (Minn. Stat § 626.8451 Subd. 1 and 4).

Information Technology Use

320.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of department information technology resources, including computers, electronic devices, hardware, software and systems.

320.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented, or licensed by the South Saint Paul Police Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or department funding.

Cybersecurity incident - An action taken through the use of an information system or network that results in an actual or potentially adverse effect on an information system, network, or the information within (Minn. Stat. § 16E.36, Subd. 1).

Hardware - Includes but is not limited to computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, modems, or any other tangible computer device generally understood to comprise hardware.

Software - Includes but is not limited to all computer programs, systems, and applications, including shareware and firmware. This does not include files created by the individual user.

Temporary file, permanent file, or file - Any electronic document, information, or data residing or located, in whole or in part, on the system including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs, or videos.

320.2 INSPECTION OR REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member's duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor or during the course of regular duties that require such information.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Information Technology Use

320.3 PROTECTION OF AGENCY SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the computer system.

Members shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off, and password protections enabled whenever the user is not present. Access passwords, logon information, and other individual security data, protocols, and procedures are confidential information and are not to be shared. Password length, format, structure, and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor. Passwords for accounts that access CJI are governed by the CJIS Access, Maintenance, and Security Policy.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the internet) to a supervisor.

320.4 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisors or Sergeants.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

320.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any department computer. Members shall not install personal copies of any software onto any department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Information Technology Use

Introduction of software by members should only occur as part of the automated maintenance or update process of department- or City-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

320.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

320.4.3 INTERNET USE

Internet access provided by or through the Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include but are not limited to adult forums, pornography, gambling, chat rooms, and similar or related internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information from the internet shall be limited to messages, mail, and data files.

320.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other "off the clock" work-related activities. This also applies to personally owned computers that are used to access department resources.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

320.5 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any department computer system.

The Department reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network and/or any information placed into storage on any department system or device. This includes records of all keystrokes or Web-browsing history made at any

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Information Technology Use

department computer or over any department network. The fact that access to a database, service or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices or networks.

320.6 POLICY

It is the policy of the South Saint Paul Police Department that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy.

320.7 CYBERSECURITY INCIDENTS

The Chief of Police or the authorized designee shall report any cybersecurity incident that impacts the Department to the Minnesota Bureau of Criminal Apprehension within 72 hours after an incident has been identified (Minn. Stat. § 16E.36, Subd. 2).

Report Preparation

321.1 PURPOSE AND SCOPE

Report preparation is a major part of each employee's job. The purpose of reports is to document sufficient information to refresh the employee's memory and to provide sufficient information for follow-up investigation and successful prosecution. Report writing is the subject of substantial formalized and on-the-job training.

321.1.1 REPORT PREPARATION

Employees should ensure that their reports are sufficient for their purpose and reasonably free of errors prior to submission. It is the responsibility of the assigned employee to complete and submit all reports taken during the shift before going off-duty, unless permission to hold the report has been approved by a supervisor. Generally, reports requiring prompt follow-up action on active leads, or arrest reports where the suspect remains in custody should not be held.

Employees who dictate reports shall use appropriate grammar and punctuation. Employees who generate reports on computers are subject to all requirements of this policy.

All reports shall accurately reflect the identity of the persons involved, all pertinent information seen, heard or assimilated by any other sense and any actions taken. Employees shall not suppress, conceal or distort the facts of any reported incident nor shall any employee make a false report orally or in writing. Generally, the reporting employee's opinions should not be included in reports unless specifically identified as such.

321.2 REQUIRED REPORTING

Written reports are required in all of the following situations on the appropriate Department-approved form unless otherwise approved by a supervisor.

321.2.1 CRIMINAL ACTIVITY

When a member responds to a call for service, or as a result of self-initiated activity becomes aware of any activity where a crime has occurred, the member shall document the incident regardless of whether a victim desires prosecution.

Activity to be documented in a written report includes:

- (a) All arrests
- (b) All felony crimes
- (c) All incidents involving violations of crimes or ordinances motivated by bias (Minn. Stat. § 626.5531)
- (d) Non-felony incidents involving threats or stalking behavior
- (e) Situations covered by separate policy. These include:
 - 1. Use of Force Policy

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Report Preparation

2. Domestic Abuse Policy
3. Child Abuse Policy
4. Adult Abuse Policy
5. Hate or Prejudice Crimes Policy
6. Suspicious Activity Reports Policy

- (f) All misdemeanor crimes where the victim desires a report

Misdemeanor crimes where the victim does not desire a report shall be documented using the department-approved alternative reporting method (e.g., dispatch log).

321.2.2 NON-CRIMINAL ACTIVITY

The following incidents shall be documented using the appropriate approved report:

- (a) Any time an officer points a firearm at any person
- (b) Any use of force against any person by a member of this department (see the Use of Force Policy)
- (c) Any firearm discharge (see the Firearms Policy)
- (d) Any time a person is reported missing, regardless of jurisdiction (see the Missing Persons Policy)
- (e) Any time an officer responds to the report of a disturbance involving family or household members. Family or household members is defined as:
 1. spouses and former spouses;
 2. parents and children;
 3. persons related by blood;
 4. persons who are presently residing together or who have resided together in the past;
 5. persons who have a child in common regardless of whether they have been married or have lived together at any time;
 6. a man and woman if the woman is pregnant and the man is alleged to be the father, regardless of whether they have been married or have lived together at any time; and
 7. persons involved in a significant romantic or sexual relationship.
- (f) Any found property or found evidence
- (g) Any traffic collisions above the minimum reporting level (see the Traffic Collision Response and Reporting Policy)
- (h) Suspicious incidents that may indicate a potential for crimes against children or that a child's safety is in jeopardy

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Report Preparation

- (i) All protective custody detentions
- (j) Suspicious incidents that may place the public or others at risk
- (k) Whenever the employee believes the circumstances should be documented or at the direction of a supervisor
- (l) Any watercraft collision or accident, drowning death and/or general water accident should be reported on the appropriate Department of Natural Resource Form (Minn. Stat. § 86B.105(a))

321.2.3 DEATH REPORTS

Reports shall be completed by the handling employee. All deaths shall be handled in compliance with the Death Investigations Policy.

321.2.4 INJURY OR DAMAGE BY CITY PERSONNEL

Reports shall be taken if an injury occurs that is a result of an act of a City employee. Additionally, reports shall be taken involving damage to City property or City equipment.

321.2.5 MISCELLANEOUS INJURIES

Any injury that is reported to this department shall require a report when:

- (a) The injury is a result of a drug overdose.
- (b) Attempted suicide.
- (c) The injury is major or serious, whereas death could result.
- (d) The circumstances surrounding the incident are suspicious in nature and it is desirable to record the event.

The above reporting requirements are not intended to be all-inclusive. A supervisor may direct an employee to document any incident he/she deems necessary.

321.3 GENERAL POLICY OF EXPEDITIOUS REPORTING

In general, all employees and supervisors shall act with promptness and efficiency in the preparation and processing of all reports. An incomplete report, unorganized reports or reports delayed without supervisory approval are not acceptable. Reports shall be processed according to established priorities or according to special priority necessary under exceptional circumstances.

321.3.1 GENERAL USE OF OTHER HANDWRITTEN FORMS

County, state and federal agency forms may be block printed as appropriate. In general, the form itself may make the requirement for typing apparent.

321.4 REPORT CORRECTIONS

Supervisors shall review reports for content and accuracy. If a correction is necessary, the reviewing supervisor should reject the report back to the employee for correction with reasons stated. The original report should be returned to the reporting employee for correction as soon

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Report Preparation

as practicable. It shall be the responsibility of the originating employee to ensure that any report returned for correction is processed in a timely manner.

321.5 REPORT CHANGES OR ALTERATIONS

Reports that have been approved by a supervisor and submitted to the Records Section for filing and distribution shall not be modified or altered except by way of a supplemental report. Reviewed reports that have not yet been submitted to the Records Section may be corrected or modified by the authoring employee only with the knowledge and authorization of the reviewing supervisor.

321.6 ELECTRONIC SIGNATURES

The South Saint Paul Police Department has established an electronic signature procedure for use by all employees of the South Saint Paul Police Department. The Patrol Division Commander shall be responsible for maintaining the electronic signature system, for ensuring that each employee creates a unique, confidential password for his/her electronic signature and that the use of electronic signatures otherwise complies with the law.

- Employees may only use their electronic signature for official reports or other official communications.
- Each employee shall be responsible for the security and use of his/her electronic signature and shall promptly notify a supervisor if the electronic signature has or may have been compromised or misused.

321.7 FIREARM INJURY REPORTING FROM HEALTH PROFESSIONALS

Members receiving a report from a health professional of a bullet or gunshot wound, powder burns or any other injury arising from, or caused by, the discharge of any gun, pistol or any other firearm shall thoroughly investigate the facts surrounding the incident (Minn. Stat. § 626.52, Subd. 2; Minn. Stat. § 626.553, Subd. 1).

The Records Section shall ensure that the report received from the health professional is forwarded to the commissioner of the Department of Health (Minn. Stat. § 626.53, Subd. 2). If the injury resulted from a hunting incident, the Records Section shall ensure that the findings of the investigation are forwarded to the commissioner of the Department of Natural Resources using the form provided by the commissioner (Minn. Stat. § 626.553, Subd. 1).

News Media Relations

322.1 PURPOSE AND SCOPE

This policy provides guidelines for media releases and media access to scenes of disasters, criminal investigations, emergencies and other law enforcement activities.

322.2 RESPONSIBILITIES

The ultimate authority and responsibility for the release of information to the media shall remain with the Chief of Police. However, in situations not warranting immediate notice to the Chief of Police and in situations where the Chief of Police has given prior approval, Division Commanders, Sergeants and designated Police Chief(s) may prepare and release information to the media in accordance with this policy and the applicable law.

322.2.1 MEDIA REQUEST

Any media request for information or access to a law enforcement situation shall be referred to the designated Department media representative, or if unavailable, to the first available supervisor. Prior to releasing any information to the media, employees shall consider the following:

- (a) At no time shall any employee of this department make any comment or release any official information to the media without prior approval from a supervisor or the designated Department media representative.
- (b) In situations involving multiple law enforcement agencies, every reasonable effort should be made to coordinate media releases with the authorized representative of each involved agency prior to the release of any information by this department.
- (c) Under no circumstance should any member of this department make any comment(s) to the media regarding any law enforcement incident not involving this department without prior approval of the Chief of Police.

322.3 MEDIA ACCESS

Authorized members of the media shall be provided access to scenes of disasters, criminal investigations, emergencies and other law enforcement activities subject to the following conditions:

- (a) Media personnel have a right to observe, document and disseminate information to the public regarding government activities that are conducted in public. Law enforcement shall never prevent, deter or otherwise intimidate media from lawfully capturing and providing this information to the public. Media shall be permitted to observe and shall be permitted close enough access during arrests to document the contact with the arrestees. Even after a dispersal order has been given, clearly documented and identified media shall be permitted to carry out their professional duties in any area where arrests are being made. However, if their presence would unduly interfere with the enforcement action, they shall be instructed to relocate to an area near the arrest location. Law enforcement shall ensure this policy is consistent with any court or state executive order such as a curfew order. This identified area must be made clear to

South Saint Paul Police Department

S Saint Paul PD Policy Manual

News Media Relations

the media personnel so that they understand where they need to relocate or what actions they must take. If after several requests have been made to the media to relocate due to their interference and individual media personnel fail to do so causing additional interference, those individuals may be arrested. A decision to arrest should be a last resort and the reasons for the arrest and why relocation was not successful must be fully documented. Media shall never be targeted for dispersal or enforcement action merely because of their status. Individuals claiming to be media personnel should provide credentials identifying who they are and the media outlet to which they are associated. If you are unable to identify who they are after credentials have been provided, efforts should be made to further identify them by whatever means is available.

- (b) No member of this department shall be required to submit to media visits or interviews without the consent of the involved employee.
- (c) Media interviews with individuals who are in custody shall not be permitted unless in compliance with a jail facility policy. Exceptions are only permitted with the approval of the Chief of Police and the express written consent of the person in custody.

A tactical operation should be handled in the same manner as a crime scene, except the news media shall be permitted within within a designated area near the scene, subject to any restrictions as determined by the supervisor in charge. Department members shall not jeopardize a tactical operation in order to accommodate the news media. All comments to the media shall be coordinated through a supervisor or the Police Chief.

322.3.1 TEMPORARY FLIGHT RESTRICTIONS

Whenever the presence of media or other aircraft poses a threat to public or officer safety or significantly hampers incident operations, the field supervisor should consider requesting a Temporary Flight Restriction (TFR). All requests for a TFR should be routed through the Sergeant. The TFR request should include specific information regarding the perimeter and altitude necessary for the incident and should be requested through the appropriate control tower. If the control tower is not known, the Federal Aviation Administration should be contacted (14 CFR 91.137).

322.3.2 PROVIDING ADVANCE INFORMATION

To protect the safety and rights of officers and other persons, advance information about planned actions by law enforcement personnel, such as movement of persons in custody or the execution of an arrest or search warrant, should not be disclosed to the news media nor should media representatives be invited to be present at such actions except with the prior approval of the Chief of Police.

Any exceptions to the above should only be considered for the furtherance of legitimate law enforcement purposes. Prior to approving any exception, the Chief of Police will consider, at minimum, whether the release of information or presence of the media would unreasonably endanger any individual, prejudice the rights of any person or is otherwise prohibited by law.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

News Media Relations

322.4 SCOPE OF INFORMATION SUBJECT TO RELEASE

The Department will maintain a daily information log of significant law enforcement activities that shall be made available, upon request, to media representatives through the Sergeant. This log will consist of data classified as public and should generally contain the following information (Minn. Stat. § 13.82):

- (a) The date, time, location, case number, type of crime, extent of injury or loss and names of individuals (except confidential informants) involved in crimes occurring within this jurisdiction, unless the release of such information would endanger the safety of any individual or jeopardize the successful completion of any ongoing investigation.
- (b) The date, time, location, case number, name, birth date and charges for each person arrested by this department, unless the release of such information would endanger the safety of any individual or jeopardize the successful completion of any ongoing investigation.
- (c) The time and location of other significant law enforcement activities or requests for service with a brief summary of the incident subject to the restrictions of this policy and applicable law.

At no time shall identifying information pertaining to a juvenile arrestee be publicly released without prior approval of a competent court or as permitted by state law (Minn. Stat. § 260B.171, Subd. 5).

At no time shall identifying information pertaining to a victim be publicly released without prior approval of a competent court when access to the data would reveal the identity of a victim or alleged victim of criminal sexual conduct or a violation of Minn. Stat. § 617.246, Subd. 2 (Minn. Stat. § 13.82 Subd. 17 (b)).

At no time shall identifying information pertaining to a juvenile witness be publicly released without prior approval of a competent court when this department has determined that the identity of a juvenile witness reasonably requires protection (Minn. Stat. § 13.82, Subd. 17 (g)).

Information concerning incidents involving persons whose identities are classified as private data under Minn. Stat. § 13.82, Subd. 17, shall be restricted from disclosure in accordance with that statute. Further detail is available in the Records Maintenance and Release Policy.

Identifying information concerning deceased individuals should only be released to the media when the decedent's identity has been verified and the release is approved by a supervisor.

Any requests for copies of related reports or additional information not contained in this log shall be referred to the designated media representative, the custodian of records, or if unavailable, to the Sergeant. Such requests will generally be processed in accordance with the provisions of the Minnesota Data Practices Act (Minn. Stat. § 13.03).

322.4.1 STATE RESTRICTED INFORMATION

It shall be the responsibility of the authorized employee dealing with media requests to ensure that restricted information is not inappropriately released to the media by this department

South Saint Paul Police Department

S Saint Paul PD Policy Manual

News Media Relations

(See the Records Maintenance and Release Policy and the Personnel Files Policy). When in doubt, authorized and available legal counsel should be obtained. Examples of such restricted information include, but are not limited to:

- (a) The identities of involved officers only when the release hinders a law enforcement purpose or reveals the identity of an undercover law enforcement officer and as otherwise required by law (Minn. Stat. § 13.82).
- (b) Photographs of an officer without his/her permission except as provided in Minn. Stat. § 626.89 Subd. 12.
- (c) Copies of traffic collision reports except to those authorized pursuant to Minn. Stat. § 169.09 Subd. 13.
- (d) Information that would tend to endanger the safety of any individual or jeopardize the successful completion of any ongoing investigation.
- (e) Information pertaining to pending litigation involving this department.
- (f) Information that uniquely describes stolen, lost, confiscated or recovered property (Minn. Stat. § 13.82 Subd. 20).
- (g) Any information that is otherwise privileged or restricted under state or federal law.

Court Appearance and Subpoenas

323.1 PURPOSE AND SCOPE

This policy establishes the guidelines for department members who must appear in court. It will allow the South Saint Paul Police Department to cover any related work absences and keep the Department informed about relevant legal matters.

323.2 POLICY

South Saint Paul Police Department members will respond appropriately to all subpoenas and any other court-ordered appearances.

323.3 SUBPOENAS

Only department members authorized to receive a subpoena on behalf of this department or any of its members may do so (Minn. R. Civ. P. 45.02; Minn. R. Crim. P. 22.03).

A court notice from a prosecutor or other government attorney may be served by delivery to the member's workstation or mail box. Members shall check for delivery of such documents during each shift worked.

Subpoenas shall not be accepted in a civil action in which the member or Department is not a party without properly tendered fees pursuant to applicable law (Minn. Stat. § 357.23; Minn. R. Civ. P. 45.03).

323.3.1 SPECIAL NOTIFICATION REQUIREMENTS

Any member who is subpoenaed to testify, agrees to testify or provides information on behalf of or at the request of any party other than the City Attorney or the prosecutor shall notify his/her immediate supervisor without delay regarding:

- (a) Any civil case where the City or one of its members, as a result of his/her official capacity, is a party.
- (b) Any civil case where any other city, county, state or federal unit of government or a member of any such unit of government, as a result of his/her official capacity, is a party.
- (c) Any criminal proceeding where the member is called to testify or provide information on behalf of the defense.
- (d) Any civil action stemming from the member's on-duty activity or because of his/her association with the South Saint Paul Police Department.
- (e) Any personnel or disciplinary matter when called to testify or to provide information by a government entity other than the South Saint Paul Police Department.

The supervisor will then notify the Chief of Police and the appropriate prosecuting attorney as may be indicated by the case. The Chief of Police should determine if additional legal support is necessary.

No member shall be retaliated against for testifying in any matter.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Court Appearance and Subpoenas

323.3.2 CIVIL SUBPOENA

The Department will compensate members who appear in their official capacities on civil matters arising out of their official duties, in accordance with any collective bargaining agreement.

The Department should seek reimbursement for the member's compensation through the civil attorney of record who subpoenaed the member.

323.3.3 OFF-DUTY RELATED SUBPOENAS

Members receiving valid subpoenas for off-duty actions not related to their employment or appointment will not be compensated for their appearance. Arrangements for time off shall be coordinated through their immediate supervisors.

323.4 FAILURE TO APPEAR

Any member who fails to comply with the terms of any properly served subpoena or court-ordered appearance may be subject to discipline. This includes properly served orders to appear that were issued by a state administrative agency.

323.5 STANDBY

To facilitate standby agreements, members are required to provide and maintain current information on their addresses and contact telephone numbers with the Department.

If a member on standby changes his/her location during the day, the member shall notify the designated department member of how he/she can be reached. Members are required to remain on standby until released by the court or the party that issued the subpoena.

323.6 COURTROOM PROTOCOL

When appearing in court, members shall:

- (a) Be punctual and prepared to proceed immediately with the case for which they are scheduled to appear.
- (b) Dress in the department uniform or business attire.
- (c) Observe all rules of the court in which they are appearing and remain alert to changes in the assigned courtroom where their matter is to be heard.

323.6.1 TESTIMONY

Before the date of testifying, the subpoenaed member shall request a copy of relevant reports and become familiar with the content in order to be prepared for court.

323.7 OVERTIME APPEARANCES

When a member appears in court on his/her off-duty time, he/she will be compensated in accordance with any current collective bargaining agreement .

Outside Agency Assistance

324.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members when requesting or responding to a request for mutual aid or when assisting another law enforcement agency.

324.2 POLICY

It is the policy of the South Saint Paul Police Department to promptly respond to requests for assistance by other law enforcement agencies, subject to available resources and consistent with the applicable laws and policies of this department.

324.3 ASSISTING OUTSIDE AGENCIES

Generally, requests for any type of assistance from another agency should be routed to the Sergeant's office for approval. Any such response to assist an outside agency may be considered for authorization regardless of whether an agreement for reciprocal aid under Minn. Stat. § 626.76, Subd. 1 exists. In some instances, a memorandum of understanding or other established protocol may exist that eliminates the need for approval of individual requests.

When another law enforcement agency requests assistance from this department, the Sergeant may authorize, if available, an appropriate number of personnel to assist. Members are reminded that their actions when rendering assistance must conform with applicable laws and be consistent with the policies of this department.

Officers may respond to a request for emergency assistance; however, they shall notify a supervisor of their activity as soon as practicable.

Arrestees may be temporarily detained by this department until arrangements for transportation are made by the outside agency. Probation violators who are temporarily detained by this department will not ordinarily be booked at this department. Only in exceptional circumstances, and subject to supervisor approval, will this department provide transportation of arrestees to other facilities on behalf of another agency.

When transportation assistance is rendered, a report shall be prepared and submitted by the handling member unless otherwise directed by a supervisor.

324.3.1 AGREEMENTS

The Department may, at the discretion of the Chief of Police, establish an agreement with another law enforcement agency to (Minn. Stat. § 626.76, Subd.1):

- (a) Assist other peace officers in the line of their duty and within the course of their employment.
- (b) Exchange department peace officers with peace officers of another agency on a temporary basis.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Outside Agency Assistance

324.3.2 INITIATED ACTIVITY

Any on-duty officer who engages in law enforcement activities of any type that are not part of a mutual aid request and take place outside the jurisdiction of the South Saint Paul Police Department shall notify his/her supervisor or the Sergeant and Dispatch as soon as practicable. This requirement does not apply to special enforcement details or multi-agency units that regularly work in multiple jurisdictions.

324.4 REQUESTING OUTSIDE ASSISTANCE

If assistance is needed from another agency, the member requesting assistance should, if practicable, first notify a supervisor. The handling member or supervisor should direct assisting personnel to where they are needed and to whom they should report when they arrive.

The requesting member should arrange for appropriate radio communication capabilities, if necessary and available, so that communication can be coordinated between assisting personnel.

324.5 REPORTING REQUIREMENTS

Incidents of outside assistance or law enforcement activities that are not documented in a crime report shall be documented in a general case report or as directed by the Sergeant.

324.6 MANDATORY SHARING

Equipment and supplies purchased with federal funds or grants that require such equipment and supplies be shared with other agencies should be documented and updated as necessary by the Administration Division Commander or the authorized designee.

The documentation should include:

- (a) The conditions relative to sharing.
- (b) The training requirements for:
 - 1. The use of the supplies and equipment.
 - 2. The members trained in the use of the supplies and equipment.
- (c) Any other requirements for use of the equipment and supplies.

Copies of the documentation should be provided to Dispatch and the Sergeant to ensure use of the equipment and supplies is in compliance with the applicable sharing agreements.

The Support Services Commander should maintain documentation that the appropriate members have received the required training.

Registered Predatory Offender

325.1 PURPOSE AND SCOPE

This policy establishes guidelines by which the South Saint Paul Police Department will address issues associated with certain offenders who are residing in the jurisdiction and how the Department will disseminate information and respond to public inquiries for information about registered offenders.

325.2 POLICY

It is the policy of the South Saint Paul Police Department to identify and monitor registered offenders living within this jurisdiction and to take reasonable steps to address the risks those persons may pose.

325.3 REGISTRATION

The assigned Sergeant shall establish a process to reasonably accommodate registration of certain offenders. The process should rebut any allegation on the part of the offender that the registration process was too confusing, burdensome or difficult for compliance. If it is reasonable to do so, an investigator assigned to related investigations should conduct the registration in order to best evaluate any threat the person may pose to the community. Employees assigned to register offenders should receive appropriate training regarding the registration process.

Upon conclusion of the registration process, the investigator shall ensure that the registration information is provided to the Bureau of Criminal Apprehension (BCA) in accordance with Minn. Stat. § 243.166 within three days of the registration. Registration and updated information from a person who lacks a primary residence shall be forwarded within two days. Updated primary address information from any registered predatory offender shall also be forwarded within two days (Minn. Stat. § 243.166).

The refusal of a registrant to provide any of the required information or complete the process should initiate a criminal investigation for failure to register.

325.3.1 REGISTRATION PROCESS

When an offender arrives to register with this department, the assigned investigator should:

- (a) Determine in what state the offense was committed.
- (b) Confirm the individual is required to register by reviewing the list of Minnesota offenses on the BCA's Predatory Offender Registration website or in the BCA Predatory Offender Registration (POR) Manual that is available on the BCA's secure website.
- (c) If a person is required to register, search the BCA's secure website to verify whether the offender is already registered and a DNA sample has been submitted.
- (d) If the offender is already registered, complete a Change of Information Form (available on the BCA's secure website).
- (e) If the offender is not registered, complete a POR Form (available at BCA's secure website).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Registered Predatory Offender

- (f) If the offender is from another state, contact the state (information for each state is listed on the BCA's website) and request a copy of the offender's original registration form, criminal complaint and sentencing documents.
 - 1. Documents obtained should be submitted to the BCA with a registration form.
 - 2. The BCA will determine if registration is required and inform the department and the offender.

Additional information regarding offender registration is available in the POR Manual or by contacting the Predatory Offender Unit by phone or through the BCA secure website.

325.3.2 GUIDELINES AND FORMS

The registration process shall be in accordance with Minn. Stat. § 243.166 and follow the guidelines implemented by the BCA. Forms used in the registration process are available from the secure website operated by the BCA.

325.3.3 NOTIFICATION TO REGISTRANTS

The registration process established by the Operations Commander should include procedures for determining whether an individual requires notification of his/her requirement to register because the individual was not otherwise notified of the requirement by the sentencing court or assigned a corrections agent (Minn. Stat. § 243.166).

325.4 MONITORING OF REGISTERED OFFENDERS

The Operations Commander should establish a system to periodically, and at least once annually, verify that a registrant remains in compliance with his/her registration requirements after the initial registration. This verification should include:

- (a) Efforts to confirm residence using an unobtrusive method, such as an internet search or drive-by of the declared residence.
- (b) Review of information on the BCA secure website or the Department of Corrections Offender Information (DOC) website.
- (c) Contact with a registrant's parole or probation officer, if any.

Any discrepancies should be reported to BCA in writing.

The Operations Commander should also establish a procedure to routinely disseminate information regarding registered offenders to South Saint Paul Police Department personnel who have a need to know, including timely updates regarding new or relocated registrants.

325.5 DISSEMINATION OF PUBLIC INFORMATION

Members will not make a public notification advising the community of a particular registrant's presence in the community without permission from the Chief of Police. Members who believe notification is appropriate should promptly advise their supervisor. The supervisor should evaluate the request and forward the information to the Chief of Police if warranted. A determination will be made by the Chief of Police based on statutory requirements, with the assistance of legal counsel as necessary, whether such a public alert should be made.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Registered Predatory Offender

The Records Supervisor shall release local registered offender information to residents in accordance with state law (Minn. Stat. § 244.052; Minn. Stat. § 243.166, Subd. 7; Minn. Stat. § 13.01 et seq.) and in compliance with a Minnesota Government Data Practices Act request.

325.5.1 MANDATORY DISSEMINATION

The Department shall provide and release predatory offender data, or updated data, obtained from the DOC based upon the offender's status of a Level 1, 2, or 3.

The Department shall continue to disclose data on an offender as required by law for as long as the offender is required to register under Minn. Stat. § 243.166.

Disclosure to the health care facility, home care provider, or hospice provider of the status of any registered predatory offender under Minn. Stat. § 243.166 who is receiving care shall be made by this department (Minn. Stat. § 244.052, Subd. 4c).

The Department shall provide an offender's change of status to the entities and individuals who were initially notified if the Department becomes aware that the area where notification was made is no longer where the offender resides, is employed, or is regularly found (Minn. Stat. § 244.052, Subd. 4).

325.5.2 LEVEL 1 DISCLOSURE

Data maintained by law enforcement may be subject to limited disclosure (Minn. Stat. § 244.052, Subd. 4) (refer to the DOC document "Confidential Fact Sheet - For Law Enforcement Agency Use Only" or other DOC guidance):

- (a) Mandatory disclosure:
 - 1. Victims who have requested disclosure
 - 2. Adult members of the offender's immediate household
- (b) Discretionary disclosure:
 - 1. Other witnesses or victims
 - 2. Other law enforcement agencies

325.5.3 LEVEL 2 DISCLOSURE

Data is subject to limited disclosure for the purpose of securing institutions and protecting individuals in their care while they are on or near the premises of the institution (Minn. Stat. § 244.052, Subd. 4) (refer to DOC document "Law Enforcement Agency Fact Sheet - Notification of Release in Minnesota - Risk Level 2" or other DOC guidance):

- (a) In addition to Level 1 disclosure, the Department may disclose data to:
 - 1. Staff members of public and private educational institutions, day care establishments and establishments that primarily serve individuals likely to be victimized by the offender.
 - 2. Individuals likely to be victimized by the offender.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Registered Predatory Offender

- (b) Discretionary notification must be based on the offender's pattern of offending or victim preference as documented by the DOC or the Minnesota Department of Human Services (DHS).

325.5.4 LEVEL 3 DISCLOSURE

Data is subject to disclosure not only to safeguard facilities and protect the individuals they serve but also to protect the community as a whole (Minn. Stat. § 244.052, Subd. 4) (refer to the DOC document "Law Enforcement Agency Fact Sheet - Notification of Release in Minnesota" or other DOC guidance):

- (a) The Department shall disclose information to the persons and entities provided for Level 1 and 2 disclosures.
- (b) The Department shall disclose data to other members of the community that the offender is likely to encounter unless public safety would be compromised by the disclosure or a more limited disclosure is necessary to protect the identity of the victim.
- (c) A good faith effort must be made to complete the disclosure within 14 days of receiving a confirmed address from the DOC.
- (d) The process of notification is determined by this department. The DOC has recommended that the community be invited to a public meeting and disclose the necessary data. Assistance is available from the DOC Risk Assessment/Community Notification (RA/CN) Unit.

Data disclosed to the public of a Level 3 predatory offender shall be forwarded to the DOC within two days of the department's determination to disclose (Minn. Stat. § 244.052, Subd. 4(g)).

325.5.5 HEALTH CARE FACILITY NOTIFICATION

Upon notice that a registered predatory offender is planning to be in this jurisdiction or has been admitted to a health care facility, home care provider, or hospice provider in this jurisdiction, this department shall provide a fact sheet to the facility administrator with the following data (Minn. Stat. § 243.166, Subd. 4b) (refer to the DOC documents, "Law Enforcement Agency Fact Sheet Health Care Facility Notification Data on a Registered Offender Not For Distribution to Facility Residents" and "Law Enforcement Agency Fact Sheet Health Care Facility Notification Data on a Registered Offender For Distribution to Facility Residents" or other DOC guidance):

- (a) Name and physical description of the offender
- (b) Offender's conviction history, including the dates of conviction
- (c) Risk level assigned to the offender, if any
- (d) Profile of likely victims

325.5.6 SPECIALIZED NOTIFICATION

Offenders from other states and offenders released from federal facilities are also subject to notification (Minn. Stat. § 244.052, Subd. 3a):

- (a) If this department learns that a person under its jurisdiction is subject to registration and desires consultation on whether the person is eligible for notification, the Department

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Registered Predatory Offender

must contact the DOC. The DOC will review the governing law of the other state and, if comparable to Minnesota requirements, inform this department whether to proceed with community notification in accordance with the level assigned by the other state.

- (b) If the DOC determines that the governing law in the other state is not comparable, community notification by this department may be made consistent with that authorized for risk Level 2.
- (c) If this department believes that a risk level assessment is needed, the Department may request an end-of-confinement review. The Department shall provide to the DOC the necessary documents required to assess a person for a risk level.

325.5.7 VICTIM NOTIFICATION

If a predatory offender resides, expects to reside, is employed or is regularly found in this jurisdiction, the Department shall provide victims who have requested notification with data that is relevant and necessary to protect the victim. Information disclosed should be obtained from the risk assessment report provided by DOC (Minn. § Stat. 244.052, Subd. 3).

The DOC will provide victim contact data to this department when there is a victim who has requested notification (refer to the DOC document "Victim Data Confidential for Law Enforcement Agency Use Only").

It may be appropriate for members of the Department to directly contact the victim. Community victim advocacy or prosecutor resources may also be available to assist with locating and notifying a victim. Assistance is also available from the DOC victim services staff.

Members of the Department may contact other victims, witnesses and other individuals who are likely to be victimized by the offender.

325.5.8 HOMELESS NOTIFICATION PROCESS

If public notice (Level 2 or 3) is required on a registered homeless offender, that notice should be as specific as possible. These offenders are required to check in weekly with local law enforcement, unless an alternative reporting procedure is approved by the Operations Commander (Minn. Stat. § 243.166, Subd. 3a).

325.5.9 LIMITATIONS OF RELEASE OF DATA

Disclosures permitted or required for Level 2 or 3 offenders shall not be made if the offender is placed or resides in a DOC-licensed residential facility. Upon notification that the offender is released to a permanent address, the disclosures permitted or required by law shall be made (Minn. Stat. § 244.052, Subd. 4). Data regarding the victim or witnesses shall not be disclosed (Minn. Stat. § 244.052, Subd. 4(e)).

The broadest disclosures authorized under Minn. Stat. § 244.052, Subd. 4 may still be made for certain offenders (sexually dangerous persons or persons with a sexual psychopathic personality) even though still residing in a residential facility (Minn. Stat. § 253D.32, Subd. 1).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Registered Predatory Offender

325.6 DISCLOSURE TO LOCAL WELFARE AGENCY

Upon request, members may disclose the status of an individual as a predatory offender to a child protection worker who is conducting an assessment of child safety, risk of subsequent child maltreatment, and family strengths and needs under Chapter 260E (Minn. Stat. § 243.166).

Major Incident Notification

326.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members of this department in determining when, how and to whom notification of major incidents should be made.

326.2 POLICY

The South Saint Paul Police Department recognizes that certain incidents should be brought to the attention of supervisors or other specified personnel of this department to facilitate the coordination of activities and ensure that inquiries from the media and the public may be properly addressed.

326.3 MINIMUM CRITERIA FOR NOTIFICATION

Most situations where the media show a strong interest are also of interest to the Chief of Police and the affected Division Commander. The following list of incident types is provided as a guide for notification and is not intended to be all inclusive:

- Homicides.
- Traffic collisions with fatalities.
- Officer-involved shooting, whether on- or off-duty (See Officer-Involved Shootings and Deaths Policy for special notifications).
- Significant injury or death to an employee, whether on- or off-duty.
- Death of a prominent South Saint Paul official.
- Arrest of Department employee or prominent South Saint Paul official.
- Aircraft crash with major damage and/or injury or death.
- In-custody deaths.
- Any other incident, which has or is likely to attract significant media attention.

326.4 SUPERVISOR RESPONSIBILITIES

The Sergeant or OIC is responsible for making the appropriate notifications. They shall make reasonable attempts to obtain as much information on the incident as possible before notification and shall attempt to make the notifications as soon as practicable.

326.4.1 STAFF NOTIFICATION

In the event an incident occurs as identified in the Minimum Criteria for Notification, the Chief of Police shall be notified along with the affected Division Commander and the Investigations Division Commander if that division is providing assistance.

326.4.2 INVESTIGATOR NOTIFICATION

If the incident requires that an investigator respond from home, the immediate supervisor of the appropriate detail shall be contacted.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Major Incident Notification

326.4.3 POLICE CHIEF (PIO)

The Police Chief shall be called after members of staff have been notified that it appears the media may have a significant interest in the incident.

Death Investigation

328.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for situations where officers initially respond to and investigate the circumstances of a deceased person.

Some causes of death may not be readily apparent and some cases differ substantially from what they appeared to be initially. The thoroughness of death investigations and the use of appropriate resources and evidence gathering techniques is critical.

328.2 INVESTIGATION CONSIDERATIONS

Death investigation cases require certain actions be taken. Emergency Medical Services shall be called in all suspected death cases unless the death is obvious (e.g., decapitated or decomposed). Peace officers are not authorized to pronounce death unless they are also Coroners or deputy coroners. A supervisor shall be notified in all death investigations.

328.2.1 MEDICAL EXAMINER REQUEST

The Medical Examiner shall be called in all sudden or unexpected deaths or deaths due to other than natural causes, including, but not limited to (Minn. Stat. § 390.11):

- (a) Unnatural deaths, including violent deaths arising from homicide, suicide or accident.
- (b) Deaths due to a fire or associated with burns or chemical, electrical or radiation injury.
- (c) Unexplained or unexpected perinatal and postpartum maternal deaths.
- (d) Deaths under suspicious, unusual or unexpected circumstances.
- (e) Deaths of persons whose bodies are to be cremated or otherwise disposed of so that the bodies will later be unavailable for examination.
- (f) Deaths of inmates of public institutions and persons in custody of law enforcement officers who have not been hospitalized primarily for organic disease.
- (g) Deaths that occur during, in association with or as the result of diagnostic, therapeutic or anesthetic procedures.
- (h) Deaths due to culpable neglect.
- (i) Stillbirths of 20 weeks or longer gestation unattended by a physician.
- (j) Sudden deaths of persons not affected by recognizable disease.
- (k) Unexpected deaths of persons notwithstanding a history of underlying disease.
- (l) Deaths in which a fracture of a major bone, such as a femur, humerus or tibia, has occurred within the past six months.
- (m) Deaths unattended by a physician occurring outside of a licensed health care facility or licensed residential hospice program.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Death Investigation

- (n) Deaths of persons not seen by their physician within 120 days of demise.
- (o) Deaths of persons occurring in an emergency department.
- (p) Stillbirths or deaths of newborn infants in which there has been maternal use of or exposure to unprescribed controlled substances, including street drugs, or in which there is a history or evidence of maternal trauma.
- (q) Unexpected deaths of children.
- (r) Solid organ donors.
- (s) Unidentified bodies.
- (t) Skeletonized remains.
- (u) Unexpected deaths occurring within 24 hours of arrival at a health care facility.
- (v) Deaths associated with the decedent's employment.
- (w) Deaths of non-registered hospice patients or patients in non-licensed hospice programs.
- (x) Deaths attributable to acts of terrorism.

328.2.2 SEARCHING DEAD BODIES

The Medical Examiner or his/her assistants and authorized investigators are generally the only persons permitted to move, handle or search a dead body (Minn. Stat. § 390.221).

An officer shall make a reasonable search of an individual who it is reasonable to believe is dead, or near death, for information identifying the individual as an organ donor or as an individual who made a refusal. If a donor document is located, the Medical Examiner shall be promptly notified (Minn. Stat. § 525A.12).

Should exigent circumstances indicate to an officer that any other search of a known dead body is warranted prior to the arrival of the Medical Examiner, the investigating officer shall first obtain verbal consent from the Medical Examiner.

The Medical Examiner is required to release property or articles to law enforcement that are necessary for conducting an investigation unless reasonable basis exists pursuant to Minn. Stat. § 390.225 Subd. 2 to not release the property or articles (Minn. Stat. § 390.221).

Whenever reasonably possible, a witness, preferably a relative of the deceased or a member of the household, should be requested to remain nearby the scene and available to the officer, pending the arrival of the Medical Examiner.

The name and address of this person shall be included in the narrative of the death report. Whenever personal effects are removed from the body of the deceased by the Medical Examiner, a receipt shall be obtained. This receipt shall be attached to the death report.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Death Investigation

328.2.3 DEATH NOTIFICATION

When practicable, and if not handled by the Medical Examiner, notification to the next-of-kin of the deceased person shall be made, in person, by the officer assigned to the incident. If the next-of-kin lives in another jurisdiction, a law enforcement official from that jurisdiction shall be requested to make the personal notification. If the relatives live outside this county, the Medical Examiner may be requested to make the notification. The Medical Examiner needs to know if notification has been made. Assigned investigators may need to talk to the next-of-kin.

If a deceased person has been identified as a missing person, this department shall attempt to locate family members and inform them of the death and the location of the deceased missing person's remains. All efforts to locate and notify family members shall be recorded in appropriate reports and properly retained (Minn. Stat. § 390.25 Subd. 2 (b)).

This department shall immediately notify the state fire marshal or South Saint Paul's chief officer (if that position exists) when a human death results from a fire, (Minn. Stat. § 299F.04 Subd. 5 (b)).

328.2.4 UNIDENTIFIED DEAD BODIES

If the identity of a dead body cannot be established after the Medical Examiner arrives, the Medical Examiner will issue a "John Doe" or "Jane Doe" number for the report.

328.2.5 UNIDENTIFIED BODIES DATA ENTRY

As soon as reasonably possible, but no later than 30 working days after the date a death is reported to the Department, any information or items pertaining to identifying features of the unidentified body, dental records, fingerprints, any unusual physical characteristics, description of clothing or personal belongings found on or with the body, that are in the possession of SSP PD shall be forwarded to the Medical Examiner for transmission to the BCA for eventual entry into systems designed to assist in the identification process, such as the Missing Children and Missing Persons Information Clearinghouse and the National Crime Information Center (NCIC) files (Minn. Stat. § 390.25 Subd. 2 (a)).

328.2.6 DEATH INVESTIGATION REPORTING

All incidents involving a death shall be documented on the appropriate form.

328.2.7 SUSPECTED HOMICIDE

If the initially assigned officer suspects that the death involves a homicide or other suspicious circumstances, the officer shall take steps to protect the scene and the Investigative Division shall be notified to determine the possible need for an investigator to respond to the scene for further immediate investigation.

If the on-scene supervisor, through consultation with the Investigations supervisor, is unable to determine the manner of death, the investigation shall proceed as though it is a homicide.

The investigator of a homicide or suspicious-circumstances death may, with the approval of his/her supervisor, request the Medical Examiner to conduct physical examinations and tests and provide a report with the costs borne by the Department (Minn. Stat. § 390.251).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Death Investigation

328.2.8 EMPLOYMENT RELATED DEATHS OR INJURIES

Any member of this agency who responds to and determines that a death, serious illness or serious injury has occurred as a result of an accident at or in connection with the victim's employment, should ensure that the nearest office of the Minnesota Department of Labor and Industry is notified with all pertinent information.

Identity Theft

329.1 PURPOSE AND SCOPE

Identity theft is a growing trend that frequently involves related crimes in multiple jurisdictions. This policy is intended to provide guidelines for the reporting and investigation of such crimes.

329.2 REPORTING

- (a) A report shall be taken any time a person living within the jurisdiction of the South Saint Paul Police Department reports that he/she has been a victim of identity theft (Minn. Stat. § 609.527, Subd. 5). This includes:
 - 1. Taking a report even if the location of the crime is outside the jurisdiction of this department or has not been determined.
 - 2. Providing the victim with department information, as set forth in the Victim and Witness Assistance Policy. Officers should encourage the individual to review the material, and assist with any questions.
- (b) A report should also be taken if a person living outside the department jurisdiction reports an identity theft that may have been committed or facilitated within this jurisdiction (e.g., use of a post office box in South Saint Paul to facilitate the crime).
- (c) Officers should include all known incidents of fraudulent activity (e.g., credit card number applied for in victim's name when the victim has never made such an application).
- (d) Officers should also cross-reference all known reports made by the victim (e.g., U.S. Secret Service, credit reporting bureaus, U.S. Postal Service and the Department of Public Safety's Driver and Vehicle Services Division) with all known report numbers.
- (e) Following supervisory review and Department processing, the initial report should be forwarded to the appropriate investigator for follow-up investigation, coordination with other agencies and prosecution as circumstances dictate.

329.3 PREVENTATIVE MEASURES

The victim should be advised to place a security freeze on his/her consumer report as allowed by law (Minn. Stat. § 13C.016 Subd. 2). A victim may also access the Minnesota Attorney General's office for additional detailed information.

329.4 VICTIM DATA

The victim may be provided the Consent to Create an FBI Identity Theft File Form and a Notice About Providing Your Social Security Number. These completed forms should be submitted to the Records Section for appropriate filing and entry into the NCIC Identity Theft File. Forms and details are available on the Bureau of Criminal Apprehension identity theft website.

329.5 INFORMATION

The victim should also be encouraged to contact the Federal Trade Commission (FTC), which is responsible for receiving and processing complaints under the Identity Theft and Assumption

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Identity Theft

Deterrence Act. The victim can contact the FTC online or by telephone. Additional information may be found at the U.S. Department of Justice (USDOJ) website.

Private Persons Arrests

330.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the handling of private person's arrests made pursuant to Minn. Stat. § 629.30 Subd. 2 (4).

330.2 ADVISING PRIVATE PERSONS OF THE ARREST PROCESS

All officers shall advise civilians of the right to make a private person's arrest, including advice on how to safely execute such an arrest. In all situations, officers should use sound discretion in determining whether to advise an individual of the arrest process.

- (a) When advising any individual regarding the right to make a private person's arrest, officers should refrain from encouraging or dissuading any individual from making such an arrest and should instead limit advice to the legal requirements for such an arrest, as listed below.
- (b) Private individuals should be discouraged from using force to effect a private person's arrest. Absent immediate threat to their own safety or the safety of others, private individuals should be encouraged to refer matters to law enforcement officials for further investigation or arrest.
- (c) Private individuals shall be informed of the requirement to take the arrested person before a judge or to a peace officer without unnecessary delay (Minn. Stat. § 629.39).

330.3 ARRESTS BY PRIVATE PERSONS

A private person may arrest another under the following circumstances (Minn. Stat. § 629.37):

- (a) For a public offense committed or attempted in his/her presence.
- (b) When the person arrested has committed a felony, although not in his/her presence.
- (c) When a felony has been committed and he/she has reasonable cause for believing the person to be arrested committed the felony.
- (d) When directed by a judge or a peace officer to arrest another person (Minn. Stat. § 629.403).

330.4 OFFICER RESPONSIBILITIES

Any officer presented with a private person wishing to make an arrest must determine whether there is reasonable cause to believe that such an arrest would be lawful.

- (a) Should any officer determine that there is no reasonable cause to believe that a private person's arrest is lawful, the officer should take no action to further detain or restrain the individual beyond that which reasonably appears necessary to investigate the matter, determine the lawfulness of the arrest and protect the public safety.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Private Persons Arrests

1. Any officer who determines that a private person's arrest appears to be unlawful should promptly release the arrested individual. The officer must include the basis of such a determination in a related report.
 2. Absent reasonable cause to support a private person's arrest or other lawful grounds to support an independent arrest by the officer, the officer should advise the parties that no arrest will be made and that the circumstances will be documented in a related report.
- (b) Whenever an officer determines that there is reasonable cause to believe that a private person's arrest is lawful, the officer may exercise any of the following options:
1. Take the individual into physical custody for booking.
 2. Release the individual upon a misdemeanor citation or pending formal charges.

330.5 REPORTING REQUIREMENTS

In all circumstances in which a private person is claiming to have made an arrest, the individual must provide a recorded statement detailing the circumstances of the incident. If the person fails or refuses to do so the arrest subject shall be released unless the officer has an independent reason to take the person into custody.

In addition to the citizen's recorded statement, officers shall complete a narrative report regarding the circumstances and disposition of the incident.

Limited English Proficiency Services

331.1 PURPOSE AND SCOPE

This policy provides guidance to members when communicating with individuals with limited English proficiency (LEP) (42 USC § 2000d).

331.1.1 DEFINITIONS

Definitions related to this policy include:

Authorized interpreter - A person who has been screened and authorized by the Department to act as an interpreter and/or translator for others.

Interpret or interpretation - The act of listening to a communication in one language (source language) and orally converting it to another language (target language), while retaining the same meaning.

Limited English proficient (LEP) - Any individual whose primary language is not English and who has a limited ability to read, write, speak or understand English. These individuals may be competent in certain types of communication (e.g., speaking or understanding) but still be LEP for other purposes (e.g., reading or writing). Similarly, LEP designations are context-specific; an individual may possess sufficient English language skills to function in one setting but these skills may be insufficient in other situations. This includes individuals who, because of difficulty in speaking or comprehending the English language, cannot fully understand any charges made against them, the seizure of their property, or they are incapable of presenting or assisting in the presentation of a defense (Minn. Stat. § 611.31).

Qualified bilingual member - A member of the South Saint Paul Police Department, designated by the Department, who has the ability to communicate fluently, directly and accurately in both English and another language. Bilingual members may be fluent enough to communicate in a non-English language but may not be sufficiently fluent to interpret or translate from one language into another.

Translate or translation - The replacement of written text from one language (source language) into an equivalent written text (target language).

331.2 POLICY

It is the policy of the South Saint Paul Police Department to reasonably ensure that LEP individuals have meaningful access to law enforcement services, programs and activities, while not imposing undue burdens on its members.

The Department will not discriminate against or deny any individual access to services, rights or programs based upon national origin or any other protected interest or right.

331.3 LEP COORDINATOR

The Chief of Police shall designate the Operations Division Commander to act as the Department's LEP Coordinator.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Limited English Proficiency Services

The responsibilities of the LEP Coordinator include, but are not limited to:

- (a) Coordinating and implementing all aspects of the South Saint Paul Police Department's LEP services to LEP individuals.
- (b) Developing procedures that will enable members to access LEP services, including telephonic interpreters, and ensuring the procedures are available to all members.
- (c) Ensuring that a list of all qualified bilingual members and authorized interpreters is maintained and available to each Supervisor. The list should include information regarding the following:
 - 1. Languages spoken
 - 2. Contact information
 - 3. Availability
- (d) Ensuring signage stating that interpreters are available free of charge to LEP individuals is posted in appropriate areas and in the most commonly spoken languages.
- (e) Reviewing existing and newly developed documents to determine which are vital documents and should be translated, and into which languages the documents should be translated.
- (f) Annually assessing demographic data and other resources, including contracted language services utilization data and community-based organizations, to determine if there are additional documents or languages that are appropriate for translation.
- (g) Identifying standards and assessments to be used by the Department to qualify individuals as qualified bilingual members or authorized interpreters.
- (h) Periodically reviewing efforts of the Department in providing meaningful access to LEP individuals, and, as appropriate, developing reports, new procedures or recommending modifications to this policy.
- (i) Receiving and responding to complaints regarding department LEP services.
- (j) Ensuring appropriate processes are in place to provide for the prompt and equitable resolution of complaints and inquiries regarding discrimination in access to department services, programs and activities.

331.4 FOUR-FACTOR ANALYSIS

Since there are many different languages that members could encounter, the Department will utilize the four-factor analysis outlined in the U.S. Department of Justice (DOJ) Guidance to Federal Financial Assistance Recipients, available at the DOJ website, to determine which measures will provide meaningful access to its services and programs. It is recognized that law enforcement contacts and circumstances will vary considerably. This analysis, therefore, must remain flexible and will require an ongoing balance of four factors, which are:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Limited English Proficiency Services

- (a) The number or proportion of LEP individuals eligible to be served or likely to be encountered by department members, or who may benefit from programs or services within the jurisdiction of the Department or a particular geographic area.
- (b) The frequency with which LEP individuals are likely to come in contact with department members, programs or services.
- (c) The nature and importance of the contact, program, information or service provided.
- (d) The cost of providing LEP assistance and the resources available.

331.5 TYPES OF LEP ASSISTANCE AVAILABLE

South Saint Paul Police Department members should never refuse service to an LEP individual who is requesting assistance, nor should they require an LEP individual to furnish an interpreter as a condition for receiving assistance. The Department will make every reasonable effort to provide meaningful and timely assistance to LEP individuals through a variety of services.

The Department will utilize all reasonably available tools, such as language identification cards, when attempting to determine an LEP individual's primary language.

LEP individuals may choose to accept department-provided LEP services at no cost or they may choose to provide their own.

Department-provided LEP services may include, but are not limited to, the assistance methods described in this policy.

331.6 WRITTEN FORMS AND GUIDELINES

Vital documents or those that are frequently used should be translated into languages most likely to be encountered. The LEP Coordinator will arrange to make these translated documents available to members and other appropriate individuals, as necessary.

331.7 AUDIO RECORDINGS

The Department may develop audio recordings of important or frequently requested information in a language most likely to be understood by those LEP individuals who are representative of the community being served.

331.8 QUALIFIED BILINGUAL MEMBERS

Bilingual members may be qualified to provide LEP services when they have demonstrated through established department procedures a sufficient level of skill and competence to fluently communicate in both English and a non-English language. Members utilized for LEP services must demonstrate knowledge of the functions of an interpreter/translator and the ethical issues involved when acting as a language conduit. Additionally, bilingual members must be able to communicate technical and law enforcement terminology, and be sufficiently proficient in the non-English language to perform complicated tasks, such as conducting interrogations, taking statements, collecting evidence or conveying rights or responsibilities.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Limited English Proficiency Services

When a qualified bilingual member from this department is not available, personnel from other City departments, who have been identified by the Department as having the requisite skills and competence, may be requested.

331.9 AUTHORIZED INTERPRETERS

Any person designated by the Department to act as an authorized interpreter and/or translator must have demonstrated competence in both English and the involved non-English language, must have an understanding of the functions of an interpreter that allows for correct and effective translation, and should not be a person with an interest in the department case or investigation involving the LEP individual. A person providing interpretation or translation services may be required to establish the accuracy and trustworthiness of the interpretation or translation in a court proceeding.

Authorized interpreters must pass a screening process established by the LEP Coordinator which demonstrates that their skills and abilities include:

- (a) The competence and ability to communicate information accurately in both English and in the target language.
- (b) Knowledge, in both languages, of any specialized terms or concepts peculiar to this department and of any particularized vocabulary or phraseology used by the LEP individual.
- (c) The ability to understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.
- (d) Knowledge of the ethical issues involved when acting as a language conduit.

331.9.1 SOURCES OF AUTHORIZED INTERPRETERS

The Department may contract with authorized interpreters who are available over the telephone. Members may use these services with the approval of a supervisor and in compliance with established procedures.

Other sources may include:

- Qualified bilingual members of this department or personnel from other City departments.
- Individuals employed exclusively to perform interpretation services.
- Contracted in-person interpreters, such as state or federal court interpreters, among others.
- Interpreters from other agencies who have been qualified as interpreters by this department, and with whom the Department has a resource-sharing or other arrangement that they will interpret according to department guidelines.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Limited English Proficiency Services

331.9.2 COMMUNITY VOLUNTEERS AND OTHER SOURCES OF LANGUAGE ASSISTANCE

Language assistance may be available from community volunteers who have demonstrated competence in either monolingual (direct) communication and/or in interpretation or translation (as noted in above), and have been approved by the Department to communicate with LEP individuals.

Where qualified bilingual members or other authorized interpreters are unavailable to assist, approved community volunteers who have demonstrated competence may be called upon when appropriate. However, department members must carefully consider the nature of the contact and the relationship between the LEP individual and the volunteer to ensure that the volunteer can provide neutral and unbiased assistance.

While family or friends of an LEP individual may offer to assist with communication or interpretation, members should carefully consider the circumstances before relying on such individuals. For example, children should not be relied upon except in exigent or very informal and non-confrontational situations.

331.10 CONTACT AND REPORTING

While all law enforcement contacts, services and individual rights are important, this department will utilize the four-factor analysis to prioritize service to LEP individuals so that such services may be targeted where they are most needed, according to the nature and importance of the particular law enforcement activity involved.

Whenever any member of this department is required to complete a report or other documentation, and interpretation services are provided to any involved LEP individual, such services should be noted in the related report. Members should document the type of interpretation services utilized and whether the individual elected to use services provided by the Department or some other identified source.

331.11 RECEIVING AND RESPONDING TO REQUESTS FOR ASSISTANCE

The South Saint Paul Police Department will take reasonable steps and will work with the Department of Human Resources to develop in-house language capacity by hiring or appointing qualified members proficient in languages representative of the community being served.

331.12 FIELD ENFORCEMENT

Field enforcement will generally include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, crowd/traffic control and other routine field contacts that may involve LEP individuals. The scope and nature of these activities and contacts will inevitably vary. Members and/or supervisors must assess each situation to determine the need and availability of language assistance to all involved LEP individuals and utilize the methods outlined in this policy to provide such assistance.

Although not every situation can be addressed in this policy, it is important that members are able to effectively communicate the reason for a contact, the need for information and the meaning

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Limited English Proficiency Services

or consequences of any enforcement action. For example, it would be meaningless to request consent to search if the officer is unable to effectively communicate with an LEP individual.

If available, officers should obtain the assistance of a qualified bilingual member or an authorized interpreter before placing an LEP individual under arrest.

331.13 INVESTIGATIVE FIELD INTERVIEWS

In any situation where an interview may reveal information that could be used as the basis for arrest or prosecution of an LEP individual and a qualified bilingual member is unavailable or lacks the skills to directly communicate with the LEP individual, an authorized interpreter should be used. This includes interviews conducted during an investigation with victims, witnesses and suspects. In such situations, audio recordings of the interviews should be made when reasonably possible. Identification and contact information for the interpreter (e.g., name, address) should be documented so that the person can be subpoenaed for trial if necessary.

If an authorized interpreter is needed, officers should consider calling for an authorized interpreter in the following order:

- An authorized department member or allied agency interpreter
- An authorized telephone interpreter
- Any other authorized interpreter

Any *Miranda* warnings shall be provided to suspects in their primary language by an authorized interpreter or, if the suspect is literate, by providing a translated *Miranda* warning card.

The use of an LEP individual's bilingual friends, family members, children, neighbors or bystanders may be used only when a qualified bilingual member or authorized interpreter is unavailable and there is an immediate need to interview an LEP individual.

331.14 CUSTODIAL INTERROGATIONS

Miscommunication during custodial interrogations may have a substantial impact on the evidence presented in a criminal prosecution. Only qualified bilingual members or, if none is available or appropriate, authorized interpreters shall be used during custodial interrogations. *Miranda* warnings shall be provided to suspects in their primary language by the qualified bilingual member or an authorized interpreter.

In order to ensure that translations during custodial interrogations are accurately documented and are admissible as evidence, interrogations should be recorded whenever reasonably possible. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

331.14.1 OTHER TIMING AND NOTIFICATION MANDATES

The investigating or arresting officer shall immediately make necessary contacts to get an authorized interpreter for an in-custody LEP person at the earliest possible time in order to assist the person throughout the interrogation or taking of a statement. This applies even when the interrogation will be conducted by a bilingual member (Minn. Stat. § 611.32).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Limited English Proficiency Services

The following shall be explained to the LEP person with the assistance of the authorized interpreter (Minn. Stat. § 611.32):

- (a) All charges filed against the person
- (b) All procedures relating to the person's detainment and release
- (c) In the case of any seizure under the provisions of the Asset Forfeiture Policy:
 - 1. The possible consequences of the seizure
 - 2. The person's right to judicial review

331.15 BOOKINGS

When gathering information during the booking process, members should remain alert to the impediments that language barriers can create. In the interest of the arrestee's health and welfare, the safety and security of the facility, and to protect individual rights, it is important that accurate medical screening and booking information be obtained. Members should seek the assistance of a qualified bilingual member whenever there is concern that accurate information cannot be obtained or that booking instructions may not be properly understood by an LEP individual.

331.16 COMPLAINTS

The Department shall ensure that LEP individuals who wish to file a complaint regarding members of this department are able to do so. The Department may provide an authorized interpreter or translated forms, as appropriate. Complaints will be referred to the LEP Coordinator.

Investigations into such complaints shall be handled in accordance with the Personnel Complaints Policy. Authorized interpreters used for any interview with an LEP individual during an investigation should not be members of this department.

Any notice required to be sent to an LEP individual as a complaining party pursuant to the Personnel Complaints Policy should be translated or otherwise communicated in a language-accessible manner.

331.17 COMMUNITY OUTREACH

Community outreach programs and other such services offered by this department are important to the ultimate success of more traditional law enforcement duties. This department will continue to work with community groups, local businesses and neighborhoods to provide equal access to such programs and services.

331.18 TRAINING

To ensure that all members who may have contact with LEP individuals are properly trained, the Department will provide periodic training on this policy and related procedures, including how to access department-authorized telephonic and in-person interpreters and other available resources.

The Support Services Commander shall be responsible for ensuring new members receive LEP training. Those who may have contact with LEP individuals should receive refresher training at

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Limited English Proficiency Services

least once every two years thereafter. The Support Services Commander shall maintain records of all LEP training provided, and will retain a copy in each member's training file in accordance with established records retention schedules.

Pupil Arrest Reporting

333.1 PURPOSE AND SCOPE

The purpose of this policy is to describe the procedures to follow when a pupil is arrested on school grounds and during school hours.

333.2 PUPIL ARREST REPORTING

In the event a school pupil is arrested, the arresting officer shall include the necessary information in the report to ensure that the Records Section notifies the chief administrative officer of the school, or an appropriate designee, of the pupil's arrest.

If there is probable cause to believe an incident involved alcohol or a controlled substance, the arresting officer shall complete the appropriate form and submit the form with the report to the Records Section. The Records Section shall ensure the form is distributed to the chemical abuse pre-assessment team of the school within two weeks of the occurrence (Minn. Stat. § 121A.28).

333.2.1 PUPIL ARREST AFTER NOTIFICATION

Based upon the circumstances of the investigation, it may be appropriate to notify the school prior to the arrest. Prior notification and assistance from the school, may reduce disruption to school operations and other students.

333.2.2 PUPIL ARREST BEFORE NOTIFICATION

Based upon the circumstances of the investigation, it may be appropriate to arrest the pupil before notifying the school. This may be appropriate if the pupil is a flight risk, if prior notification will impede the investigation or if notification creates additional risks to students, faculty, the officer or the public.

Proper notification to the school after the pupil's arrest should then be made when circumstances reasonably allow.

333.2.3 PARENTAL NOTIFICATION

Upon arrest, it is the arresting officer's responsibility to ensure the parents of the arrested pupil are properly notified. Notification shall be made by the officer, regardless of subsequent notifications by the juvenile detention facility. Notifications should be documented and include the charges against the pupil and where the pupil will be taken.

Biological Samples

334.1 PURPOSE AND SCOPE

This policy provides guidelines for the collection of biological samples from those individuals required to provide samples upon conviction for certain offenses. This policy does not apply to biological samples collected at a crime scene or taken from a person in conjunction with a criminal investigation. Nor does it apply to biological samples collected from those required to register, for example, as sex offenders.

334.2 POLICY

The South Saint Paul Police Department will assist in the expeditious collection of required biological samples from offenders in accordance with the laws of this state and with as little reliance on force as practicable.

334.3 PERSONS SUBJECT TO BIOLOGICAL SAMPLE COLLECTION

The following persons must submit a biological sample:

- (a) Adults who are subject to a court order requiring a biological sample after sentencing (Minn. Stat. § 609.117).
- (b) Juveniles who are subject to a court order requiring a biological sample after being adjudicated delinquent (Minn. Stat. § 609.117).

334.4 PROCEDURE

When an individual is required to provide a biological sample, a trained employee shall attempt to obtain the sample in accordance with this policy.

334.4.1 COLLECTION

The following steps should be taken to collect a sample:

- (a) Verify that the individual is required to provide a sample pursuant to Minn. Stat. § 609.117.
- (b) Verify that a biological sample has not been previously collected from the offender by querying the person's criminal history. There is no need to obtain a biological sample if one has been previously obtained.
- (c) Use the designated collection kit provided by the Minnesota Bureau of Criminal Apprehension to perform the collection and take steps to avoid cross contamination.

334.5 USE OF FORCE TO OBTAIN SAMPLES

If a person refuses to cooperate with the sample collection process, officers should attempt to identify the reason for refusal and seek voluntary compliance without resorting to using force. Force will not be used in the collection of samples except as authorized by court order or approval of legal counsel and only with the approval of a supervisor. Methods to consider when seeking voluntary compliance include contacting:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Biological Samples

- (a) The person's parole or probation officer when applicable.
- (b) The prosecuting attorney to seek additional charges against the person for failure to comply or to otherwise bring the refusal before a judge.
- (c) The judge at the person's next court appearance.
- (d) The person's attorney.
- (e) A chaplain.
- (f) Another custody facility with additional resources, where an arrestee can be transferred to better facilitate sample collection.
- (g) A supervisor who may be able to authorize custodial disciplinary actions to compel compliance, if any are available.

The supervisor shall review and approve any plan to use force and be present to document the process.

334.5.1 VIDEO RECORDING

A video recording should be made any time force is used to obtain a biological sample. The recording should document all staff participating in the process, in addition to the methods and all force used during the collection. The recording should be part of the investigation file, if any, or otherwise retained in accordance with the department's records retention schedule.

Chaplains

335.1 PURPOSE AND SCOPE

This policy establishes the guidelines for South Saint Paul Police Department chaplains to provide counseling or emotional support to members of the Department, their families and members of the public.

335.2 POLICY

The South Saint Paul Police Department shall ensure that department chaplains are properly appointed, trained and supervised to carry out their responsibilities without financial compensation.

335.3 ELIGIBILITY

Requirements for participation as a chaplain for the Department may include, but are not limited to:

- (a) Being above reproach, temperate, prudent, respectable, hospitable, able to teach, be free from addiction to alcohol or other drugs and excessive debt.
- (b) Managing their households, families and personal affairs well.
- (c) Having a good reputation in the community.
- (d) Successful completion of an appropriate-level background investigation.
- (e) Possession of a valid driver's license.

The Chief of Police may apply exceptions for eligibility based on organizational needs and the qualifications of the individual.

335.4 REQUIREMENTS

Candidates for the Chaplain Program shall meet the following requirements before formally being designated as a Law Enforcement Chaplain:

- (a) Must be ecclesiastically certified and/or endorsed, ordained, licensed or commissioned by a recognized religious body.
- (b) Must have some successful ministry experience within a recognized faith community and / or a law enforcement background.
- (c) Membership in good standing with the International Conference of Police Chaplains (ICPC) or any other recognized Chaplain groups, organizations and trainings.

335.4.1 RECRUITMENT

Chaplains should be recruited on a continuous and ongoing basis consistent with department policy on equal opportunity and nondiscriminatory employment. A primary qualification for participation in the application process should be an interest in and an ability to assist the Department in serving the public. Chaplain candidates are encouraged to participate in ride-alongs with department members before and during the selection process.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Chaplains

335.4.2 SELECTION AND APPOINTMENT

Chaplain candidates shall successfully complete the following process prior to appointment as a chaplain:

- (a) Submit the appropriate written application.
- (b) Include a recommendation from employers or volunteer programs.
- (c) Interview with the Chief of Police and the chaplain coordinator.
- (d) Successfully complete an appropriate-level background investigation.
- (e) Complete an appropriate probationary period as designated by the Chief of Police.

Chaplains are volunteers and serve at the discretion of the Chief of Police. Chaplains shall have no property interest in continued appointment. However, if a chaplain is removed for alleged misconduct, the chaplain will be afforded an opportunity solely to clear his/her name through a liberty interest hearing, which shall be limited to a single appearance before the Chief of Police or the authorized designee.

335.5 IDENTIFICATION AND UNIFORMS

As representatives of the Department, chaplains are responsible for presenting a professional image to the community. Chaplains shall dress appropriately for the conditions and performance of their duties. Uniforms and necessary safety equipment will be provided for each chaplain. Identification symbols worn by chaplains shall be different and distinct from those worn by officers through the inclusion of "Chaplain" on the uniform and not reflect any religious affiliation.

Chaplains will be issued South Saint Paul Police Department identification cards, which must be carried at all times while on-duty. The identification cards will be the standard South Saint Paul Police Department identification cards, with the exception that "Chaplain" will be indicated on the cards. Chaplains shall be required to return any issued uniforms or department property at the termination of service.

Chaplains shall conform to all uniform regulations and appearance standards of this policy.

335.6 DUTIES AND RESPONSIBILITIES

Chaplains are volunteer members of the Department, and except as otherwise specified within this policy, are required to comply with the Volunteer Program Policy in this manual and other applicable Department policies. The duties of a chaplain include, but are not limited to, the following:

- (a) Assisting in making notification to families of Department members who have been seriously injured or killed.
- (b) After notification, responding to the hospital or home of the Department member.
- (c) Visiting sick or injured law enforcement personnel in the hospital or at home.
- (d) Attending and participating, when requested, in funerals of active or retired members of the Department.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Chaplains

- (e) Assisting other personnel in the diffusion of a conflict or incident when requested to by on-scene staff.
- (f) Responding to natural and accidental deaths, suicides and attempted suicides, family disturbances and any other incident that, in the judgment of the Supervisor, aids in accomplishing the mission of the Department.
- (g) Being on call, and if possible on-duty, during major demonstrations or any public function that requires the presence of a large number of Department personnel.
- (h) Attending Department and academy graduations, ceremonies and social events and offering invocations and benedictions, as requested.
- (i) Responding to all major disasters, such as floods, bombings and similar critical incidents.
- (j) Providing liaison with various religious leaders of the community.
- (k) Assisting public safety personnel and the community in any other function of the clergy profession as requested.
- (l) Participating in in-service training classes.
- (m) Willing to train to enhance effectiveness.
- (n) Promptly facilitating requests for representatives or leaders of other denominations.
- (o) Making referrals in cases where specialized attention is needed, or in those cases that are beyond the chaplain's ability to assist.

Chaplains may not proselytize or attempt to recruit members of the department or the public into a religious affiliation while on-duty unless the receiving person has solicited spiritual guidance or teaching. If there is any question as to the receiving person's intent, chaplains should verify that the person is desirous of spiritual counseling or guidance before engaging in such discussion.

Chaplains may not accept gratuities for any service or any subsequent actions and follow-up provided while functioning as a chaplain for the South Saint Paul Police Department.

335.7 DUTIES AND RESPONSIBILITIES

Chaplains assist the Department, its members and the community, as needed. Assignments of chaplains will usually be to augment the Patrol Division. Chaplains may be assigned to other areas within the Department as needed. Chaplains should be placed only in assignments or programs that are consistent with their knowledge, skills, abilities and the needs of the Department.

All chaplains will be assigned to duties by the chaplain coordinator or the authorized designee.

Chaplains may not proselytize or attempt to recruit members of the Department or the public into a religious affiliation while representing themselves as chaplains with this department. If there is any question as to the receiving person's intent, chaplains should verify that the person is desirous of spiritual counseling or guidance before engaging in such discussion.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Chaplains

Chaplains may not accept gratuities for any service or any subsequent actions or follow-up contacts that were provided while functioning as a chaplain for the South Saint Paul Police Department.

335.7.1 COMPLIANCE

Chaplains are volunteer members of this department, and except as otherwise specified within this policy, are required to comply with the Volunteer Program Policy and other applicable policies.

335.7.2 OPERATIONAL GUIDELINES

- (a) Chaplains will be scheduled to be on-call for a period of seven consecutive days during each month, beginning on Monday and ending on the following Sunday.
- (b) Generally, each chaplain will serve with South Saint Paul Police Department personnel a minimum of eight hours per month.
- (c) At the end of each watch the chaplain will complete a chaplain shift report and submit it to the Chief of Police or the authorized designee.
- (d) Chaplains shall be permitted to ride with officers during any shift and observe South Saint Paul Police Department operations, provided the Sergeant has been notified and has approved the activity.
- (e) Chaplains shall not be evaluators of members of the Department.
- (f) In responding to incidents a chaplain shall never function as an officer.
- (g) When responding to in-progress calls for service chaplains may be required to stand-by in a secure area until the situation has been deemed safe.
- (h) Chaplains shall serve only within the jurisdiction of the South Saint Paul Police Department unless otherwise authorized by the Chief of Police or the authorized designee.
- (i) Each chaplain shall have access to current department member rosters, addresses, telephone numbers, duty assignments and other information that may assist in his/her duties. Such information will be considered private personnel data and each chaplain will exercise appropriate security measures to prevent distribution of the data.

335.7.3 ASSISTING DEPARTMENT/OFFICE MEMBERS

The responsibilities of a chaplain related to department members include, but are not limited to:

- (a) Assisting in making notification to families of members who have been seriously injured or killed and after notification responding to the hospital or home of the member.
- (b) Visiting sick or injured members in the hospital or at home.
- (c) Attending and participating, when requested, in funerals of active or retired members.
- (d) Serving as a resource for members when dealing with the public in incidents, such as accidental deaths, suicides, suicidal subjects, serious accidents, drug and alcohol abuse and other such situations that may arise.
- (e) Providing counseling and support for members and their families.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Chaplains

- (f) Being alert to the needs of members and their families.

335.7.4 ASSISTING THE DEPARTMENT/OFFICE

The responsibilities of a chaplain related to this department include, but are not limited to:

- (a) Assisting members in the diffusion of a conflict or incident when requested.
- (b) Responding to natural and accidental deaths, suicides and attempted suicides, family disturbances and any other incident that in the judgment of the Sergeant or supervisor aids in accomplishing the mission of the Department.
- (c) Responding to all major disasters, such as natural disasters, bombings and similar critical incidents.
- (d) Being on-call and, if reasonably possible, on-duty during major demonstrations or any public function that requires the presence of a large number of department members.
- (e) Attending department and academy graduations, ceremonies and social events and offering invocations and benedictions, as requested.
- (f) Participating in in-service training classes.
- (g) Willingness to train others to enhance the effectiveness of the Department.

335.7.5 ASSISTING THE COMMUNITY

The duties of a chaplain related to the community include, but are not limited to:

- (a) Fostering familiarity with the role of law enforcement in the community.
- (b) Providing an additional link between the community, other chaplain coordinators and the Department.
- (c) Providing liaison with various civic, business and religious organizations.
- (d) Promptly facilitating requests for representatives or leaders of various denominations.
- (e) Assisting the community in any other function as needed or requested.
- (f) Making referrals in cases where specialized attention is needed or in cases that are beyond the chaplain's ability to assist.

335.7.6 CHAPLAIN MEETINGS

All chaplains are required to attend scheduled meetings. Any absences must be satisfactorily explained to the chaplain coordinator.

335.8 COMMAND STRUCTURE

- (a) Under the general direction of the Chief of Police or designee chaplains shall report to the Sergeant who oversees the program.
- (b) The Chief of Police shall make all appointments to the Chaplain Program.
- (c) The Sergeant in charge of the Chaplain Program shall serve as the liaison between the Chaplain Unit and the Chief of Police. He/she will act as chairman of all chaplain meetings, prepare schedules, maintain records on all activities of the Chaplain Unit,

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Chaplains

coordinate activities that may concern the members of the Chaplain Unit and arrange for training classes for chaplains.

335.9 OPERATIONAL GUIDELINES

- (a) Chaplains shall be permitted to ride with officers during any shift and observe South Saint Paul Police Department operations, provided the Sergeant has been notified and has approved the activity.
- (b) Chaplains shall not be evaluators of employees.
- (c) In responding to incidents, a chaplain shall never function as an officer.
- (d) When responding to in-progress calls for service, chaplains may be required to standby in a secure area until the situation has been deemed safe.
- (e) Chaplains shall serve only within the jurisdiction of the South Saint Paul Police Department unless otherwise authorized by the Chief of Police or designee.

Service Animals

336.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines necessary to ensure that the rights of individuals who use service animals to assist with disabilities are protected in accordance with Title II of the Americans with Disabilities Act (ADA).

336.1.1 DEFINITIONS

Definitions related to this policy include:

Service animal - A dog that is trained to do work or perform tasks for the benefit of an individual with a disability, including a physical, sensory, psychiatric, intellectual, or other mental disability. The work or tasks performed by a service animal must be directly related to the individual's disability (28 CFR 35.104; Minn. Stat. § 363A.19 (c)).

Service animal also includes a miniature horse if the horse is trained to do work or perform tasks for people with disabilities, provided the horse is housebroken, is under the handler's control, the facility can accommodate the horse's type, size, and weight, and the horse's presence will not compromise legitimate safety requirements necessary for safe operation of the facility (28 CFR 35.136(i)).

336.2 POLICY

It is the policy of the South Saint Paul Police Department to provide equal access to services, programs, and activities of the Department to persons with service animals. Department members shall protect the rights of persons assisted by service animals in accordance with state and federal law. This protection extends to any person who is training a service dog (Minn. Stat. § 256C.02).

336.3 IDENTIFICATION AND USE OF SERVICE ANIMALS

Service animals that are assisting individuals with disabilities are permitted in all public facilities and areas where the general public is allowed. Department members are expected to treat individuals with service animals with the same courtesy and respect that the South Saint Paul Police Department affords to all members of the public (28 CFR 35.136; Minn. Stat. § 256C.02; Minn. Stat. § 363A.19).

Some service animals may be readily identifiable. However, many do not have a distinctive symbol, harness, or collar.

Service animals may be used in a number of ways to provide assistance including:

- Guiding people who are blind or have low vision.
- Alerting people who are deaf or hard of hearing.
- Retrieving or picking up items, opening doors, or flipping switches for people who have limited use of their hands, arms, or legs.
- Pulling wheelchairs.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Service Animals

- Providing physical support and assisting with stability and balance.
- Doing work or performing tasks for persons with traumatic brain injury, intellectual disabilities, or psychiatric disabilities, such as reminding a person with depression to take medication.
- Alerting a person with anxiety to the onset of panic attacks, providing tactile stimulation to calm a person with post-traumatic stress disorder, assisting people with schizophrenia to distinguish between hallucinations and reality, and helping people with traumatic brain injury to locate misplaced items or follow daily routines.

336.4 INQUIRIES REGARDING SERVICE ANIMALS

If it is apparent or if a member is aware that an animal is a service animal, the individual generally should not be asked any questions as to the status of the animal. If it is unclear whether an animal meets the definition of a service animal, the member should ask the individual only the following questions (28 CFR 35.136(f)):

- Is the animal required because of a disability?
- What task or service has the service animal been trained to perform?

If the individual explains that the animal is required because of a disability and has been trained to work or perform at least one task, the animal meets the definition of a service animal and no further questions as to the animal's status should be asked. The individual should not be questioned about their disabilities nor should members ask any individual to provide any license, certification, or identification card for the service animal.

336.5 CONTACT WITH SERVICE ANIMALS

Service animals are not pets. Department members should not interfere with a service animal by talking to, petting, or otherwise initiating contact.

336.6 REMOVAL OF SERVICE ANIMALS

If a service animal is not housebroken, exhibits vicious behavior, poses a direct threat to the health of others, or unreasonably disrupts or interferes with normal business operations, a department supervisor may direct the handler to remove the animal from the premises. Barking alone is not a threat nor does a direct threat exist if the person takes prompt, effective action to control the service animal (28 CFR 35.136(b); 28 CFR 35.139).

Each incident must be considered individually, and past incidents alone are not cause for excluding a service animal. Removal of a service animal may not be used as a reason to refuse access to services, programs, and activities to an individual with a disability. Members are expected to provide all services, programs, and activities that are reasonably available to an individual with a disability, with or without a service animal.

336.7 COMPLAINTS

When handling calls of a complaint regarding a service animal, members should remain neutral and should be prepared to explain the ADA requirements concerning service animals to the

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Service Animals

concerned parties. Businesses are required to allow service animals to accompany their handlers into the same areas that other customers or members of the public are allowed (28 CFR 36.302).

Absent a violation of law independent of the ADA, officers should take no enforcement action beyond keeping the peace. Individuals who believe they have been discriminated against as a result of a disability should be referred to the Civil Rights Division of the U.S. Department of Justice (DOJ).

Police Reserve and Explorer Programs

337.1 PURPOSE AND SCOPE

It is the policy of this department to use qualified volunteers for specified tasks and duties in order to create efficiencies for the Department and improve services to the community. Volunteers are intended to supplement and support, rather than supplant, licensed officers and civilian personnel. Volunteers can be an important part of any organization and have proven to be a valuable asset to law enforcement agencies. Volunteers help to increase department responsiveness, delivery of services and information input, and provide new program opportunities. In addition, volunteers bring new skills and expertise to the Department and prompt new enthusiasm.

337.1.1 DEFINITION OF VOLUNTEER

An individual who performs a service for the Department without promise, expectation or receipt of compensation for services rendered. This may include unpaid chaplains, Reserve officers, interns, persons providing administrative support and youth involved in a law enforcement Explorer Post, among others.

337.1.2 VOLUNTEER ELIGIBILITY

Requirements for participation as an South Saint Paul Police Department volunteer include:

- (a) At least 19 years of age for all positions other than Explorer.
- (b) At least 14 years of age for Explorer.
- (c) A valid driver's license if the position requires vehicle operation.
- (d) No conviction of a felony, any crime of a sexual nature, any crime related to assault, any crime related to dishonesty, or any crime related to impersonating a law enforcement officer.
- (e) No conviction of a misdemeanor or gross misdemeanor crime within the past 5 years, excluding petty misdemeanor traffic offenses.
- (f) The applicant must not have any mental illness or chemical dependency condition that may adversely affects the person's ability to serve in the position.
- (g) Physical requirements reasonably appropriate to the assignment.
- (h) A personal background history and character suitable for a person representing the Department, as validated by a background investigation.

The Chief of Police may apply exceptions for eligibility based on organizational needs and the qualification of the individual.

337.2 VOLUNTEER MANAGEMENT

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Police Reserve and Explorer Programs

337.2.1 VOLUNTEER COORDINATOR

Sergeants and / or Lieutenants will be assigned as the Volunteer Coordinators to provide a central coordinating point for effective volunteer management within the Department, and to direct and assist staff and volunteer efforts to jointly provide more productive services. The Volunteer Coordinators or designee shall be responsible for the following:

- (a) Recruiting, selecting and training qualified volunteers for various positions.
- (b) Maintaining records for each volunteer.
- (c) Tracking and evaluating the contribution of volunteers.
- (d) Maintaining the volunteer handbook and outlining expectations, policies and responsibilities for all volunteers.
- (e) Maintaining a record of volunteer schedules and work hours.
- (f) Completion and dissemination as appropriate of all necessary paperwork and information.
- (g) Planning periodic recognition events.
- (h) Administering discipline when warranted.
- (i) Maintaining liaison with other volunteer-utilizing programs in the community and assisting in community-wide efforts to recognize and promote volunteering.

337.2.2 RECRUITMENT

Volunteers should be recruited on a continuous and ongoing basis in accordance with department policy on equal opportunity nondiscriminatory employment. A primary qualification for participation in the application process should be an interest in, and an ability to assist the Department in serving the public.

Requests for volunteers should be submitted in writing by interested staff to the Volunteer Coordinator through the requester's immediate supervisor. A complete position description and a requested time frame should be included in the request. All parties should understand that the recruitment of volunteers is enhanced by creative and interesting assignments. The Volunteer Coordinator may withhold assignment of any volunteer until such time as the requesting unit is prepared to make effective use of volunteer resources.

337.2.3 SCREENING

All prospective volunteers should complete the volunteer application form. The Volunteer Coordinator or designee should conduct a face-to-face interview with the applicant.

A documented background investigation shall be completed on each volunteer applicant and shall include, but not necessarily be limited to, the following:

- (a) Traffic and criminal background check
- (b) Employment

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Police Reserve and Explorer Programs

(c) References

A volunteer whose assignment requires the use of, access to or places him/her in the vicinity of criminal histories, investigative files or information portals, shall require submission of prints and clearance through the Bureau of Criminal Apprehension (BCA).

337.2.4 SELECTION AND PLACEMENT

Service as a volunteer shall begin with an official notice of acceptance or appointment to a volunteer position. Notice may only be given by an authorized representative of the Department, who will normally be the Volunteer Program Manager. No volunteer should begin performance of any position until he/she has been officially accepted for that position and completed all necessary screening and paperwork. At the time of final acceptance, each volunteer should complete all necessary enrollment paperwork.

Volunteers should be placed only in assignments or programs that are consistent with their knowledge, skills, abilities and the needs of the Department.

337.2.5 EMPLOYEES WORKING AS OFFICERS

Qualified employees of this department, when authorized, may also serve as reserve officers. However, the Department must not utilize the services of a or volunteer in such a way that it would violate employment laws or labor agreements (Example: a detention officer working as an officer for reduced or no pay). Therefore, the Coordinator should consult the Department of Human Resources prior to an employee serving in a or volunteer capacity (29 CFR 553.30).

337.2.6 TRAINING

Volunteers will be provided with an orientation program to acquaint them with the department, personnel, policies and procedures that have a direct impact on their work assignment.

Volunteers should receive position-specific training to ensure they have adequate knowledge and skills to complete tasks required by the position and should receive periodic ongoing training as deemed appropriate by their supervisor or the Volunteer Coordinator.

Depending on the assignment, Training may include:

- (a) Role of the volunteer.
- (b) Department policies.
- (c) Training specific to the procedure manual for the volunteer position.
- (d) Discrimination and harassment training.
- (e) CPR/first aid.
- (f) CERT/Citizens Emergency Response Training.
- (g) Search and rescue techniques.
- (h) Scenario-based searching methods.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Police Reserve and Explorer Programs

- (i) Evidence preservation.
- (j) Basic traffic direction and control.
- (k) Roadway incursion safety.
- (l) Self-defense techniques.
- (m) Vehicle operations, including specialized vehicles.

Pursuant to Minn. Stat. § 626.8466, the Department may establish training, licensing and continuing education requirements for its reserve officers.

Training should reinforce to volunteers that they should not intentionally represent themselves as, or by omission infer that they are licensed officers or other full-time members of the Department. They shall always represent themselves as volunteers.

All volunteers shall comply with the rules of conduct and with all orders and directives, either oral or written, issued by the Department. Whenever a rule, regulation or guideline in this manual refers to a licensed officer, it shall also apply to a volunteer unless by its nature it is inapplicable.

337.2.7 FITNESS FOR DUTY

No volunteer shall report to work or be on-duty when his/her judgment or physical condition has been impaired by alcohol, medication, other substances, illness or injury.

Volunteers shall report to their supervisor any changes in status that may affect their ability to fulfill their duties. This includes, but is not limited to, the following:

- (a) Driver's license
- (b) Medical condition
- (c) Arrests
- (d) Criminal investigations
- (e) All law enforcement contacts

All volunteers shall adhere to the guidelines set forth by this department regarding drug and alcohol use.

337.2.8 DRESS CODE

As representatives of the Department, volunteers are responsible for presenting a professional image to the community. Volunteers shall dress appropriately for the conditions and performance of their duties.

Volunteers shall conform to approved dress consistent with their duty assignment. Uniforms authorized for volunteers should be readily distinguishable from those worn by licensed officers. No volunteer shall wear his/her uniform or identifiable parts of that uniform while off-duty.

Volunteers shall be required to return any issued uniform or department property at the termination of service.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Police Reserve and Explorer Programs

337.3 SUPERVISION OF VOLUNTEERS

Each volunteer who is accepted to a position with the Department must have a clearly identified supervisor who is responsible for direct management of that volunteer. This supervisor will be responsible for day-to-day management and guidance of the work of the volunteer and should be available to the volunteer for consultation and assistance.

A volunteer may be assigned as, and act as a supervisor of other volunteers provided that the supervising volunteer is under the direct supervision of a paid staff member.

Functional supervision of volunteers is the responsibility of the supervisor in charge of the unit where the volunteer is assigned. Following are some considerations to keep in mind while supervising volunteers:

- (a) Take the time to introduce volunteers to employees on all levels.
- (b) Ensure volunteers have work space and necessary office supplies.
- (c) Make sure the work is challenging. Do not hesitate to give them an assignment or task that will tap these valuable resources.

337.4 PROPERTY AND EQUIPMENT

Volunteers will be issued an identification card that must be worn at all times while on-duty. Any fixed and portable equipment issued by the Department shall be for official and authorized use only. Any property or equipment issued to a volunteer shall remain the property of the Department and shall be returned at the termination of service.

337.4.1 VEHICLE USE

Volunteers assigned to duties such as vacation house checks or other assignments that require the use of a vehicle must first complete the following:

- (a) A driving safety briefing.
- (b) Verification that the volunteer possesses a valid driver's license.
- (c) Verification that the volunteer carries current vehicle insurance.

When operating a Department vehicle, volunteers shall obey all rules of the road, including seat belt requirements.

Volunteers should not operate a marked patrol car unless there is a prominently placed sign indicating that it is out of service and is being operated for maintenance purposes only; that it is operated during a POST-approved skills course; that it is being used to transport prisoners or equipment; or is being used to provide supplementary assistance under the direction of an on-duty licensed officer (Minn. Stat. 169.98 Subd. 1 b. Volunteers are not authorized to operate a Department vehicle under emergency conditions (lights and siren).

337.4.2 RADIO AND MDC USAGE

Volunteers shall successfully complete state and federal database access training and radio procedures training prior to using the law enforcement radio or MDT and shall comply with all

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Police Reserve and Explorer Programs

related provisions. The Volunteer Coordinator should ensure that radio and database access training is provided for volunteers whenever necessary.

337.5 DISCIPLINARY PROCEDURES/TERMINATION

A volunteer may be removed from the volunteer program at the discretion of the Chief of Police or the Volunteer Coordinator. Volunteers shall have no property interests in their continued appointment.

Volunteers may resign from volunteer service with this department at any time. It is requested that volunteers who intend to resign provide advance notice of their departure and a reason for their decision.

337.6 EMERGENCY CALLOUT FOR VOLUNTEER PERSONNEL

The Volunteer Coordinator shall develop a plan outlining an emergency callout procedure for volunteer personnel.

Native American Graves Protection and Repatriation

338.1 PURPOSE AND SCOPE

This policy is intended to ensure the protection and security of ancient or historic grave sites, including notification of personnel responsible for cultural items, in compliance with the Native American Graves Protection and Repatriation Act (NAGPRA) (25 USC § 3001 et seq.).

338.1.1 DEFINITIONS

Definitions related to this policy include (43 CFR 10.2):

Funerary objects - Objects that, as part of the death rite or ceremony of a Native American culture, are reasonably believed to have been placed intentionally at the time of death or later with or near individual human remains. Funerary objects are either associated funerary objects or unassociated funerary objects.

Associated funerary objects are any funerary objects related to removed human remains, where the location of the human remains is known. This includes objects that were made exclusively for burial purposes or to contain human remains, regardless of the physical location or existence of any related human remains.

Unassociated funerary objects are any other funerary objects that are identified by a preponderance of the evidence such as:

- Related to human remains but the remains were not removed, or the location of the remains is unknown.
- Related to specific individuals or families.
- Removed from specific burial sites with Native American cultural affiliation.
- Removed from an area where such burial sites are known to have existed, but the site no longer exists.

Native American human remains - Any physical part of the body of a Native American individual.

Objects of cultural patrimony - Objects having ongoing historical, traditional, or cultural importance that is central to the Native American group or culture itself and, therefore, cannot be appropriated or conveyed by any individual, including members of the Native American group or Native Hawaiian organization. Such objects must have been considered inalienable by the Native American group at the time the object was separated from the group.

Sacred objects - Specific ceremonial objects needed by traditional Native American religious leaders for the practice of traditional Native American religions.

338.2 POLICY

It is the policy of the South Saint Paul Police Department that the protection of Native American human remains, funerary objects, associated funerary objects, unassociated funerary objects,

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Native American Graves Protection and Repatriation

sacred objects, or objects of cultural patrimony is the responsibility of all members. Such protection includes minimizing destruction, contamination, inadvertent disruption, or complicated custody transfer processes.

338.3 COMPLIANCE WITH THE NATIVE AMERICAN GRAVES PROTECTION AND REPATRIATION ACT

Upon discovery or arrival upon a scene where it reasonably appears that a Native American grave, human remains, funerary objects, associated funerary objects, unassociated funerary objects, sacred objects, or objects of cultural patrimony are exposed or otherwise unsecured, members shall secure the site in the same manner as a crime scene. All activity at the scene other than scene preservation activity must cease (43 CFR 10.5).

No photography or video recording may be permitted by the media or any group or individual who may wish to exhibit the remains.

Without delay, the appropriate agency or group shall be notified to respond and take control of the scene. These include the following (43 CFR 10.5):

- Federal land - Appropriate agency at the U.S. Department of the Interior or U.S. Department of Agriculture
- State land - State archaeologist (Minn. Stat. § 307.08, Subd. 7)
- Tribal land - Responsible Indian tribal official

338.4 EVIDENCE AND PROPERTY

If the location has been investigated as a possible homicide scene prior to identification as a NAGPRA site, investigators shall work with other appropriate agencies and individuals to ensure the proper transfer and repatriation of any material collected. Members shall ensure that any remains or artifacts located at the site are expediently processed (43 CFR 10.7).

338.5 BURIAL GROUNDS

All human burials, human remains and human burial grounds shall be afforded equal treatment and respect for human dignity, regardless of ethnic origins, cultural backgrounds or religious affiliations (Minn. Stat. § 307.08, Subd. 1).

This department shall cooperate with other government agencies, the Minnesota Office of the State Archaeologist and the Minnesota Indian Affairs Council to carry out any provisions of state law (Minn. Stat. § 307.08, Subd. 9).

Off-Duty Law Enforcement Actions

339.1 PURPOSE AND SCOPE

The decision to become involved in a law enforcement action when off-duty can place an officer as well as others at great risk and must be done with careful consideration. This policy is intended to provide guidelines for officers of the South Saint Paul Police Department with respect taking law enforcement action while off-duty.

339.2 POLICY

Officers generally should not initiate law enforcement action while off-duty. Officers should not attempt to initiate enforcement action when witnessing minor crimes, such as suspected intoxicated drivers, reckless driving or minor property crimes. Such incidents should be promptly reported to the appropriate law enforcement agency.

When the safety of the public or the prevention of major property damage requires immediate action, officers should first consider reporting and monitoring the activity and only take direct action as a last resort.

Officers are not expected to place themselves in unreasonable peril. However, any licensed member of this department who becomes aware of an incident or circumstance that the member reasonably believes would justify the use of deadly force or result in significant property damage may take reasonable action to minimize or eliminate the threat. See the Use of Force Policy for additional guidance.

339.3 FIREARMS

Officers of this department may carry firearms while off-duty in accordance with federal regulations, state law and department policy. All firearms and ammunition must meet guidelines as described in the Firearms Policy. When carrying firearms while off-duty, officers shall also carry their department-issued badge and identification.

Officers should refrain from carrying firearms when the consumption of alcohol is likely or when the need to carry a firearm is outweighed by safety considerations. Firearms shall not be carried by any officer who has consumed an amount of an alcoholic beverage or taken any drugs that would tend to adversely affect the officer's senses or judgment.

339.4 DECISION TO INTERVENE

There is no legal requirement for off-duty officers to take law enforcement action. However, should officers decide to intervene, they must evaluate whether the action is necessary or desirable and should take into consideration:

- (a) The tactical disadvantage of being alone and the fact there may be multiple or hidden suspects.
- (b) The inability to communicate with responding units.
- (c) The lack of equipment, such as handcuffs, Oleoresin Capsicum (OC) spray or a baton.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Off-Duty Law Enforcement Actions

- (d) The lack of cover.
- (e) The potential for increased risk to bystanders if the off-duty officer were to intervene.
- (f) Unfamiliarity with the surroundings.
- (g) The potential for the off-duty officer to be misidentified by other peace officers or members of the public.

Officers should consider waiting for on-duty uniformed officers to arrive and gather as much accurate intelligence as possible instead of immediately intervening.

339.4.1 INTERVENTION PROCEDURE

If involvement is reasonably necessary, the officer should attempt to call or have someone else call 9-1-1 to request immediate assistance. The operator should be informed that an off-duty officer is on-scene and should be provided a description of the officer if reasonably possible.

Whenever reasonably practicable, the officer should loudly and repeatedly identify him/herself as an South Saint Paul Police Department officer until acknowledged. Official identification should also be displayed.

339.4.2 INCIDENTS OF PERSONAL INTEREST

Officers should refrain from handling incidents of personal interest (e.g., family or neighbor disputes) and should remain neutral. In such circumstances, officers should call the responsible agency to handle the matter.

339.4.3 CIVILIAN RESPONSIBILITIES

Civilian personnel should not become involved in any law enforcement actions while off-duty except to notify the local law enforcement authority and remain at the scene, if safe and reasonably practicable.

339.4.4 OTHER CONSIDERATIONS

When encountering a non-uniformed officer in public, uniformed officers should wait for acknowledgement by the non-uniformed officer in case he/she needs to maintain an undercover capability.

339.5 REPORTING

Any officer, prior to taking any off-duty law enforcement action, shall notify and receive approval of an South Saint Paul Police Department supervisor (or other applicable enforcement authority if acting outside the jurisdiction of the South Saint Paul Police Department). The Sergeant shall determine whether a report should be filed by the employee.

Officers should cooperate fully with the agency having jurisdiction in providing statements or reports as requested or as appropriate.

Department Use of Social Media

340.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that any use of social media on behalf of the Department is consistent with the department mission.

This policy does not address all aspects of social media use. Specifically, it does not address:

- Personal use of social media by department members (see the Employee Speech, Expression and Social Networking Policy).
- Use of social media in personnel processes (see the Recruitment and Selection Policy).
- Use of social media as part of a criminal investigation, other than disseminating information to the public on behalf of this department (see the Investigation and Prosecution Policy).

340.1.1 DEFINITIONS

Definitions related to this policy include:

Social media - Any of a wide array of internet-based tools and platforms that allow for the sharing of information, such as the department website or social networking services.

340.2 POLICY

The South Saint Paul Police Department may use social media as a method of effectively informing the public about department services, issues, investigations and other relevant events.

Department members shall ensure that the use or access of social media is done in a manner that protects the constitutional rights of all.

340.3 AUTHORIZED USERS

Only members authorized by the Chief of Police or the authorized designee may utilize social media on behalf of the Department. Authorized members shall use only department-approved equipment during the normal course of duties to post and monitor department-related social media, unless they are specifically authorized to do otherwise by their supervisors.

The Chief of Police may develop specific guidelines identifying the type of content that may be posted. Any content that does not strictly conform to the guidelines should be approved by a supervisor prior to posting.

Requests to post information over department social media by members who are not authorized to post should be made through the member's chain of command.

340.4 AUTHORIZED CONTENT

Only content that is appropriate for public release, that supports the department mission, and that conforms to all department policies regarding the release of information may be posted.

Examples of appropriate content include:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Department Use of Social Media

- (a) Announcements.
- (b) Tips and information related to crime prevention.
- (c) Investigative requests for information.
- (d) Requests that ask the community to engage in projects that are relevant to the department mission.
- (e) Real-time safety information that is related to in-progress crimes, geographical warnings, or disaster information.
- (f) Traffic information.
- (g) Media releases.
- (h) Recruitment of personnel.

Authorized members shall review all content prior to posting to ensure that the posting does not contain prohibited content.

340.4.1 INCIDENT-SPECIFIC USE

In instances of active incidents where speed, accuracy and frequent updates are paramount (e.g., crime alerts, public safety information, traffic issues), the Police Chief or the authorized designee will be responsible for the compilation of information to be released, subject to the approval of the Incident Commander.

340.5 PROHIBITED CONTENT

Content that is prohibited from posting includes, but is not limited to:

- (a) Content that is abusive, discriminatory, inflammatory or sexually explicit.
- (b) Any information that violates individual rights, including confidentiality and/or privacy rights and those provided under state, federal or local laws.
- (c) Any information that could compromise an ongoing investigation.
- (d) Any information that could tend to compromise or damage the mission, function, reputation or professionalism of the South Saint Paul Police Department or its members.
- (e) Any information that could compromise the safety and security of department operations, members of the Department, victims, suspects or the public.
- (f) Any content posted for personal use.
- (g) Any content that has not been properly authorized by this policy or a supervisor.

Any member who becomes aware of content on this Department's social media site that he/she believes is unauthorized or inappropriate should promptly report such content to a supervisor. The supervisor will ensure its removal from public view and investigate the cause of the entry.

340.5.1 PUBLIC POSTING

Department social media sites shall be designed, reviewed and maintained to prevent posting of improper content by the public.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Department Use of Social Media

The Department may provide a method for members of the public to contact department members directly.

Extreme Risk Protection Orders

343.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for petitioning for and serving extreme risk protection orders and accounting for firearms obtained pursuant to those orders.

343.1.1 DEFINITIONS

Definitions related to this policy include (Minn. Stat. § 624.7171):

Extreme risk protection order (ERPO) - An order prohibiting a named person from possessing or purchasing prohibited items.

Prohibited items - Firearms that are prohibited by an ERPO.

343.2 POLICY

It is the policy of the South Saint Paul Police Department, through the City Attorney, to petition for and serve ERPOs in compliance with state law, and to properly account for prohibited items obtained by the Department pursuant to such orders.

343.3 EXTREME RISK PROTECTION ORDER COORDINATOR

The Chief of Police should designate an ERPO coordinator. The responsibilities of the coordinator include:

- (a) Developing and maintaining procedures for the filing of a petition for an ERPO or a renewal of an ERPO by department members.
- (b) Identifying factors to consider when assessing whether to seek an ERPO, including:
 - 1. Are family members, household members, or guardian(s), as defined in section 524.1-201 clause (27), able to petition for relief.
 - 2. Whether threats have been made, and if so, whether the threats are credible and specific.
 - 3. Whether the potential victim is within close proximity.
 - 4. Whether the person has expressed suicidal tendencies.
 - 5. Whether the person has access to firearms.
 - 6. Whether the person has committed an act of violence toward themselves or another person.
 - 7. The criminal history of the person, in particular any history of criminal violence, including whether the person is currently on parole, probation, or monitored release.
 - 8. The mental health history of the person, in particular whether the person has any history of mental illness or has ever been detained for being a danger to themselves or others.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Extreme Risk Protection Orders

9. Any known upcoming holidays, anniversaries, or other dates of significance that may serve as a trigger for the person, such as the death of a family member.
10. Whether the person has any history of drug or alcohol abuse.
- (c) Developing and maintaining procedures for the receipt and service of ERPOs consistent with the requirements of Minn. Stat. § 624.7172; Minn. Stat. § 624.7175; and the Warrant Service and Operations Planning and Deconfliction policies. Procedures should include:
 1. Evaluation of an order to determine appropriate service and necessary precautions.
 2. Forwarding ERPOs to the Operations Director or the authorized designee.
 3. Forwarding ERPOs to the Records Supervisor for recording in appropriate databases and required notice to the court, as applicable.
 4. Preparing or obtaining a search warrant prior to attempting service of an ERPO, when appropriate (Minn. Stat. § 624.7175).
- (d) Coordinating with the Support Services Commander to provide officers who may be involved in petitioning for or serving ERPOs with training on such orders. Training should include determining when a petition is appropriate, the process for seeking ERPOs, and the service of such orders.
- (e) Reviewing each petition and any associated court documents for an ERPO prepared by members, for compliance with this policy, department procedures, and state law.
- (f) Developing and maintaining procedures for members to accept voluntarily surrendered prohibited items at times other than when an ERPO is being served by the Department (Minn. Stat. § 624.7175). Procedures should include:
 1. Preparing and providing a receipt identifying all prohibited items to the person surrendering the items.
 2. Proper handling and processing of surrendered items.

343.4 EXTREME RISK PROTECTION ORDERS

An officer who reasonably believes that an ERPO is appropriate should obtain approval from an appropriate supervisor and the extreme risk protection order coordinator or the authorized designee prior to seeking an order through the City Attorney.

343.4.1 STANDARDS

Extreme risk protection orders may be appropriate if a person poses a significant danger of bodily harm to other persons or is at significant risk of suicide by possessing a firearm (Minn. Stat. § 624.7171, Subd. 4).

If a person poses a significant danger of bodily harm to other persons or is at significant risk of suicide by possessing a firearm, and presents an immediate and present danger of either bodily harm to others or of taking their life, an ERPO may be appropriate (Minn. Stat. § 624.7174).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Extreme Risk Protection Orders

343.4.2 REQUIREMENTS OF PETITION

An application for an ERPO should be prepared, filed, and served consistent with state law and the procedures developed by the extreme risk protection order coordinator (Minn. Stat. § 624.7171).

343.5 SERVICE OF ORDERS

Officers should serve a copy of an ERPO, along with any accompanying notice of hearing and petition, affidavit, as applicable, on the person named in the order as soon as reasonably practicable (Minn. Stat. § 624.7172).

Service of ERPOs should take precedence over the service of other orders, except for orders of a similar emergency nature.

343.5.1 SAFETY CONSIDERATIONS

Upon receipt of an ERPO, the Operations Director or the authorized designee should evaluate the circumstances of the order and consider what precautions are appropriate for service of the protection order.

When appropriate based on the circumstances and department procedures, service of an order should be executed pursuant to the Operations Planning and Deconfliction Policy.

At least two officers should be present when an ERPO is being served.

343.5.2 SURRENDER OF PROHIBITED ITEMS

Officers serving an ERPO should request that the named person immediately surrender all prohibited items as required by the order and take custody of any items surrendered pursuant to the order (Minn. Stat. § 624.7172; Minn. Stat. § 624.7175).

The officer serving the ERPO should prepare a receipt identifying all surrendered items and a copy of the receipt should be given to the person. The officers should ensure the original receipt is included in the original case report and forwarded to the Records Supervisor as soon as practicable.

All items collected should be handled and booked in accordance with the Evidence Room Policy.

343.5.3 SEARCH WARRANTS

Officers should consider whether a search warrant may be reasonably necessary prior to attempting service of an ERPO.

Officers should also consider whether to seek a search warrant if the named person refuses to surrender any prohibited items or if an officer serving an ERPO reasonably believes there are prohibited items within the persons custody, control, or possession that have not been surrendered.

343.6 RELEASE OF PROHIBITED ITEMS

Any person requesting the release of any prohibited items in department custody pursuant to an ERPO should be referred to the Evidence Room.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Extreme Risk Protection Orders

343.7 EXTENSION OF EXTREME RISK PROTECTION ORDER

The Investigations supervisor is responsible for the review of any ERPO obtained by the Department to determine if renewal or extension of the order should be requested within the time prescribed by law (Minn. Stat. § 624.7172; Minn. Stat. § 624.7173).

ADA Compliance

344.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for equal access to South Saint Paul Police Department services, programs, and activities for persons with disabilities, in accordance with Title II of the Americans with Disabilities Act (ADA).

This policy also includes guidelines to provide effective communication with persons with disabilities. See the Service Animals Policy for guidance on protecting the rights of individuals who use service animals in accordance with the ADA.

344.1.1 DEFINITIONS

Definitions related to this policy include (28 CFR 35.104):

ADA coordinator - The member designated by the Chief of Police to coordinate the department's efforts to comply with the ADA (28 CFR 35.107).

Assistive devices, auxiliary aids, and services - Tools used by persons with disabilities to facilitate their participation in services, programs, and activities offered by the South Saint Paul Police Department and to facilitate effective communication. They include but are not limited to the use of gestures or visual aids to supplement oral communication; a notepad and pen or pencil to exchange written notes; a computer or typewriter; an assistive listening system or device to amplify sound; a teletypewriter (TTY) or videophones (video relay service or VRS); taped text; a qualified reader; or a qualified interpreter.

Disability - A physical or mental impairment that substantially limits a major life activity including hearing, seeing, or speaking, regardless of whether the person uses assistive devices, auxiliary aids, and services. This includes those who, because of a hearing, speech, or other communication disorder, cannot fully understand any charges made against them or the seizure of their property, or they are incapable of presenting or assisting in the presentation of a defense (Minn. Stat. § 611.31). Individuals who wear ordinary eyeglasses or contact lenses are not considered to have a disability (42 USC § 12102; 28 CFR 35.108).

Facility - All aspects of department buildings, structures, sites, complexes, equipment, rolling stock or other conveyances, roads, walkways, parking areas, and other real or personal property (28 CFR 35.108).

Modification - Any change, adjustment, alteration, adaptation, or accommodation that renders a department service, program, or activity suitable for use, enjoyment, or participation by a person with a disability. This may include alteration of existing buildings and facilities.

A modification includes any change or exception to a policy, practice, or procedure that allows a person with a disability to have equal access to services, programs, and activities. It also includes the provision or use of assistive devices, auxiliary aids, and services.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

Qualified interpreter - A person who is able to interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary. Qualified interpreters include oral interpreters, transliterators, sign language interpreters, and intermediary interpreters.

344.2 POLICY

It is the policy of the South Saint Paul Police Department that persons with disabilities, including victims, witnesses, suspects, and arrestees, have equal access to services, programs, and activities of the Department.

The Department will not discriminate against or deny any individual access to services, programs, or activities based upon the presence or suspected presence of disabilities.

344.3 ADA COORDINATOR RESPONSIBILITIES

The responsibilities of the ADA coordinator include but are not limited to (28 CFR 35.130):

- (a) Collaborating with the City ADA coordinator regarding the South Saint Paul Police Department's efforts to provide equal access to services, programs, and activities.
 - 1. Maintaining department compliance with accessibility standards for department web content and mobile applications as required by 28 CFR 35 Subpart H (28 CFR 35.200).
- (b) Collaborating with the City ADA coordinator to facilitate a process of periodic self-evaluation. The process should include:
 - 1. Inspection of current department facilities to identify access issues.
 - 2. Review of current department services, activities, and programs for access issues.
 - 3. Assessment and update, if necessary, of current compliance measures.
 - 4. Identification of recurring areas of complaint for which new methods of modification should be considered.
 - 5. Review of the department's emergency programs, services, and activities as they apply to persons with disabilities.
 - 6. Recommendation of a schedule to implement needed improvements.
- (c) Acting as a liaison with local disability advocacy groups or other disability-focused groups regarding access to department services, programs, and activities.
- (d) Developing procedures that will enable members to access assistive devices, auxiliary aids, and services, and making the procedures available as appropriate.
 - 1. A list of qualified interpreter services with contact and availability information should be maintained and easily accessible to members.
- (e) Developing procedures for the review and processing of requests for modifications that will help members provide persons with disabilities access to department services, programs, and activities, as appropriate.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

- (f) Establishing procedures for the booking process to assist members with managing commonly encountered disabilities such as sight or mobility impairments and intellectual or developmental disabilities.
- (g) Providing notice to the public regarding the rights and protections afforded by the ADA. This may include posters, published notices, handbooks, manuals, and pamphlets describing department services, programs, and activities and the availability of assistive devices, auxiliary aids, and services, as well as modifications (28 CFR 35.106).
- (h) Collaborating with other [city/county] departments during the planning process to provide that new construction and any alteration to an existing building or facility are undertaken in compliance with the ADA (28 CFR 35.151).
- (i) Developing, implementing, and publishing appropriate procedures to provide for the prompt and equitable resolution of complaints and inquiries regarding discrimination in access to services, programs, and activities. The complaint procedures should include an appeal process (28 CFR 35.107).
- (j) Verifying that third parties providing department services, programs, or activities through contract, outsourcing, licensing, or other arrangement have established reasonable policies and procedures to prevent discrimination against and denial of access to persons with disabilities.
- (k) Recommending amendments to this policy as needed.

344.4 REQUESTS

The goal of any modification should be to allow a person with a disability to participate in a service, program, or activity the same as a person who does not have a disability.

Upon receiving a request for a modification, members should make reasonable efforts to accommodate the request based on the preference of the person with the disability. Members should not ask about the nature and extent of a person's disability but should limit questions to elicit information necessary to determine the need for a modification and the appropriate type of modification.

If the requested modification or an alternative modification can reasonably be made at the time of the request, the member should make the modification. A member who is unable to accommodate a request or unsure about whether a request should be accommodated should contact a supervisor.

The supervisor should review and approve the request, if practicable and appropriate. Otherwise, the supervisor should document the requesting person's contact information and the modification being requested and forward the request to the ADA coordinator for processing as soon as reasonably practicable.

344.4.1 DENIAL OF A REQUEST

The following should be considered before denying a request for modification:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

- (a) Requests for modifications should be approved unless complying with the request would result in (28 CFR 35.150):
 - 1. A substantial alteration of the service, program, or activity.
 - 2. An undue financial or administrative burden on the Department. All resources available for use in the funding and operation of the service, program, or activity at issue should be considered in this determination.
 - 3. A threat to or the destruction of the historic significance of a historic property.
 - 4. A direct threat to the health or safety of others (28 CFR 35.139).
- (b) If any of these circumstances are present, the ADA coordinator should work with department members and the person requesting the modification to determine if an alternative modification is available.
- (c) Where new construction or physical modification of an existing building or facility would be unfeasible or unduly burdensome, the ADA coordinator should work with department members to determine whether alternative modifications are available. Alternative methods that should be considered include (28 CFR 35.150):
 - 1. Reassigning services, programs, or activities to accessible buildings or facilities.
 - 2. Utilizing technology, equipment, rolling stock, or other conveyances.
 - 3. Delivering the services, programs, or activities directly to a person with a disability by way of home visits or meeting the person at an accessible location.
 - 4. Any other means or methods that would make services, programs, or activities readily accessible.
- (d) If no alternative modification is appropriate, the ADA coordinator shall issue a written statement explaining why a modification of the service, program, or activity will not be made (28 CFR 35.150).

344.4.2 PERSONAL DEVICES AND ASSISTANCE

Although members should make every effort to comply with requests, the provision of personal devices or assistance (e.g., wheelchairs, eyeglasses, hearing aids, personal assistance in eating or using the restroom) to persons with disabilities is not required (28 CFR 35.135).

344.4.3 SURCHARGES

Surcharges shall not be imposed upon persons with disabilities to cover the costs of providing modifications (28 CFR 35.130(f)).

344.5 COMMUNICATIONS WITH PERSONS WITH DISABILITIES

Members should remain alert to the possibility of communication problems when engaging with persons with disabilities. When a member knows or suspects an individual requires assistance to effectively communicate, the member should identify the individual's choice of assistive devices, auxiliary aids, and services. The individual's preferred communication method should be honored unless another effective method of communication exists under the circumstances (28 CFR 35.160).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

Factors to consider when determining whether an alternative method may be effective include:

- (a) The methods of communication usually used by the individual.
- (b) The nature, length, and complexity of the communication involved.
- (c) The context of the communication.

In emergency situations involving an imminent threat to the safety or welfare of any person, members may use whatever modification reasonably appears effective under the circumstances. This may include exchanging written notes or using the services of a person who knows sign language but is not a qualified interpreter, even if the person who is deaf or hard of hearing would prefer a qualified sign language interpreter. Once the emergency has ended, the method of communication should be reconsidered. The member should inquire as to the individual's preference and give primary consideration to that preference.

344.5.1 TYPES OF ASSISTANCE AVAILABLE

Department members shall not refuse an available type of assistive device, auxiliary aid, or service to a person with a disability who is requesting assistance. The Department will not require persons with disabilities to furnish their own assistive device, auxiliary aid, or service as a condition for receiving access to department services, programs, and activities. The Department will make every reasonable effort to provide equal access and timely assistance to persons with disabilities through a variety of assistive devices, auxiliary aids, and services (28 CFR 35.160).

The Department will not require that persons with disabilities use department-provided assistive devices, auxiliary aids, and services. Department-provided assistive devices, auxiliary aids, and services may include but are not limited to the means described in this policy.

344.5.2 AUDIO RECORDINGS AND ENLARGED PRINT

The Department may develop audio recordings to assist people who are blind or have a visual impairment. If such a recording is not available, members may read aloud from the appropriate form or provide forms with enlarged print.

344.5.3 QUALIFIED INTERPRETERS

A qualified interpreter may be needed in lengthy or complex transactions (e.g., interviewing a victim, witness, suspect, or arrestee) with individuals who normally rely on sign language or speechreading (i.e., lip-reading) to understand what others are saying.

The qualified interpreter should not be a person with an interest in the matter. A person providing interpretation services may be required to establish the accuracy and trustworthiness of the interpretation in a legal proceeding.

Qualified interpreters should be:

- (a) Available within a reasonable amount of time.
- (b) Experienced in providing interpretation services related to law enforcement matters in the person's primary language.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

- (c) Familiar with the use of text- and video-based communications products and systems.
- (d) Certified in either American Sign Language (ASL) or Signing Exact English (SEE).
- (e) Able to understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.
- (f) Knowledgeable of the ethical issues involved when providing interpreter services.

Members should use department-approved procedures to request a qualified interpreter at the earliest reasonable opportunity or when it is reasonably apparent that an interpreter is needed. The use of a video remote interpreting service should be considered, where appropriate, if a live interpreter is not available. Persons with disabilities shall not be required to provide an interpreter (28 CFR 35.160).

344.5.4 TELECOMMUNICATION SERVICES

In situations where an individual without a disability would have access to a telephone (e.g., during booking or attorney contacts), members must also provide those with communication-related disabilities the opportunity to place calls using an available TTY, TDD, or other voice, text, or video-based communications product or system. Members shall provide additional time, as needed, for effective communication due to the slower nature of assisted communications.

The Department will accept all TDD and computer modem calls placed by individuals with communications-related disabilities and received via a telecommunications relay service (28 CFR 35.162).

344.5.5 COMMUNITY VOLUNTEERS

Where qualified interpreters are unavailable to assist members, department-approved community volunteers who have demonstrated competence in communication services, such as ASL or SEE, may be called upon to provide interpreter services when appropriate. However, department members must carefully consider the nature of the interaction and the relationship between the individual with the disability and the volunteer to be reasonably satisfied that the volunteer can provide neutral and unbiased assistance.

344.5.6 FAMILY AND FRIENDS

While family or friends may offer to assist with interpretation, members should carefully consider the circumstances before relying on such individuals. The nature of the interaction and relationship between the individual with the disability and the person offering services must be carefully considered to determine whether the family member or friend can provide neutral and unbiased assistance.

Except in an emergency involving an imminent threat to the safety or welfare of any person and no qualified interpreter is reasonably available, members shall not use a minor child as an interpreter (28 CFR 35.160).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

344.5.7 FIELD ENFORCEMENT CONSIDERATIONS

Due to the unpredictable and varied nature of field enforcement, the Department recognizes that it is impracticable to provide immediate access to a comprehensive supply of assistive devices, auxiliary aids, and services to every member of this department. Members involved in interactions with persons with disabilities that occur in the field should assess each situation to determine if communication assistance is necessary. The length, complexity, and importance of the communication, as well as the individual's preferred method of communication, should be considered when determining what, if any, resources should be used and whether a qualified interpreter or other service is needed.

344.6 CUSTODIAL INTERROGATIONS

In an effort to ensure that the rights of individuals with disabilities are protected during a custodial interrogation, this department will provide reasonable modifications before beginning an interrogation, unless exigent circumstances exist or the individual has made a clear indication that the individual understands the process and desires to proceed without receiving a modification. *Miranda* warnings should be provided to a suspect via the individual's preferred method of communication.

Interrogations should be recorded whenever reasonably practicable. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

344.6.1 STATE REQUIREMENTS

The investigating or arresting officer shall immediately make necessary contacts to get a qualified interpreter for a person in custody at the earliest possible time (Minn. Stat. § 611.32).

The following shall be explained with the assistance of the qualified interpreter (Minn. Stat. § 611.32):

- (a) All charges filed against the person
- (b) All procedures relating to the person's detainment and release
- (c) In the case of any seizure under the Asset Forfeiture Policy:
 - 1. The possible consequences of the seizure
 - 2. The person's right to judicial review

Every qualified interpreter shall be administered and take the following oath prior to assisting in taking a statement related to a criminal matter from an in-custody deaf or hard of hearing person (Minn. Stat. § 611.33):

"I will make, to the best of my skill and judgment, a true interpretation to the disabled person being examined of all the proceedings, in a language which said person understands, and to repeat the statements, in the English language, of said person to the officials before whom the proceeding is taking place."

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

344.7 ARREST

If an individual with a communication-related disability is arrested, the arresting officer shall use department-approved procedures to provide a qualified interpreter as soon as reasonably practicable, unless the individual indicates a preference for a different assistive device, auxiliary aid, or service, or the officer reasonably determines another effective method of communication exists under the circumstances.

Individuals who are arrested and are assisted by service animals should be permitted to make arrangements for the care of such animals prior to transport.

344.8 WEBSITE ACCESS

The ADA coordinator should work with the appropriate parties to develop online content that is readily accessible to persons with disabilities. Department web content should be developed in conformance with the most current guidelines issued by the U.S. Department of Justice and federal regulations (28 CFR 35 Subpart H; 28 CFR 35.200).

Department website content should also be made available to persons with disabilities in an alternative format upon request, if reasonably practicable.

344.9 DOCUMENTATION

Whenever any modification has been provided, the member involved should document:

- (a) The type of modification, assistive device, auxiliary aid, or service provided.
- (b) Whether the individual elected to use an assistive device, auxiliary aid, or service provided by the Department or another identified source, as applicable.
- (c) Whether the individual's express preference for the modification was not honored and the reason why an alternative method was used.

The documentation and any written communications exchanged should be maintained consistent with the Records Maintenance and Release Policy.

All written communications exchanged in a criminal case shall be attached to the member's report or placed into evidence.

344.10 COMPLAINTS

A member who receives a complaint or becomes aware of potential disability discrimination, an ADA violation, or a person's inability to access the department's programs, services, or activities should document the complaint and promptly refer the matter to the ADA coordinator (28 CFR 35.107). The Department shall assist persons with disabilities who require assistance to file a complaint regarding members of this department. The Department may provide a qualified interpreter or forms in enlarged print, as appropriate.

344.11 TRAINING

Members should receive periodic training on ADA compliance, to include:

- (a) Awareness and understanding of this policy, related procedures, forms, and available resources.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

ADA Compliance

- (b) Procedures for handling requests for modifications.
- (c) Accessing assistive devices, auxiliary aids, and services needed to accommodate requests for modifications.
- (d) General requirements of the ADA, including modifying policies and practices, communicating with individuals with disabilities, and identifying alternate ways to provide access to programs, services, and activities as appropriate to the member's job duties.

Management staff, even if they do not interact regularly with individuals with disabilities, should receive training as appropriate to understand and reinforce this policy.

The Support Services Commander should maintain records of all training provided and retain a copy in each member's training file in accordance with the established records retention schedule.

344.11.1 CALL-TAKER TRAINING

Emergency call-takers shall be trained in the use of department assistive devices, auxiliary aids, and services for communicating with individuals with communication-related disabilities. Such training and information should include:

- (a) The requirements of the ADA and Section 504 of the Rehabilitation Act for telephone emergency service providers.
- (b) ASL syntax and accepted abbreviations.
- (c) Practical instruction on identifying and processing calls using TTY, TDD, or other voice, text, and video-based communications products and systems.
- (d) Hands-on experience in using TTY, TDD, or other voice, text, and video-based communications products and systems.

Training should be provided for all Dispatch members who may have contact with individuals from the public who have communication-related disabilities. Refresher training should be provided as appropriate.

Chapter 4 - Patrol Operations

Patrol Function

400.1 PURPOSE AND SCOPE

The purpose of this policy is to define the functions of the patrol unit of the Department to ensure intra-organization cooperation and information sharing.

400.1.1 FUNCTION

Officers will generally patrol in clearly marked vehicles, patrol assigned jurisdictional areas of South Saint Paul, respond to calls for assistance, act as a deterrent to crime, enforce state, local and, when authorized or empowered by agreement or statute, federal laws and respond to emergencies 24 hours per day, seven days per week.

Patrol will generally provide the following services within the limits of available resources:

- (a) Patrol that is directed at the prevention of criminal acts, traffic violations and collisions, the maintenance of public order and the discovery of hazardous situations or conditions.
- (b) Crime prevention activities, such as residential inspections, business inspections and community presentations.
- (c) Calls for service, both routine and emergency.
- (d) Investigation of both criminal and non-criminal acts.
- (e) The apprehension of criminal offenders.
- (f) Community Oriented Policing and problem-solving activities, such as citizen assists and individual citizen contacts of a positive nature.
- (g) The sharing of information between the Patrol and other division within the Department, as well as other government agencies.
- (h) The application of resources to specific problems or situations within the community that may be improved or resolved by Community Oriented Policing and problem-solving strategies.
- (i) Traffic direction and control.

400.1.2 TERRORISM

It is the goal of the South Saint Paul Police Department to make every reasonable effort to accurately and appropriately gather and report any information that may relate to either foreign or domestic terrorism. Officers should advise a supervisor as soon as practicable of any activity believed to be terrorism related and should document such incidents with a written report and advisory to the appropriate state agency. The supervisor should ensure that all terrorism-related reports are forwarded to the Investigations Supervisor in a timely fashion.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Patrol Function

400.2 PATROL INFORMATION SHARING PROCEDURES

The following guidelines are intended to develop and maintain intra-organization cooperation and information flow between the various divisions of the South Saint Paul Police Department.

400.2.1 CRIME REPORTS

A crime report may be completed by any patrol officer who receives criminal information. The report will be processed and forwarded to the appropriate bureau for retention or follow-up investigation.

400.2.2 PATROL BRIEFINGS

Patrol supervisors, investigative sergeants and special unit sergeants are encouraged to share information as much as reasonably possible. All supervisors and/or officers will be provided an opportunity to share information through daily briefings, via email and E-briefing as time permits.

400.3 CROWDS, EVENTS AND GATHERINGS

Officers may encounter gatherings of people, including but not limited to, civil demonstrations, civic, social and business events, public displays, parades and sporting events. Officers should monitor such events as time permits in an effort to keep the peace and protect the safety and rights of those present. A patrol supervisor should be notified when it becomes reasonably foreseeable that such an event may require increased monitoring, contact or intervention.

Officers responding to an event or gathering that warrants law enforcement involvement should carefully balance the speech and association rights of those present with applicable public safety concerns before taking enforcement action. Officers are encouraged to contact organizers or responsible persons to seek voluntary compliance that may address relevant public safety/order concerns.

Officers should consider enforcement of applicable state and local laws, when the activity blocks the entrance or egress of a facility or location and when voluntary compliance with the law is not achieved.

Bias-Based Policing

401.1 PURPOSE AND SCOPE

This policy provides guidance to department members that affirms the South Saint Paul Police Department's commitment to policing that is fair and objective.

Nothing in this policy prohibits the use of specified characteristics in law enforcement activities designed to strengthen the department's relationship with its diverse communities (e.g., cultural and ethnicity awareness training, youth programs, community group outreach, partnerships).

401.1.1 DEFINITIONS

Definitions related to this policy include:

Bias-based policing or improper profiling - An inappropriate reliance on actual or perceived characteristics such as race, ethnicity, national origin (including limited English proficiency), religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, disability, or affiliation with any non-criminal group (protected characteristics) as the basis for providing differing law enforcement service or enforcement. This includes explicit and implicit biases (i.e., conscious and unconscious beliefs or attitudes towards certain groups).

This also includes use of racial or ethnic stereotypes as factors in selecting whom to stop and search. It does not include law enforcement's use of race or ethnicity to determine whether a person matches a specific description of a particular subject (Minn. Stat. § 626.8471).

401.2 POLICY

The South Saint Paul Police Department is committed to providing law enforcement services to the community with due regard for the racial, cultural or other differences of those served. It is the policy of this department to provide law enforcement services and to enforce the law equally, fairly, objectively and without discrimination toward any individual or group (Minn. Stat. § 626.8471, Subd. 3).

401.3 BIAS-BASED POLICING PROHIBITED

Bias-based policing is strictly prohibited.

However, nothing in this policy is intended to prohibit an officer from considering protected characteristics in combination with credible, timely and distinct information connecting a person or people of a specific characteristic to a specific unlawful incident, or to specific unlawful incidents, specific criminal patterns or specific schemes.

401.4 MEMBER RESPONSIBILITIES

Every member of this department shall perform his/her duties in a fair and objective manner and is responsible for promptly reporting any suspected or known instances of bias-based policing to a supervisor. Members should, when reasonable to do so, intervene to prevent any biased-based actions by another member.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Bias-Based Policing

401.4.1 REASON FOR CONTACT

Officers contacting a person shall be prepared to articulate sufficient reason for the contact, independent of the protected characteristics of the individual.

To the extent that written documentation would otherwise be completed (e.g., arrest report, Field Interview (FI) card), the involved officer should include those facts giving rise to the contact, as applicable.

Except for required data-collection forms or methods, nothing in this policy shall require any officer to document a contact that would not otherwise require reporting.

401.4.2 INFORMATION TO BE PROVIDED

Officers shall (Minn. Stat. § 626.8471, Subd. 3):

- (a) Introduce or identify themselves and state the reason for a contact as soon as practicable unless providing the information could compromise officer or public safety.
- (b) Attempt to answer questions the person may have regarding the contact, including relevant referrals to other agencies when appropriate.
- (c) Explain the reason for the contact if it is determined the reasonable suspicion was unfounded.
- (d) When requested, provide their name and badge number and identify this department during routine stops.
- (e) When requested, officers should inform a member of the public of the process to file a misconduct complaint for bias-based policing against a member of the Department, and that bias-based policing complaints may be made by calling the Attorney General's office (Minn. Stat. § 626.9514).

401.5 SUPERVISOR RESPONSIBILITIES

Supervisors should monitor those individuals under their command for compliance with this policy and shall handle any alleged or observed violations in accordance with the Personnel Complaints Policy.

- (a) Supervisors should discuss any issues with the involved officer and his/her supervisor in a timely manner.
 - 1. Supervisors should document these discussions, in the prescribed manner.
- (b) Supervisors should periodically review MAV recordings, portable audio/video recordings, Mobile Digital Computer (MDC) data and any other available resource used to document contact between officers and the public to ensure compliance with this policy.
 - 1. Supervisors should document these periodic reviews.
 - 2. Recordings that capture a potential instance of bias-based policing should be appropriately retained for administrative investigation purposes.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Bias-Based Policing

- (c) Supervisors shall initiate investigations of any actual or alleged violations of this policy.
- (d) Supervisors should take prompt and reasonable steps to address any retaliatory action taken against any member of this department who discloses information concerning bias-based policing.

401.6 TRAINING

Training on fair and objective policing and review of this policy shall be conducted annually and include:

- (a) Explicit and implicit biases.
- (b) Avoiding improper profiling.

401.6.1 ADDITIONAL TRAINING REQUIREMENTS

The Support Services Commander should ensure that Board of Peace Officer Standards and Training (POST) approved in-service training is provided to officers on recognizing and valuing community diversity and cultural differences, including implicit bias, as required by Minn. Stat. § 626.8469, Subd. 1.

The Chief of Police and supervisors should receive and review training materials prepared by POST on how to detect and respond to racial profiling (Minn. Stat. § 626.8471, Subd. 7).

Crime and Disaster Scene Integrity

402.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance in handling a major crime or disaster.

402.2 POLICY

It is the policy of the South Saint Paul Police Department to secure crime or disaster scenes so that evidence is preserved, and to identify and mitigate the dangers associated with a major crime or disaster scene for the safety of the community and those required to enter or work near the scene.

402.3 SCENE RESPONSIBILITY

The first officer at the scene of a crime or major incident is generally responsible for the immediate safety of the public and preservation of the scene. Officers shall also consider officer safety and the safety of those persons entering or exiting the area, including those rendering medical aid to any injured parties. Once an officer has assumed or been assigned to maintain the integrity and security of the crime or disaster scene, the officer shall maintain the crime or disaster scene until he/she is properly relieved by a supervisor or other designated person.

402.4 FIRST RESPONDER CONSIDERATIONS

The following list generally describes the first responder's function at a crime or disaster scene. This list is not intended to be all-inclusive, is not necessarily in order and may be altered according to the demands of each situation:

- (a) Broadcast emergency information, including requests for additional assistance and resources.
- (b) Provide for the general safety of those within the immediate area by mitigating, reducing or eliminating threats or dangers.
- (c) Locate or identify suspects and determine whether dangerous suspects are still within the area.
- (d) Provide first aid to injured parties if it can be done safely.
- (e) Evacuate the location safely as required or appropriate.
- (f) Secure the inner perimeter.
- (g) Protect items of apparent evidentiary value.
- (h) Secure an outer perimeter.
- (i) Identify potential witnesses.
- (j) Start a chronological log noting critical times and personnel allowed access.

402.5 SEARCHES

Officers arriving at crime or disaster scenes are often faced with the immediate need to search for and render aid to victims, and to determine if suspects are present and continue to pose a threat. Once officers are satisfied that no additional suspects are present and/or there are no injured

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Crime and Disaster Scene Integrity

persons to be treated, those exigent circumstances will likely no longer exist. Officers should thereafter secure the scene and conduct no further search until additional or alternate authority for the search is obtained, such as consent or a search warrant.

402.5.1 CONSENT

When possible, officers should seek written consent to search from authorized individuals. However, in the case of serious crimes or major investigations, it may be prudent to also obtain a search warrant. Consent as an additional authorization may be sought, even in cases where a search warrant has been granted.

402.6 EXECUTION OF HEALTH ORDERS

Any licensed member of this department may assist in the enforcement of all directives of the local health officer issued for the purpose of preventing the spread of any contagious, infectious, or communicable disease (Minn. Stat. § 144.4195, Subd. 2(c)).

Ride-Along Policy

403.1 PURPOSE AND SCOPE

The Ride-Along Program provides an opportunity for persons to experience the law enforcement function first hand. This policy provides the requirements, approval process and hours of operation for the Ride-Along Program.

403.1.1 ELIGIBILITY

The South Saint Paul Police Department Ride-Along Program is offered to residents, students, family members of department employees, outside law enforcement officials and those employed within the City. Every reasonable attempt will be made to accommodate interested persons. Any applicant may be disqualified with or without cause from participating in the program.

The following factors may be considered in disqualifying an applicant and are not limited to:

- Being under 18 years of age.
- Prior criminal history.
- Pending criminal action.
- Pending lawsuit against the Department.
- Denial by any supervisor.

403.2 PROCEDURE TO REQUEST A RIDE-ALONG

Generally, ride-along requests will be scheduled by the Sergeant. The participant will complete and sign a ride-along waiver form. Information requested will include a valid driver's license, address and telephone number.

The Sergeant will schedule a date, based on availability, at least one week after the date of application. If approved, a copy of the ride-along waiver form will be forwarded to the respective Sergeant as soon as possible for his/her scheduling considerations.

If the ride-along is denied after the request has been made, a representative of the Department will contact the applicant and advise him/her of the denial.

403.2.1 PROGRAM REQUIREMENTS

Once approved, civilian ride-alongs will be allowed to ride no more than once every six months. An exception would apply to the following: cadets, Explorers, RSVP, chaplains, Reserves, police applicants, department interns, law enforcement students and all others with approval of the Sergeant.

An effort will be made to ensure that no more than one citizen will participate in a ride-along during any given time period. Normally, no more than one ride-along will be allowed in the officer's vehicle at a given time.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Ride-Along Policy

403.2.2 SUITABLE ATTIRE

Any person approved to ride-along is required to be suitably dressed in collared shirt, blouse or jacket, slacks and shoes. Sandals, T-shirts, tank tops, shorts and ripped or torn blue jeans are not permitted. Hats and ball caps will not be worn in the police vehicle. The supervisor may refuse a ride-along to anyone not properly dressed.

403.2.3 PEACE OFFICER RIDE-ALONGS

Off-duty members of this department or any other law enforcement agency will not be permitted to ride-along with on-duty officers without the express consent of the Sergeant. In the event that such a ride-along is permitted, the off-duty employee shall not be considered on-duty and shall not represent him/herself as a peace officer or participate in any law enforcement activity except as emergency circumstances may require.

403.2.4 RIDE-ALONG CRIMINAL HISTORY CHECK

All ride-along applicants are subject to a criminal history check. The criminal history check may include a local records check and a Minnesota Bureau of Criminal Apprehension Criminal History System check prior to approval (provided that the ride-along is not an employee of the South Saint Paul Police Department).

403.3 OFFICER'S RESPONSIBILITIES

The officer shall advise the dispatch and other on-duty officers that a ride-along is present in the vehicle before going into service. Officers shall consider the safety of the ride-along at all times.

Officers should use sound discretion when encountering a potentially dangerous situation, and if feasible, let the participant out of the vehicle in a well-lighted place of safety. The dispatcher will be advised of the situation and as soon as practicable have another police unit respond to pick up the participant at that location. The ride-along may be continued or terminated at this time.

Conduct by a person participating in a ride-along that results in termination of the ride or is otherwise inappropriate should be immediately reported to the Sergeant.

The Sergeant is responsible for maintaining and scheduling ride-alongs. Upon completion of the ride-along, a copy of the ride-along waiver form shall be returned to the Sergeant with any comments that may be offered by the officer.

403.4 CONTROL OF RIDE-ALONG

The assigned employee shall maintain control over the ride-along at all times and instruct him/her in the conditions that necessarily limit participation. These instructions should include:

- (a) The ride-along will follow the directions of the officer.
- (b) The ride-along will not become involved in any investigation, handling of evidence, discussions with victims or suspects or handling any police equipment.
- (c) The ride-along may terminate the ride at any time and the officer may return the observer to his/her home or to the station if the ride-along interferes with the performance of the officer's duties.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Ride-Along Policy

- (d) The officer may terminate the ride-along and return the observer to their home or to the station if the ride-along interferes with the performance of any officer's duties.
- (e) Ride-alongs may be allowed to continue riding during the transportation and booking process provided this does not jeopardize their safety.
- (f) Officers will not allow any ride-alongs to be present in any residence or situation that would jeopardize their safety or cause undue stress or embarrassment to a victim or any other person.

Hazardous Material Response

404.1 PURPOSE AND SCOPE

Hazardous materials present a potential harm to employees as a result of their exposure. To comply with Minnesota law, the following represents the policy of this department.

404.1.1 HAZARDOUS MATERIAL DEFINED

Hazardous material - Any refuse, sludge or other waste material or combinations of refuse, sludge or other waste materials in solid, semisolid, liquid or contained gaseous form, which, because of its quantity, concentration, or chemical, physical or infectious characteristics may (Minn. Stat. § 116.06 Subd. 11):

- (a) Cause or significantly contribute to an increase in mortality or an increase in serious irreversible or incapacitating reversible illness.
- (b) Pose a substantial present or potential hazard to human health or the environment when improperly treated, stored, transported, disposed of or otherwise managed.

404.2 HAZARDOUS MATERIAL RESPONSE

Employees may encounter situations involving suspected hazardous materials, such as at the scene of a traffic collision, chemical spill or fire. When employees come into contact with a suspected hazardous material, certain steps should be taken to protect themselves and other persons.

The fire department is the agency trained and equipped to properly respond and mitigate most hazardous materials and biohazards.

Responders should not perform tasks or use equipment absent proper training. A responder entering the area may require decontamination before he/she is allowed to depart the scene and should be evaluated by appropriate technicians and medical professionals for signs of exposure.

The following steps should be considered at any scene involving suspected hazardous materials:

- (a) Attempt to identify the type of hazardous material. Identification can be determined by placard, driver's manifest or statements from the person transporting the material
- (b) Notify the appropriate fire department.
- (c) Provide first aid to injured parties if it can be done safely and without contamination.
- (d) Begin evacuation of the immediate and surrounding areas dependent on the material. Voluntary evacuation should be considered. Depending on the material, mandatory evacuation may be necessary.
- (e) Contact the Minnesota Duty Officer (800-422-0798).
- (f) Responders should remain uphill and upwind of the hazard until a zone of entry and a decontamination area are established.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Hazardous Material Response

404.3 REPORTING EXPOSURE(S)

Department personnel who believe that they have been exposed to a hazardous material shall immediately report the exposure to a supervisor. Each exposure shall be documented in an incident report that shall be forwarded via chain of command to their Division Commander. Should the affected employee be unable to document the exposure for any reason, it shall be the responsibility of the notified supervisor to complete the incident report.

Injury or illness caused or believed to be caused from exposure to hazardous materials shall be reported the same as any other on-duty injury or illness, in addition to a crime report or incident report.

404.3.1 SUPERVISOR RESPONSIBILITIES

When a supervisor has been informed that an employee has been exposed to a hazardous material, he/she shall ensure that immediate medical treatment is obtained and appropriate action is taken to lessen the exposure.

To ensure the safety of employees, safety equipment is available through supervisory personnel. Safety items not maintained by the Department will be obtained through the appropriate fire department.

Hostage and Barricade Incidents

405.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for situations where officers have legal cause to contact, detain or arrest a person, and the person refuses to submit to the lawful requests of the officers by remaining in a structure or vehicle and/or by taking a hostage.

The scope of this policy is not intended to address all variables that officers encounter during their initial response or when a hostage or barricade situation has developed. This policy does not require or purport to recommend specific strategies or tactics for resolution as each incident is a dynamic and rapidly evolving event.

405.1.1 DEFINITIONS

Definitions related to this policy include:

Barricade situation - An incident where a person maintains a position of cover or concealment and ignores or resists law enforcement personnel, and it is reasonable to believe the subject is armed with a dangerous or deadly weapon.

Hostage situation - An incident where it is reasonable to believe a person is unlawfully held by a hostage-taker as security so that specified terms or conditions will be met.

405.2 POLICY

It is the policy of the South Saint Paul Police Department to address hostage and barricade situations with due regard for the preservation of life and balancing the risk of injury, while obtaining the safe release of hostages, apprehending offenders and securing available evidence.

405.3 COMMUNICATION

When circumstances permit, initial responding officers should try to establish and maintain lines of communication with a barricaded person or hostage-taker. Officers should attempt to identify any additional subjects, inquire about victims and injuries, seek the release of hostages, gather intelligence information, identify time-sensitive demands or conditions and obtain the suspect's surrender.

When available, department-authorized negotiators should respond to the scene as soon as practicable and assume communication responsibilities. Negotiators are permitted to exercise flexibility in each situation based upon their training, the circumstances presented, suspect actions or demands and the available resources.

405.3.1 EMERGENCY COMMUNICATION

A supervisor with probable cause to believe that a person is being unlawfully confined may order a telephone company to cut, reroute, or divert telephone lines for the purpose of establishing and controlling communications with a suspect (Minn. Stat. § 609.774).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Hostage and Barricade Incidents

405.4 FIRST RESPONDER CONSIDERATION

First responding officers should promptly and carefully evaluate all available information to determine whether an incident involves, or may later develop into, a hostage or barricade situation.

The first responding officer should immediately request a supervisor's response as soon as it is determined that a hostage or barricade situation exists. The first responding officer shall assume the duties of the supervisor until relieved by a supervisor or a more qualified responder. The officer shall continually evaluate the situation, including the level of risk to officers, to the persons involved and to bystanders, and the resources currently available.

The handling officer should brief the arriving supervisor of the incident, including information about suspects and victims, the extent of any injuries, additional resources or equipment that may be needed, and current perimeters and evacuation areas.

405.4.1 BARRICADE SITUATION

Unless circumstances require otherwise, officers handling a barricade situation should attempt to avoid a forceful confrontation in favor of stabilizing the incident by establishing and maintaining lines of communication while awaiting the arrival of specialized personnel and trained negotiators. During the interim the following options, while not all-inclusive or in any particular order, should be considered:

- (a) Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.
- (b) Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.
- (c) Request additional personnel, resources and equipment as needed (e.g., canine team, air support).
- (d) Provide responding emergency personnel with a safe arrival route to the location.
- (e) Evacuate non-injured persons in the immediate threat area if it is reasonably safe to do so.
- (f) Attempt or obtain a line of communication and gather as much information on the subject as possible, including weapons, other involved parties, additional hazards or injuries.
- (g) Establish an inner and outer perimeter as circumstances require and resources permit to prevent unauthorized access.
- (h) Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.
- (i) Determine the need for and notify the appropriate persons within and outside the Department, such as command officers and the Police Chief.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Hostage and Barricade Incidents

- (j) If necessary and available, establish a tactical or exclusive radio frequency for the incident.
- (k) Establish a command post.

405.4.2 HOSTAGE SITUATION

Officers presented with a hostage situation should attempt to avoid a forceful confrontation in favor of controlling the incident in anticipation of the arrival of specialized personnel and trained hostage negotiators. However, it is understood that hostage situations are dynamic and can require that officers react quickly to developing or changing threats. The following options while not all-inclusive or in any particular order, should be considered:

- Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.
- Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.
- Establish a rapid response team in the event it becomes necessary to rapidly enter a building, structure or vehicle, such as when the suspect is using deadly force against any hostages (see the Rapid Response and Deployment Policy).
- Assist hostages or potential hostages to escape if it is reasonably safe to do so. Hostages should be kept separated if practicable pending further interview.
- Request additional personnel, resources and equipment as needed (e.g., canine team, air support).
- Provide responding emergency personnel with a safe arrival route to the location.
- Evacuate non-injured persons in the immediate threat area if it is reasonably safe to do so.
- Coordinate pursuit or surveillance vehicles and control of travel routes.
- Attempt or obtain a line of communication and gather as much information about the suspect as possible, including any weapons, victims and their injuries, additional hazards, other involved parties and any other relevant intelligence information.
- Establish an inner and outer perimeter as resources and circumstances permit to prevent unauthorized access.
- Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.
- Determine the need for and notify the appropriate persons within and outside the Department, such as command officers and the Police Chief.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Hostage and Barricade Incidents

- If necessary and available, establish a tactical or exclusive radio frequency for the incident.

405.5 SUPERVISOR RESPONSIBILITY

Upon being notified that a hostage or barricade situation exists, the supervisor should immediately respond to the scene, assess the risk level of the situation, establish a proper chain of command and assume the role of Incident Commander until properly relieved. This includes requesting a [CRU] response if appropriate and apprising the [CRU] Commander of the circumstances. In addition, the following options, listed here in no particular order, should be considered:

- (a) Ensure injured persons are evacuated and treated by medical personnel.
- (b) Ensure the completion of necessary first responder responsibilities or assignments.
- (c) Request crisis negotiators, specialized units, additional personnel, resources or equipment as appropriate.
- (d) Establish a command post location as resources and circumstances permit.
- (e) Designate assistants who can help with intelligence information and documentation of the incident.
- (f) If it is practicable to do so, arrange for video documentation of the operation.
- (g) Consider contacting utility and communication providers when restricting such services (e.g., restricting electric power, gas, telephone service).
- (h) Ensure adequate law enforcement coverage for the remainder of the City during the incident. The supervisor should direct non-essential personnel away from the scene unless they have been summoned by the supervisor or Dispatch.
- (i) Identify a media staging area outside the outer perimeter and have the department Police Chief or a designated temporary media representative provide media access in accordance with the Media Relations Policy
- (j) Identify the need for mutual aid and the transition or relief of personnel for incidents of extended duration.
- (k) Debrief personnel and review documentation as appropriate.

405.6 TACTICAL TEAM RESPONSE

It will be the Incident Commander's decision, with input from the Tactical Team Commander, whether to deploy the tactical team during a hostage or barricade situation. Once the Incident Commander authorizes deployment, the Tactical Team Commander or the authorized designee will be responsible for the tactical portion of the operation. The Incident Commander shall continue supervision of the command post operation, outer perimeter security and evacuation, media access and support for the tactical team. The Incident Commander and the Tactical Team Commander or the authorized designee shall maintain communications at all times.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Hostage and Barricade Incidents

405.7 REPORTING

Unless otherwise relieved by a supervisor or Incident Commander, the handling officer at the scene is responsible for completion and/or coordination of incident reports.

Response to Bomb Calls

406.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to assist members of the South Saint Paul Police Department in their initial response to incidents involving explosives, explosive devices, explosion/bombing incidents or threats of such incidents. Under no circumstances should these guidelines be interpreted as compromising the safety of first responders or the public. When confronted with an incident involving explosives, safety should always be the primary consideration.

406.2 POLICY

It is the policy of the South Saint Paul Police Department to place a higher priority on the safety of persons and the public over damage or destruction to public or private property.

406.3 RECEIPT OF BOMB THREAT

Department members receiving a bomb threat should obtain as much information from the individual as reasonably possible, including the type, placement and alleged detonation time of the device.

If the bomb threat is received on a recorded line, reasonable steps should be taken to ensure that the recording is preserved in accordance with established department evidence procedures.

The member receiving the bomb threat should ensure that the Sergeant is immediately advised and informed of the details. This will enable the Sergeant to ensure that the appropriate personnel are dispatched and, as appropriate, the threatened location is given an advance warning.

406.4 GOVERNMENT FACILITY OR PROPERTY

A bomb threat targeting a government facility may require a different response based on the government agency.

406.4.1 SOUTH SAINT PAUL POLICE DEPARTMENT FACILITY

If the bomb threat is against the South Saint Paul Police Department facility, the Sergeant will direct and assign officers as required for coordinating a general building search or evacuation of the police department, as he/she deems appropriate.

406.4.2 OTHER COUNTY OR MUNICIPAL FACILITY OR PROPERTY

If the bomb threat is against a county or municipal facility within the jurisdiction of the South Saint Paul Police Department that is not the property of this department, the appropriate agency will be promptly informed of the threat. Assistance to the other entity may be provided as the Sergeant deems appropriate.

406.4.3 FEDERAL BUILDING OR PROPERTY

If the bomb threat is against a federal building or property, the Federal Protective Service should be immediately notified. The Federal Protective Service provides a uniformed law enforcement response for most facilities, which may include use of its Explosive Detector Dog teams.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Response to Bomb Calls

If the bomb threat is against a federal government property where the Federal Protective Service is unable to provide a timely response, the appropriate facility's security or command staff should be notified.

Bomb threats against a military installation should be reported to the military police or other military security responsible for the installation.

406.5 PRIVATE FACILITY OR PROPERTY

When a member of this department receives notification of a bomb threat at a location in the City of South Saint Paul, the member receiving the notification should obtain as much information as reasonably possible from the notifying individual, including:

- (a) The location of the facility.
- (b) The nature of the threat.
- (c) Whether the type and detonation time of the device is known.
- (d) Whether the facility is occupied, and if so, the number of occupants currently on-scene.
- (e) Whether the individual is requesting police assistance at the facility.
- (f) Whether there are any internal facility procedures regarding bomb threats in place, such as:
 - 1. No evacuation of personnel and no search for a device.
 - 2. Search for a device without evacuation of personnel.
 - 3. Evacuation of personnel without a search for a device.
 - 4. Evacuation of personnel and a search for a device.

The member receiving the bomb threat information should ensure that the Sergeant is immediately notified so that he/she can communicate with the person in charge of the threatened facility.

406.5.1 ASSISTANCE

The Sergeant should be notified when police assistance is requested. The Sergeant will make the decision whether the Department will render assistance and at what level. Information and circumstances that indicate a reasonably apparent, imminent threat to the safety of either the facility or the public may require a more active approach, including police control over the facility.

Should the Sergeant determine that the Department will assist or control such an incident, he/she will determine:

- (a) The appropriate level of assistance.
- (b) The plan for assistance.
- (c) Whether to evacuate and/or search the facility.
- (d) Whether to involve facility staff in the search or evacuation of the building.
 - 1. The person in charge of the facility should be made aware of the possibility of damage to the facility as a result of a search.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Response to Bomb Calls

2. The safety of all participants is the paramount concern.
- (e) The need for additional resources, including:
 1. Notification and response, or standby notice, for fire and emergency medical services.

Even though a facility does not request police assistance to clear the interior of a building, based upon the circumstances and known threat, officers may be sent to the scene to evacuate other areas that could be affected by the type of threat, or for traffic and pedestrian control.

406.6 FOUND DEVICE

When handling an incident involving a suspected explosive device, the following guidelines, while not all inclusive, should be followed:

- (a) No known or suspected explosive item should be considered safe regardless of its size or apparent packaging.
- (b) The device should not be touched or moved except by the bomb squad or military explosive ordnance disposal team.
- (c) Personnel should not transmit on any equipment that is capable of producing radio frequency energy within the evacuation area around the suspected device. This includes the following:
 1. Two-way radios
 2. Cell phones
 3. Other personal communication devices
- (d) The appropriate bomb squad or military explosive ordnance disposal team should be summoned for assistance.
- (e) The largest perimeter reasonably possible should initially be established around the device based upon available personnel and the anticipated danger zone.
- (f) A safe access route should be provided for support personnel and equipment.
- (g) Search the area for secondary devices as appropriate and based upon available resources.
- (h) Consider evacuation of buildings and personnel near the device or inside the danger zone and the safest exit route.
- (i) Promptly relay available information to the Sergeant including:
 1. The time of discovery.
 2. The exact location of the device.
 3. A full description of the device (e.g., size, shape, markings, construction).
 4. The anticipated danger zone and perimeter.
 5. The areas to be evacuated or cleared.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Response to Bomb Calls

406.7 EXPLOSION/BOMBING INCIDENTS

When an explosion has occurred, there are multitudes of considerations which may confront the responding officers. As in other catastrophic events, a rapid response may help to minimize injury to victims, minimize contamination of the scene by gathering crowds, or minimize any additional damage from fires or unstable structures.

406.7.1 CONSIDERATIONS

Officers responding to explosions, whether accidental or a criminal act, should consider the following actions:

- (a) Assess the scope of the incident, including the number of victims and extent of injuries.
- (b) Request additional personnel and resources, as appropriate.
- (c) Assist with first aid.
- (d) Identify and take appropriate precautions to mitigate scene hazards, such as collapsed structures, bloodborne pathogens and hazardous materials.
- (e) Assist with the safe evacuation of victims, if possible.
- (f) Establish an inner perimeter to include entry points and evacuation routes. Search for additional or secondary devices.
- (g) Preserve evidence.
- (h) Establish an outer perimeter and evacuate if necessary.
- (i) Identify witnesses.

406.7.2 NOTIFICATIONS

When an explosion has occurred, the following people should be notified as appropriate:

- Fire department
- Bomb squad
- Additional department personnel, such as investigators and forensic services
- Field supervisor
- Sergeant
- Other law enforcement agencies, including local, state or federal agencies, such as the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Other government agencies, as appropriate

406.7.3 CROWD CONTROL

Only authorized members with a legitimate need should be permitted access to the scene. Spectators and other unauthorized individuals should be restricted to a safe distance as is reasonably practicable given the available resources and personnel.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Response to Bomb Calls

406.7.4 PRESERVATION OF EVIDENCE

As in any other crime scene, steps should immediately be taken to preserve the scene. The Sergeant should assign officers to protect the crime scene area, which could extend over a long distance. Consideration should be given to the fact that evidence may be imbedded in nearby structures or hanging in trees and bushes.

Civil Commitments

407.1 PURPOSE AND SCOPE

This policy provides guidelines for when officers may place an individual in protective custody and request a 72-hour hold under the Minnesota Commitment and Treatment Act (Minn. Stat. § 253B.051).

407.2 POLICY

It is the policy of the South Saint Paul Police Department to protect the public and individuals through legal and appropriate use of the 72-hour hold process.

407.3 AUTHORITY

An officer, having probable cause to believe that any individual because of mental illness, chemical dependency, or public intoxication is in danger of injuring him/herself or others if not immediately detained, may take, or cause to be taken, the individual to an appropriate treatment facility for a 72-hour evaluation (Minn. Stat. § 253B.051, Subd. 1).

The officer shall make written application for admission of the individual to an appropriate treatment facility. The application shall contain the officer's reasons for and circumstances under which the individual was taken into custody. If danger to specific individuals is a basis for the requested emergency hold, the statement must include identifying information for those individuals to the extent reasonably practicable. The officer shall also provide the department contact information for purposes of receiving notice if the individual is released prior to the 72-hour admission or leaves the facility without consent. The facility shall make a copy of the statement available to the individual taken into custody (Minn. Stat. § 253B.051, Subd. 1).

407.3.1 VOLUNTARY EVALUATION

If an officer encounters an individual who may qualify for a 72-hour hold, he/she may inquire as to whether the person desires to voluntarily be evaluated at an appropriate facility. If the individual so desires, the officers should:

- (a) Transport the individual to an appropriate facility that is able to conduct the evaluation and admit the person pursuant to the Minnesota Commitment and Treatment Act.
- (b) If at any point the individual changes his/her mind regarding voluntary evaluation, officers should proceed with the application for a 72-hour hold, if appropriate.
- (c) Document the circumstances surrounding the individual's desire to pursue voluntary evaluation and/or admission.

407.4 CONSIDERATIONS AND RESPONSIBILITIES

Any officer handling a call involving an individual who may qualify for a 72-hour hold should consider, as time and circumstances reasonably permit:

- (a) Available information that might assist in determining the cause and nature of the individual's action or stated intentions.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Civil Commitments

- (b) Community or neighborhood mediation services.
- (c) Conflict resolution and de-escalation techniques.
- (d) Community or other resources available to assist in dealing with mental health issues.

While these steps are encouraged, nothing in this section is intended to dissuade officers from taking reasonable action to ensure the safety of the officers and others.

407.5 TRANSFER TO APPROPRIATE FACILITY

Upon arrival of the ambulance, If the individual is not seeking treatment voluntarily, the officer should provide the medic with the written application for a 72-hour hold and remain present to provide clarification of the grounds for detention, upon request.

407.6 DOCUMENTATION

The officer should complete an application for emergency admission, provide it to the medic and retain a copy of the application for inclusion in the case report.

The officer should also provide a verbal summary to the medics regarding the circumstances leading to the involuntary detention.

407.7 CRIMINAL OFFENSES

Officers investigating an individual who is suspected of committing a minor criminal offense and who is being taken into custody for purposes of a 72-hour hold should resolve the criminal matter by issuing a warning or a citation, as appropriate.

When an individual who may qualify for a 72-hour hold has committed a serious criminal offense that would normally result in an arrest and transfer to a jail facility, the officer should:

- (a) Arrest the individual when there is probable cause to do so.
- (b) Notify the appropriate supervisor of the facts supporting the arrest and the facts that would support the 72-hour hold.
- (c) Facilitate the individual's transfer to jail.
- (d) Thoroughly document in the related reports the circumstances that indicate the individual may qualify for a 72-hour hold.

In the supervisor's judgment, the individual may instead be arrested or booked and transported to the appropriate mental health facility. The supervisor should consider the seriousness of the offense, the treatment options available, the ability of this department to regain custody of the individual, department resources (e.g., posting a guard) and other relevant factors in making this decision.

407.8 FIREARMS AND OTHER WEAPONS

Whenever an individual is taken into custody for a 72-hour hold, the handling officers should seek to determine if the individual owns or has access to any firearm or other deadly weapon. Officers should consider whether it is appropriate and consistent with current search and seizure law under

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Civil Commitments

the circumstances to seize any such firearms or other dangerous weapons (e.g., safekeeping, evidence, consent).

Officers are cautioned that a search warrant may be needed before entering a residence or other place to search unless lawful warrantless entry has already been made (e.g., exigent circumstances, consent). A warrant may also be needed before searching for or seizing weapons.

The handling officers should further advise the individual of the procedure for the return of any firearm or other weapon that has been taken into custody.

Citation Releases

408.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of the South Saint Paul Police Department with guidance on when to release adults who are suspected offenders on a citation for a criminal offense, rather than having the person held in custody for a court appearance or released on bail.

This policy also provides guidance on when a court orders that a person be released.

Additional release restrictions may apply to those detained for domestic violence, as outlined in the Domestic Abuse Policy.

408.2 POLICY

The South Saint Paul Police Department will consider its resources and its mission of protecting the community when exercising any discretion to release suspected offenders on a citation, when authorized to do so.

408.3 RELEASE

A suspected offender shall be released on issuance of a citation:

- (a) When the offender has been arrested without a warrant and either a prosecutor or district court judge orders that the offender should be released (Minn. R. Crim. P. 4.02; Minn. R. Crim. P. 6.01).
 - 1. Release is not required if a reviewing supervisor determines that the offender should be held pursuant to Minn. R. Crim. P. 6.01 Subd. 1.
- (b) When the offender is charged with a petty or fine-only misdemeanor (Minn. R. Crim. P. 6.01).
- (c) In misdemeanor cases unless it reasonably appears to the arresting officer that the offender will (Minn. R. Crim. P. 6.01):
 - 1. Cause bodily injury to him/herself or another if he/she is not detained.
 - 2. Continue engaging in criminal conduct.
 - 3. Not respond to a citation.
- (d) When the offender is from another state which has a reciprocal agreement with Minnesota unless the offense is (Minn. Stat. § 169.91):
 - 1. One which would result in the revocation of the offender's driver's license under Minnesota law upon conviction.
 - 2. A violation of a highway weight limitation.
 - 3. A violation of a law governing the transportation of hazardous materials.
 - 4. That the offender was driving without a valid driver's license.

408.4 PROHIBITIONS

The release of a suspected offender on a citation is not permitted when:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Citation Releases

The offender has committed a driving while impaired (DWI) offense requiring a mandatory appearance (Minn. Stat. § 169A.40; Minn. Stat. § 169.91).

- (a) The offender is arrested for a violation of state law or an ordinance related to the operation or registration of a vehicle punishable as a misdemeanor or felony and (Minn. Stat. § 169.91):
 - 1. The offender demands an immediate appearance before a judge.
 - 2. The offender is charged with:
 - (a) An offense involving an accident that resulted in injury or death.
 - (b) Criminal vehicular homicide.
 - (c) Failure to stop after being involved in an accident that resulted in death, personal injuries or damage to property.
 - 3. There is reasonable cause to believe that the offender may leave the state.

See the Domestic Abuse Policy for release restrictions related to those investigations.

408.5 FISH AND GAME AND ENVIRONMENT-RELATED OFFENSES

In the case of game and fish laws or other environment-related offenses, as specified in Minn. Stat. § 97A.211, officers should release the offender unless there is reason to believe that criminal conduct will continue or that the offender will not respond as required by the citation (Minn. Stat. § 97A.211).

Foreign Diplomatic and Consular Representatives

409.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that members of the South Saint Paul Police Department extend appropriate privileges and immunities to foreign diplomatic and consular representatives in accordance with international law.

409.2 POLICY

The South Saint Paul Police Department respects international laws related to the special privileges and immunities afforded foreign diplomatic and consular representatives assigned to the United States.

All foreign diplomatic and consular representatives shall be treated with respect and courtesy, regardless of any privileges or immunities afforded them.

409.3 CLAIMS OF IMMUNITY

If a member comes into contact with a person where law enforcement action may be warranted and the person claims diplomatic or consular privileges and immunities, the member should, without delay:

- (a) Notify a supervisor.
- (b) Advise the person that his/her claim will be investigated and he/she may be released in accordance with the law upon confirmation of the person's status.
- (c) Request the person's identification card, either issued by the U.S. Department of State (DOS), Office of the Chief of Protocol, or in the case of persons accredited to the United Nations, by the U.S. Mission to the United Nations. These are the only reliable documents for purposes of determining privileges and immunities.
- (d) Contact the DOS Diplomatic Security Command Center at 571-345-3146 or toll free at 866-217-2089, or at another current telephone number and inform the center of the circumstances.
- (e) Verify the immunity status with DOS and follow any instructions regarding further detention, arrest, prosecution and/or release, as indicated by the DOS representative. This may require immediate release, even if a crime has been committed.

Identity or immunity status should not be presumed from the type of license plates displayed on a vehicle. If there is a question as to the status or the legitimate possession of a Diplomat or Consul license plate, a query should be run via the National Law Enforcement Telecommunications System (NLETS), designating "US" as the state.

409.4 ENFORCEMENT ACTION

If the DOS is not immediately available for consultation regarding law enforcement action, members shall be aware of the following:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Foreign Diplomatic and Consular Representatives

- (a) Generally, all persons with diplomatic and consular privileges and immunities may be issued a citation or notice to appear. However, the person may not be compelled to sign the citation.
- (b) All persons, even those with a valid privilege or immunity, may be reasonably restrained in exigent circumstances for purposes of self-defense, public safety or the prevention of serious criminal acts.
- (c) An impaired foreign diplomatic or consular representative may be prevented from driving a vehicle, even if the person may not be arrested due to privileges and immunities.
 - 1. Investigations, including the request for field sobriety tests, chemical tests and any other tests regarding impaired driving may proceed but they shall not be compelled.
- (d) The following persons may not be detained or arrested, and any property or vehicle owned by these persons may not be searched or seized:
 - 1. Diplomatic-level staff of missions to international organizations and recognized family members
 - 2. Diplomatic agents and recognized family members
 - 3. Members of administrative and technical staff of a diplomatic mission and recognized family members
 - 4. Career consular officers, unless the person is the subject of a felony warrant
- (e) The following persons may generally be detained and arrested:
 - 1. International organization staff; however, some senior officers are entitled to the same treatment as diplomatic agents.
 - 2. Support staff of missions to international organizations.
 - 3. Diplomatic service staff and consular employees; however, special bilateral agreements may exclude employees of certain foreign countries.
 - 4. Honorary consular officers.

409.5 DOCUMENTATION

All contacts with persons who have claimed privileges and immunities afforded foreign diplomatic and consular representatives should be thoroughly documented and the related reports forwarded to DOS.

409.6 DIPLOMATIC IMMUNITY TABLE

Reference table on diplomatic immunity:

Category	Arrested or Detained	Enter Residence Subject to Ordinary Procedures	Issued Traffic Citation	Subpoenaed as Witness	Prosecuted	Recognized Family Members

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Foreign Diplomatic and Consular Representatives

Diplomatic Agent	No (note b)	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
Member of Admin and Tech Staff	No (note b)	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
Service Staff	Yes (note a)	Yes	Yes	Yes	No for official acts Yes otherwise (note a)	No immunity or inviolability (note a)
Career Consul Officer	Yes if for a felony and pursuant to a warrant (note a)	Yes (note d)	Yes	Yes	No for official acts Yes otherwise (note a)	No immunity or inviolability
Honorable Consul Officer	Yes	Yes	Yes	No for official acts Yes otherwise	No for official acts Yes otherwise	No immunity or inviolability
Consulate Employees	Yes (note a)	Yes	Yes	No for official acts Yes otherwise	No for official acts Yes otherwise (note a)	No immunity or inviolability (note a)
Int'l Org Staff (note b)	Yes (note c)	Yes (note c)	Yes	Yes (note c)	No for official acts Yes otherwise (note c)	No immunity or inviolability
Diplomatic-Level Staff of Missions to Int'l Org	No (note b)	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
Support Staff of Missions to Int'l Orgs	Yes	Yes	Yes	Yes	No for official acts Yes otherwise	No immunity or inviolability

Notes for diplomatic immunity table:

- (a) This table presents general rules. The employees of certain foreign countries may enjoy higher levels of privileges and immunities on the basis of special bilateral agreements.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Foreign Diplomatic and Consular Representatives

- (b) Reasonable constraints, however, may be applied in emergency circumstances involving self-defense, public safety, or in the prevention of serious criminal acts.
- (c) A small number of senior officers are entitled to be treated identically to diplomatic agents.
- (d) Note that consul residences are sometimes located within the official consular premises. In such cases, only the official office space is protected from police entry.

Rapid Response and Deployment

410.1 PURPOSE AND SCOPE

Violence that is committed in schools, workplaces and other locations by individuals or a group of individuals who are determined to target and kill persons and to create mass casualties presents a difficult situation for law enforcement. The purpose of this policy is to identify guidelines and factors that will assist officers in situations that call for rapid response and deployment.

410.2 POLICY

The South Saint Paul Police Department will endeavor to plan for rapid response to crisis situations, and to coordinate response planning with other emergency services as well as with those that are responsible for operating sites that may be the target of a critical incident.

Nothing in this policy shall preclude the use of reasonable force, deadly or otherwise, by members of the Department in protecting themselves or others from death or serious injury.

410.3 FIRST RESPONSE

If there is a reasonable belief that acts or threats by a suspect are placing lives in imminent danger, first responding officers should consider reasonable options to reduce, prevent or eliminate the threat. Officers must decide, often under a multitude of difficult and rapidly evolving circumstances, whether to advance on the suspect, take other actions to deal with the threat or wait for additional resources.

If a suspect is actively engaged in the infliction of serious bodily harm or other life-threatening activity toward others, officers should take immediate action, if reasonably possible, while requesting additional assistance.

Officers should remain aware of the possibility that an incident may be part of a coordinated multi-location attack that may require some capacity to respond to other incidents at other locations.

When deciding on a course of action officers should consider:

- (a) Whether to advance on or engage a suspect who is still a possible or perceived threat to others. Any advance or engagement should be based on information known or received at the time.
- (b) Whether to wait for additional resources or personnel. This does not preclude an individual officer from taking immediate action.
- (c) Whether individuals who are under imminent threat can be moved or evacuated with reasonable safety.
- (d) Whether the suspect can be contained or denied access to victims.
- (e) Whether the officers have the ability to effectively communicate with other personnel or resources.
- (f) Whether planned tactics can be effectively deployed.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Rapid Response and Deployment

- (g) The availability of rifles, shotguns, shields, breaching tools, control devices and any other appropriate tools, and whether the deployment of these tools will provide a tactical advantage.

In a case of a barricaded suspect with no hostages and no immediate threat to others, officers should consider summoning and waiting for additional assistance (special tactics and/or hostage negotiation team response).

410.4 CONSIDERATIONS

When dealing with a crisis situation members should:

- (a) Assess the immediate situation and take reasonable steps to maintain operative control of the incident.
- (b) Obtain, explore and analyze sources of intelligence and known information regarding the circumstances, location and suspect involved in the incident.
- (c) Attempt to attain a tactical advantage over the suspect by reducing, preventing or eliminating any known or perceived threat.
- (d) Attempt, if feasible and based upon the suspect's actions and danger to others, a negotiated surrender of the suspect and release of the hostages.

410.5 PLANNING

The Patrol Division Commander should coordinate critical incident planning. Planning efforts should consider:

- (a) Identification of likely critical incident target sites, such as schools, shopping centers, entertainment and sporting event venues.
- (b) Availability of building plans and venue schematics of likely critical incident target sites.
- (c) Communications interoperability with other law enforcement and emergency service agencies.
- (d) Training opportunities in critical incident target sites, including joint training with site occupants.
- (e) Evacuation routes in critical incident target sites.
- (f) Patrol first-response training.
- (g) Response coordination and resources of emergency medical and fire services.
- (h) Equipment needs.
- (i) Mutual aid agreements with other agencies.
- (j) Coordination with private security providers in critical incident target sites.

410.6 TRAINING

The Support Services Commander should include rapid response to critical incidents in the training plan. This training should address:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Rapid Response and Deployment

- (a) Orientation to likely critical incident target sites, such as schools, shopping centers, entertainment and sporting event venues.
- (b) Communications interoperability with other law enforcement and emergency service agencies.
- (c) Patrol first-response training, including patrol rifle, shotgun, breaching tool and control device training.
- (d) First aid, including gunshot trauma.
- (e) Reality-based scenario training (e.g., active shooter, disgruntled violent worker).

Immigration Violations

412.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to members of the South Saint Paul Police Department relating to immigration and interacting with federal immigration officials.

412.2 POLICY

It is the policy of the South Saint Paul Police Department that all members make personal and professional commitments to equal enforcement of the law and equal service to the public. Confidence in this commitment will increase the effectiveness of this department in protecting and serving the entire community and recognizing the dignity of all persons, regardless of their national origin or immigration status.

412.3 VICTIMS AND WITNESSES

To encourage crime reporting and cooperation in the investigation of criminal activity, all individuals, regardless of their immigration status, must feel secure that contacting or being addressed by members of law enforcement will not automatically lead to immigration inquiry and/or deportation. While it may be necessary to determine the identity of a victim or witness, members shall treat all individuals equally and not in any way that would violate the United States or Minnesota constitutions.

412.4 DETENTIONS

An officer should not detain any individual, for any length of time, for a civil violation of federal immigration laws or a related civil warrant.

An officer who has a reasonable suspicion that an individual already lawfully contacted or detained has committed a criminal violation of federal immigration law may detain the person for a reasonable period of time in order to contact federal immigration officials to verify whether an immigration violation is a federal civil violation or a criminal violation. If the violation is a criminal violation, the officer may continue to detain the person for a reasonable period of time if requested by federal immigration officials (8 USC § 1357(g)(10)). No individual who is otherwise ready to be released should continue to be detained only because questions about the individual's status are unresolved.

If the officer has facts that establish probable cause to believe that a person already lawfully detained has committed a criminal immigration offense, he/she may continue the detention and may request a federal immigration official to respond to the location to take custody of the detained person (8 USC § 1357(g)(10)).

An officer is encouraged to forgo detentions made solely on the basis of a misdemeanor offense when time limitations, availability of personnel, issues of officer safety, communication capabilities, or the potential to obstruct a separate investigation outweigh the need for the detention.

An officer should notify a supervisor as soon as practicable whenever an individual is being detained for a criminal immigration violation.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Immigration Violations

412.4.1 SUPERVISOR RESPONSIBILITIES

When notified that an officer has detained an individual and established reasonable suspicion or probable cause to believe the person has violated a criminal immigration offense, the supervisor should determine whether it is appropriate to:

- (a) Transfer the person to federal authorities.
- (b) Lawfully arrest the person for a criminal offense or pursuant to a judicial warrant (see the Law Enforcement Authority Policy).

412.5 ARREST NOTIFICATION TO IMMIGRATION AND CUSTOMS ENFORCEMENT

Generally, an officer should not notify federal immigration officials when booking arrestees at a county jail facility. Any required notification will be handled according to jail operation procedures. No individual who is otherwise ready to be released should continue to be detained solely for the purpose of notification.

412.6 FEDERAL REQUESTS FOR ASSISTANCE

Requests by federal immigration officials for assistance from this department should be directed to a supervisor. The Department may provide available support services, such as traffic control or peacekeeping efforts.

412.7 INFORMATION SHARING

No member of this department will prohibit, or in any way restrict, any other member from doing any of the following regarding the citizenship or immigration status, lawful or unlawful, of any individual (8 USC § 1373):

- (a) Sending information to, or requesting or receiving such information from federal immigration officials
- (b) Maintaining such information in department records
- (c) Exchanging such information with any other federal, state, or local government entity

412.7.1 IMMIGRATION DETAINERS

No individual should be held based solely on a federal immigration detainer under 8 CFR 287.7 unless the person has been charged with a federal crime or the detainer is accompanied by a warrant, affidavit of probable cause, or removal order. Notification to the federal authority issuing the detainer should be made prior to the release.

412.8 U VISA AND T VISA NONIMMIGRANT STATUS

Under certain circumstances, federal law allows temporary immigration benefits, known as a U visa, to victims and witnesses of certain qualifying crimes (8 USC § 1101(a)(15)(U)).

Similar immigration protection, known as a T visa, is available for certain qualifying victims of human trafficking (8 USC § 1101(a)(15)(T)).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Immigration Violations

Any request for assistance in applying for U visa or T visa status should be forwarded in a timely manner to the Investigations supervisor assigned to oversee the handling of any related case.

The Investigations supervisor should:

- (a) Consult with the assigned investigator to determine the current status of any related case and whether further documentation is warranted.
- (b) Contact the appropriate prosecutor assigned to the case, if applicable, to ensure the certification or declaration has not already been completed and whether a certification or declaration is warranted.
- (c) Address the request and complete the certification or declaration, if appropriate, in a timely manner.
 - 1. The instructions for completing certification and declaration forms can be found on the U.S. Department of Homeland Security (DHS) website.
- (d) Ensure that any decision to complete, or not complete, a certification or declaration form is documented in the case file and forwarded to the appropriate prosecutor. Include a copy of any completed form in the case file.

412.9 TRAINING

The Support Services Commander should ensure officers receive training on this policy.

Training should include:

- (a) Identifying civil versus criminal immigration violations.
- (b) Factors that may be considered in determining whether a criminal immigration offense has been committed.

Patrol Rifles

413.1 PURPOSE AND SCOPE

To more effectively and accurately address the increasing level of firepower and body armor utilized by criminal suspects, the South Saint Paul Police Department will make patrol rifles available to qualified officers as an additional and more immediate tactical resource.

413.2 PATROL RIFLE

413.2.1 DEFINITION

Patrol Rifle - An authorized weapon which is owned by the Department and which is made available to properly trained and qualified officers as a supplemental resource to their duty handgun or shotgun. No personally owned rifles may be carried for patrol duty unless pre-approved in writing by the Chief of Police and the Department armorer.

413.3 SPECIFICATIONS

Only weapons and ammunition that meet agency authorized specifications, approved by the Chief of Police and issued by the Department, may be used by officers in their law enforcement responsibilities. The authorized patrol rifle issued by the Department is the M4 carbine.

413.4 RIFLE MAINTENANCE

- (a) Primary responsibility for maintenance of patrol rifles shall fall on the Operations Commander or armorer, who should inspect and service each patrol rifle on a regular basis.
- (b) Each patrol officer shall be responsible for promptly reporting any damage or malfunction of an assigned patrol rifle to a supervisor, the Operations Commander or armorer.
- (c) Any patrol rifle found to be unserviceable shall also be clearly identified as non-serviceable, including details regarding the unserviceable condition.
- (d) Each patrol rifle shall be subject to inspection by a supervisor, the Operations Commander or armorer at any time.
- (e) No modification shall be made to any patrol rifle without prior authorization from the Operations Commander or armorer.

413.5 TRAINING

Officers shall not carry or utilize the patrol rifle unless they have successfully completed Department training. This training shall consist of an initial patrol rifle user's course and qualification score with a certified patrol rifle instructor. Officers shall thereafter be required to successfully complete biannual training and yearly firearms proficiency qualification conducted by a certified patrol rifle instructor.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Patrol Rifles

Any officer who fails to qualify or who fails to successfully complete two or more Department-sanctioned training/qualification sessions within a calendar year will no longer be authorized to carry the patrol rifle without successfully retaking the initial patrol officers user's course and qualification.

413.6 DEPLOYMENT OF THE PATROL RIFLE

Officers may deploy the patrol rifle in any circumstance where the officer can articulate a reasonable expectation that the rifle may be needed. Examples of some general guidelines for deploying the patrol rifle may include, but are not limited to:

- (a) Situations where the officer reasonably anticipates an armed encounter.
- (b) When an officer is faced with a situation that may require the delivery of accurate and effective fire at long range.
- (c) Situations where an officer reasonably expects the need to meet or exceed a suspect's firepower.
- (d) When an officer reasonably believes that there may be a need to deliver fire on a barricaded suspect or a suspect with a hostage.
- (e) When an officer reasonably believes that a suspect may be wearing body armor.
- (f) When authorized or requested by a supervisor.
- (g) When appropriate to aid in the dispatch of an animal.

413.7 DISCHARGE OF THE PATROL RIFLE

The discharge of the patrol rifle shall be governed by the Use of Force Policy and the Shooting Policy.

413.8 PATROL READY

Any qualified officer carrying a patrol rifle in the field shall maintain the weapon in a patrol ready condition until deployed. A rifle is considered in a patrol ready condition when it has been inspected by the assigned officer, the chamber is empty, the trigger is spent, and a fully loaded magazine is inserted into the magazine well.

413.9 RIFLE STORAGE

- (a) When not deployed, patrol rifles will be stored in the Department armory in rifle racks.
- (b) In-service patrol rifles should be secured in the vehicle gun lock or case.

Aircraft Accidents

414.1 PURPOSE AND SCOPE

The purpose of this policy is to provide department members with guidelines for handling aircraft accidents.

This policy does not supersede, and is supplementary to, applicable portions of the Crime and Disaster Scene Integrity, Emergency Operations Plan and Hazardous Material Response policies.

414.1.1 DEFINITIONS

Definitions related to this policy include:

Aircraft - Any fixed wing aircraft, rotorcraft, balloon, blimp/dirigible or glider that is capable of carrying a person or any unmanned aerial vehicle other than those intended for non-commercial recreational use.

414.2 POLICY

It is the policy of the South Saint Paul Police Department to provide an appropriate emergency response to aircraft accidents. This includes emergency medical care and scene management.

414.3 ARRIVAL AT SCENE

Officers or other authorized members tasked with initial scene management should establish an inner and outer perimeter to:

- (a) Protect persons and property.
- (b) Prevent any disturbance or further damage to the wreckage or debris, except to preserve life or rescue the injured.
- (c) Preserve ground scars and marks made by the aircraft.
- (d) Manage the admission and access of public safety and medical personnel to the extent necessary to preserve life or to stabilize hazardous materials.
- (e) Maintain a record of persons who enter the accident site.
- (f) Consider implementation of an Incident Command System (ICS).

414.4 INJURIES AND CASUALTIES

Members should address emergency medical issues and provide care as a first priority.

Those tasked with the supervision of the scene should coordinate with the National Transportation Safety Board (NTSB) before the removal of bodies. If that is not possible, the scene supervisor should ensure documentation of what was disturbed, including switch/control positions and instrument/gauge readings.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Aircraft Accidents

414.5 NOTIFICATIONS

When an aircraft accident is reported to this department, the responding supervisor shall ensure notification is or has been made to NTSB, the Federal Aviation Administration (FAA), and when applicable, the appropriate branch of the military.

Supervisors shall ensure other notifications are made once an aircraft accident has been reported. The notifications will vary depending on the type of accident, extent of injuries or damage, and the type of aircraft involved. When an aircraft accident has occurred, it is generally necessary to notify the following:

- (a) Fire department
- (b) Appropriate airport tower
- (c) Emergency medical services (EMS)

414.6 CONTROLLING ACCESS AND SCENE AUTHORITY

Prior to NTSB arrival, scene access should be limited to authorized personnel from the:

- (a) FAA.
- (b) Fire department, EMS or other assisting law enforcement agencies.
- (c) Medical Examiner.
- (d) Air Carrier/Operators investigative teams with NTSB approval.
- (e) Appropriate branch of the military, when applicable.
- (f) Other emergency services agencies (e.g., hazardous materials teams, biohazard decontamination teams, fuel recovery specialists, explosive ordnance disposal specialists).

The NTSB has primary responsibility for investigating accidents involving civil aircraft. In the case of a military aircraft accident, the appropriate branch of the military will have primary investigation responsibility.

After the NTSB or military representative arrives on-scene, the efforts of this department will shift to a support role for those agencies.

If NTSB or a military representative determines that an aircraft or accident does not qualify under its jurisdiction, the on-scene department supervisor should ensure the accident is still appropriately investigated and documented.

414.7 DANGEROUS MATERIALS

Members should be aware of potentially dangerous materials that might be present. These may include, but are not limited to:

- (a) Fuel, chemicals, explosives, biological or radioactive materials and bombs or other ordnance.
- (b) Pressure vessels, compressed gas bottles, accumulators and tires.
- (c) Fluids, batteries, flares and igniters.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Aircraft Accidents

- (d) Evacuation chutes, ballistic parachute systems and composite materials.

414.8 DOCUMENTATION

All aircraft accidents occurring within the City of South Saint Paul shall be documented. At a minimum the documentation should include the date, time and location of the incident; any witness statements, if taken; the names of SSP PD members deployed to assist; other City resources that were utilized; and cross reference information to other investigating agencies. Suspected criminal activity should be documented on the appropriate crime report.

414.8.1 WRECKAGE

When reasonably safe, members should:

- (a) Obtain the aircraft registration number (N number) and note the type of aircraft.
- (b) Attempt to ascertain the number of casualties.
- (c) Obtain photographs or video of the overall wreckage, including the cockpit and damage, starting at the initial point of impact, if possible, and any ground scars or marks made by the aircraft.
 - 1. Military aircraft may contain classified equipment and therefore shall not be photographed unless authorized by a military commanding officer (18 USC § 795).
- (d) Secure, if requested by the lead authority, any electronic data or video recorders from the aircraft that became dislodged or cell phones or other recording devices that are part of the wreckage.
- (e) Acquire copies of any recordings from security cameras that may have captured the incident.

414.8.2 WITNESSES

Members tasked with contacting witnesses should obtain:

- (a) The location of the witness at the time of his/her observation relative to the accident site.
- (b) A detailed description of what was observed or heard.
- (c) Any photographs or recordings of the accident witnesses may be willing to voluntarily surrender.
- (d) The names of all persons reporting the accident, even if not yet interviewed.
- (e) Any audio recordings of reports to 9-1-1 regarding the accident and dispatch records.

414.9 MEDIA RELATIONS

The Police Chief ([PIO]) should coordinate a response to the media, including access issues, road closures, detours and any safety information that is pertinent to the surrounding community. Any release of information regarding details of the accident itself should be coordinated with the NTSB or other authority who may have assumed responsibility for the investigation.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Aircraft Accidents

Depending on the type of aircraft, the airline or the military may be responsible for family notifications and the release of victims' names. The [PIO] should coordinate with other involved entities before the release of information.

Field Training Officer Program

415.1 PURPOSE AND SCOPE

The Field Training Officer Program is intended to provide a standardized program to facilitate the officer's transition from the academic setting to the actual performance of general law enforcement duties of the South Saint Paul Police Department.

It is the policy of this department to assign all new police officers to a structured Field Training Officer Program that is designed to prepare the new officer to perform in a patrol assignment and to acquire all of the skills needed to operate in a safe, productive and professional manner.

415.2 FIELD TRAINING OFFICER - SELECTION AND TRAINING

The Field Training Officer (FTO) is an experienced officer trained in the art of supervising, training and evaluating entry-level and lateral police officers in the application of their previously acquired knowledge and skills.

415.2.1 SELECTION PROCESS

FTOs will be selected based on the following requirements:

- (a) Desire to be an FTO.
- (b) Demonstrated ability as a positive role model.
- (c) Evaluation by supervisors and current FTOs.
- (d) Possess an FTO certificate of completion from a Minnesota POST Board-approved course.

415.3 FIELD TRAINING OFFICER PROGRAM SUPERVISOR

The Field Training Officer Program Supervisor will be selected by the Operations Division Commander or designee.

The responsibilities of the FTO Program Supervisor include the following:

- (a) Assignment of trainees to FTOs.
- (b) Conduct FTO meetings.
- (c) Maintain and ensure FTO/trainee performance evaluations are completed.
- (d) Maintain, update and issue the Field Training Manual to each trainee.
- (e) Monitor individual FTO performance.
- (f) Monitor overall FTO Program.
- (g) Develop ongoing training for FTOs.

The FTO Program supervisor will be required to obtain a Field Training Officer Supervisory certificate from a Minnesota POST Board-approved course.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Field Training Officer Program

415.4 TRAINEE DEFINED

Trainee - Any entry level or lateral police officer newly appointed to the South Saint Paul Police Department who possesses a Minnesota POST license or is eligible to be licensed.

415.5 REQUIRED TRAINING

Entry level officers shall be required to successfully complete the Field Training Program.

The training period for lateral officers may be modified depending on the trainee's demonstrated performance and level of experience.

The required training will take place on at least two different shifts and with at least two different FTOs if reasonably possible.

415.5.1 FIELD TRAINING MANUAL

Each new officer will be issued a Field Training Manual at the beginning of his/her Primary Training Phase. This manual is an outline of the subject matter and skills necessary to properly function as an officer with the South Saint Paul Police Department. The officer shall become knowledgeable of the subject matter as outlined. He/she shall also become proficient with those skills as set forth in the manual.

The Field Training Manual will specifically cover those policies, procedures, rules and regulations enacted by the South Saint Paul Police Department.

415.5.2 ENTRY LEVEL OFFICER RESTRICTIONS

Officers currently assigned to Field Training are restricted from carrying their assigned duty weapon when not on duty, working off-duty law enforcement details and are not to be counted toward shift minimum manpower.

415.6 EVALUATIONS

Evaluations are an important component of the training process and shall be completed as outlined below.

415.6.1 FIELD TRAINING OFFICER

The FTO will be responsible for the following:

- (a) Completing and submitting evaluations on the performance of the assigned trainee to the Field Training Program Supervisor.
- (b) Reviewing the Daily Trainee Performance Evaluations with the trainee each day.
- (c) Completing a detailed end-of-phase performance evaluation on the assigned trainee at the end of each phase of training.
- (d) Signing off all completed topics contained in the Field Training Manual, noting the method of learning and evaluating the performance of the assigned trainee.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Field Training Officer Program

415.6.2 FIELD TRAINING ADMINISTRATOR

The Field Training Sergeant will review and approve the Daily Trainee Performance Evaluations submitted by the FTO through his/her immediate supervisor.

The Field Training Sergeant will hold periodic meetings with all FTOs to ensure understanding and compliance with the requirements of the Field Training Program. As needed, the Field Training Administrator will hold a process review meeting with all FTOs to discuss changes needed in the FTO Program. A summary of this meeting, with any recommendations or changes made, will be documented and forward to the Chief of Police for review and approval.

415.6.3 TRAINEE

At the completion of the Field Training Program, the trainee shall submit a performance evaluation of each of his/her FTOs and of the Field Training Program.

415.7 DOCUMENTATION

All documentation of the Field Training Program will be retained in the officer's training files and will consist of the following:

- (a) Daily Trainee Performance Evaluations.
- (b) End of phase evaluations.
- (c) A letter of completion, certifying that the trainee has successfully completed field training.
- (d) All incident reports.
- (e) All recordings.
- (f) Any other documentation generated by the entry level officer.

Shift Sergeants

416.1 PURPOSE AND SCOPE

Each patrol shift must be directed by supervisors who are capable of making decisions and communicating in a manner consistent with Department policies, procedures, practices, functions and objectives. To accomplish this goal, a Sergeant heads each watch.

416.2 OFFICER IN CHARGE

When a Sergeant is unavailable for duty, in most instances the senior qualified officer in charge shall be designated as Officer in Charge.

Mobile Video Recorders

417.1 PURPOSE AND SCOPE

The South Saint Paul Police Department has equipped marked patrol cars with Mobile Video Recording (MVR) systems to provide records of events and assist officers in the performance of their duties. This policy provides guidance on the use of these systems.

417.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - Any process that causes the MVR system to transmit or store video or audio data in an active mode.

In-car camera system and Mobile Video Recorder (MVR) - Synonymous terms - that refer to any system that captures audio and video signals that is capable of installation in a vehicle and that includes at minimum, a camera, microphone, recorder and monitor.

Law Enforcement Operator (LEO) - Primarily a licensed peace officer but on occasion may be a non-licensed representative of the Department who is authorized and assigned to operate MVR-equipped vehicles to the extent consistent with Minn. Stat. § 169.98.

MGDPA - The Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13.

MVR technician - Personnel certified or trained in the operational use and repair of MVRs, duplicating methods, storage and retrieval methods and procedures, and who possess a working knowledge of video forensics and evidentiary procedures.

Recorded media - Audio-video signals recorded or digitally stored on a storage device or portable media.

417.2 POLICY

It is the goal of the South Saint Paul Police Department to use mobile video recorder (MVR) technology to more effectively fulfill the department's mission and to ensure these systems are used securely and efficiently.

417.3 OFFICER RESPONSIBILITIES

Prior to going into service each officer will properly equip him/herself to record audio and video in the field. At the end of the shift each officer will follow the established procedures for providing to the Department any recordings or used media and any other related equipment. Each officer should have adequate recording media for the entire duty assignment. In the event an officer works at a remote location and reports in only periodically additional recording media may be issued. Only South Saint Paul Police Department identified and labeled media with tracking numbers is to be used.

At the start of each shift, officers should test the MVR system operation in accordance with manufacturer specifications and department operating procedures and training.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Mobile Video Recorders

System documentation is accomplished by the officer recording his/her name, serial number, badge, or PIN number and the current date and time at the start and again at the end of each shift. If the system is malfunctioning, the officer shall take the vehicle out of service unless a supervisor requests the vehicle remain in service.

417.4 ACTIVATION OF THE MVR

The MVR system is designed to turn on whenever the unit's emergency lights are activated. The system remains on until it is turned off manually. The audio portion is independently controlled and should be activated manually by the officer whenever appropriate. When audio is being recorded the video will also record.

Operators are encouraged to narrate events using the audio recording so as to provide the best documentation for pretrial and courtroom presentation.

417.4.1 REQUIRED ACTIVATION OF THE MVR

This policy is not intended to describe every possible situation in which the MVR system may be used, although there are many situations where its use is appropriate. An officer may activate the system any time the officer believes its use would be appropriate and/or valuable to document an incident.

In some circumstances it is not possible to capture images of the incident due to conditions or the location of the camera. However the audio portion can be valuable evidence and is subject to the same activation requirements as the MVR. The MVR system should be activated in any of the following situations:

- (a) All field contacts involving actual or potential criminal conduct within video or audio range:
 - 1. Traffic stops (to include, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops)
 - 2. Priority responses
 - 3. Vehicle pursuits
 - 4. Suspicious vehicles
 - 5. Arrests
 - 6. Vehicle searches
 - 7. Physical or verbal confrontations or use of force
 - 8. Prisoner transports
 - 9. Non-custody transports
 - 10. Pedestrian checks
 - 11. DWI investigations including field sobriety tests
 - 12. Consensual encounters
 - 13. Crimes in progress

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Mobile Video Recorders

14. Responding to an in-progress call
15. Medical incidents attended to by members of the Department
- (b) All self-initiated activity in which an officer would normally notify Dispatch
- (c) Any call for service involving a crime where the recorder may aid in the apprehension and/or prosecution of a suspect:
 1. Family violence calls
 2. Disturbance of peace calls
 3. Offenses involving violence or weapons
- (d) Any other contact that becomes adversarial after the initial contact, in a situation that would not otherwise require recording
- (e) Any other circumstance where the officer believes that a recording of an incident would be appropriate

417.4.2 CESSATION OF RECORDING

Once activated the MVR system should remain on until the incident has concluded. For purposes of this section conclusion of an incident has occurred when all arrests have been made, arrestees have been transported and all witnesses and victims have been interviewed. Recording may cease if an officer is simply waiting for a tow truck or a family member to arrive, or in other similar situations.

417.4.3 WHEN ACTIVATION IS NOT REQUIRED

Activation of the MVR system is not required when exchanging information with other officers or during breaks, lunch periods, when not in service or actively on patrol.

No member of this department may surreptitiously use City equipment to record a conversation of any other member of this department except with a court order or when lawfully authorized by the Chief of Police or the authorized designee for the purpose of conducting a criminal or administrative investigation.

417.4.4 SUPERVISOR RESPONSIBILITIES

Supervisors should determine if vehicles with non-functioning MVR systems should be placed into service. If these vehicles are placed into service, the appropriate documentation should be made, including notification of Dispatch.

At reasonable intervals, supervisors should validate that:

- (a) Beginning and end-of-shift recording procedures are followed.
- (b) Logs reflect the proper chain of custody, including:
 1. The tracking number of the MVR system media.
 2. The date it was issued.
 3. The law enforcement operator or the vehicle to which it was issued.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Mobile Video Recorders

4. The date it was submitted.
 5. Law enforcement operators submitting the media.
 6. Holds for evidence indication and tagging as required.
- (c) The operation of MVR systems by new employees is assessed and reviewed no less than biweekly.

When an incident arises that requires the immediate retrieval of the recorded media (e.g., serious crime scenes, peace officer-involved shootings, department-involved collisions), a supervisor shall respond to the scene and ensure that the appropriate supervisor, MVR technician or crime scene investigator properly retrieves the recorded media. The media may need to be treated as evidence and should be handled in accordance with current evidence procedures for recorded media. Copies may be distributed to investigators as appropriate to the investigation.

Supervisors may activate the MVR system remotely to monitor a developing situation such as a chase, riot or an event that may threaten public safety, officer safety or both, when the purpose is to obtain tactical information to assist in managing the event.

417.5 REVIEW OF MVR RECORDINGS

All recording media, recorded images and audio recordings are the property of the agency and subject to the provisions of the MGDPA. Dissemination outside of the agency is strictly prohibited except to the extent permitted or required under the MGDPA, Peace Officer Disciplinary Procedures Act or other applicable law.

To prevent damage to, or alteration of, the original recorded media, it shall not be copied, viewed or otherwise inserted into any device not approved by the department MVR technician or forensic media staff. When reasonably possible a copy of the original media shall be used for viewing (unless otherwise directed by the courts) to preserve the original media.

Recordings may be reviewed in any of the following situations.

- (a) For use when preparing reports or statements
- (b) By a supervisor investigating a specific act of officer conduct
- (c) By a supervisor to assess officer performance
- (d) To assess proper functioning of MVR systems
- (e) By department investigators, after approval of a supervisor, who are participating in an official investigation such as a personnel complaint, administrative inquiry or a criminal investigation
- (f) By department personnel who request to review recordings
- (g) By an officer who is captured on or referenced in the video or audio data and reviews and uses the data for any purpose relating to his/her employment
- (h) By court personnel through proper process or with permission of the Chief of Police or the authorized designee

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Mobile Video Recorders

- (i) By the media through proper process or with an MGDPA request (Minn. Stat. § 13.01 et seq.)
- (j) To assess possible training value
- (k) Recordings may be shown for staff or public safety training purposes. If an involved officer objects to showing a recording, his/her objection will be submitted to the staff to determine if the training value outweighs the officer's objection

Employees desiring to view any previously uploaded or archived MVR recording should submit a request in writing to the Sergeant. Approved requests should be forwarded to the MVR technician for processing.

In no event shall any recording be used or shown for the purpose of ridiculing or embarrassing any employee.

417.6 DOCUMENTING MVR USE

If any incident is recorded with either the video or audio system, the existence of that recording shall be documented in the officer's report. If a citation is issued, the officer shall make a notation on the records copy of the citation indicating that the incident was recorded.

417.7 RECORDING MEDIA STORAGE AND INTEGRITY

Once uploaded for storage, all recording media will be retained on a designated server for a minimum of 45 days and then purged in accordance with the MVR retention settings. All recording media submitted as evidence will be copied to an alternative server and disposed of in compliance with the established records retention schedule.

417.7.1 COPIES OF ORIGINAL RECORDING MEDIA

Upon proper request a copy of the original recording media will be made for use as authorized in this policy.

417.7.2 MVR RECORDINGS AS EVIDENCE

Officers who reasonably believe that an MVR recording is likely to contain evidence relevant to a criminal offense, potential claim against the officer or against the South Saint Paul Police Department should indicate this in an appropriate report. Officers should ensure relevant recordings are preserved.

417.8 SYSTEM OPERATIONAL STANDARDS

- (a) MVR system vehicle installations should be based on officer safety requirements and vehicle and device manufacturer recommendations.
- (b) The MVR system should be configured to minimally record for 30 seconds prior to an event.
- (c) The MVR system may not be configured to record audio data occurring prior to activation.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Mobile Video Recorders

- (d) To prevent bleed-over and/or noise from other MVRs in systems using low band transmitters (analog) only the primary LEO initiating the contact shall activate his/her audio recorder.
- (e) LEOs using digital transmitters that are individually synchronized to their individual MVR shall activate both audio and video recordings when responding in a support capacity in order to obtain additional perspectives of the incident scene.
- (f) With the exception of law enforcement radios or other emergency equipment other electronic devices should not be used within the law enforcement vehicle in order to intentionally interfere with the capability of the MVR system to record audio data.
- (g) LEOs shall not erase, alter, reuse, modify or tamper with MVR recordings. Only a supervisor, MVR technician or other approved designee may erase and reissue previously recorded recordings and may only do so pursuant to the provisions of this policy.
- (h) To prevent damage original recordings shall not be viewed on any equipment other than the equipment issued or authorized by the MVR technician.

417.9 TRAINING

Users of the MVR systems and supervisors shall successfully complete an approved course of instruction prior to being deployed with MVR systems in operational settings.

Mobile Digital Computer Use

418.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper access, use and application of the Mobile Digital Computer (MDC) system in order to ensure appropriate access to confidential records from local, state and national law enforcement databases, and to ensure effective electronic communications between department members and Dispatch.

418.2 POLICY

South Saint Paul Police Department members using the MDC shall comply with all appropriate federal and state rules and regulations and shall use the MDC in a professional manner, in accordance with this policy.

418.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to messages accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use Policy for additional guidance).

418.4 RESTRICTED ACCESS AND USE

MDC use is subject to the Information Technology Use and Protected Information policies.

Members shall not access the MDC system if they have not received prior authorization and the required training. Members shall immediately report unauthorized access or use of the MDC by another member to their supervisors or Sergeants.

Use of the MDC system to access law enforcement databases or transmit messages is restricted to official activities, business-related tasks and communications that are directly related to the business, administration or practices of the Department. In the event that a member has questions about sending a particular message or accessing a particular database, the member should seek prior approval from his/her supervisor.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing or any other inappropriate messages on the MDC system is prohibited and may result in discipline.

It is a violation of this policy to transmit a message or access a law enforcement database under another member's name or to use the password of another member to log in to the MDC system unless directed to do so by a supervisor. Members are required to log off the MDC or secure the MDC when it is unattended. This added security measure will minimize the potential for unauthorized access or misuse.

418.4.1 USE WHILE DRIVING

Use of the MDC by the vehicle operator should generally be limited to times when the vehicle is stopped. When the vehicle is in motion, the operator should only attempt to read messages that are likely to contain information that is required for immediate enforcement, investigative or safety needs.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Mobile Digital Computer Use

Short transmissions, such as a license plate check, are permitted if it reasonably appears that it can be done safely. In no case shall an operator attempt to send or review lengthy messages while the vehicle is in motion.

418.5 DOCUMENTATION OF ACTIVITY

Except as otherwise directed by the Sergeant or other department-established protocol, all calls for service assigned by a dispatcher should be communicated by voice over the police radio and electronically via the MDC unless security or confidentiality prevents such broadcasting.

MDC and voice transmissions are used to document the member's daily activity. To ensure accuracy:

- (a) All contacts or activity shall be documented at the time of the contact.
- (b) Whenever the activity or contact is initiated by voice, it should be documented by a dispatcher.
- (c) Whenever the activity or contact is not initiated by voice, the member shall document it via the MDC.

418.5.1 STATUS CHANGES

All changes in status (e.g., arrival at scene, meal periods, in service) will be transmitted over the police radio or through the MDC system.

Members responding to in-progress calls should advise changes in status over the radio to assist other members responding to the same incident. Other changes in status can be made on the MDC.

418.5.2 EMERGENCY ACTIVATION

If there is an emergency activation and the member does not respond to a request for confirmation of the need for emergency assistance or confirms the need, available resources will be sent to assist in locating the member. If the location is known, the nearest available officer should respond in accordance with the Officer Response to Calls Policy.

Members should ensure a field supervisor and the Sergeant are notified of the incident without delay.

Officers not responding to the emergency shall refrain from transmitting on the police radio until a no-further-assistance broadcast is made or if they are also handling an emergency.

418.6 EQUIPMENT CONSIDERATIONS

418.6.1 MALFUNCTIONING MDC

Whenever possible, members will not use vehicles with malfunctioning MDCs. Whenever members must drive a vehicle in which the MDC is not working, they shall notify Dispatch. It shall be the responsibility of the dispatcher to document all information that will then be transmitted verbally over the police radio.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Mobile Digital Computer Use

418.6.2 BOMB CALLS

When investigating reports of possible bombs, members should not communicate on their MDCs when in the evacuation area of a suspected explosive device. Radio frequency emitted by the MDC could cause some devices to detonate.

Policy Title

Portable Audio/Video Recorders

420.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of this department while in the performance of their duties (Minn. Stat. § 626.8473). Portable audio/video recording devices include all recording systems whether body-worn, hand-held, or integrated into portable equipment.

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any South Saint Paul Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices).

420.1.1 DEFINITIONS

Definitions related to this policy include:

Portable recording system - A device worn by a member that is capable of both video and audio recording of the member's activities and interactions with others or collecting digital multimedia evidence as part of an investigation and as provided in Minn. Stat. § 13.825.

420.2 POLICY

The South Saint Paul Police Department may provide members with access to portable recorders for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Department by accurately capturing contacts between members of the Department and the public.

420.3 MEMBER PRIVACY EXPECTATION

All recordings made by members on any department-issued device at any time or while acting in an official capacity of this department, regardless of ownership of the device, shall remain the property of the Department. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

420.4 MEMBER RESPONSIBILITIES

Prior to going into service, uniformed members will be responsible for making sure that they are equipped with a portable recorder issued by the Department, and that the recorder is in good working order (Minn. Stat. § 13.825). If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to their supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner at or above the mid-line of the waist and notify persons that they are being recorded, whenever reasonably practicable (Minn. Stat. § 626.8473).

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Portable Audio/Video Recorders

conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

When using a portable recorder, the assigned member shall record their name, employee number, and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording.

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording (Minn. Stat. § 626.8473). Members should include the reason for deactivation.

420.5 ACTIVATION OF THE AUDIO/VIDEO RECORDER

This policy is not intended to describe every possible situation in which the recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

The recorder should be activated in any of the following situations:

- (a) All enforcement and investigative contacts including stops and field interview (FI) situations
- (b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops
- (c) Self-initiated activity in which a member would normally notify Dispatch
- (d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is a member expected to jeopardize his/her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

420.5.1 CESSATION OF RECORDING

Once activated, the portable recorder should remain on continuously until the member reasonably believes that his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Portable Audio/Video Recorders

420.5.2 SURREPTITIOUS RECORDINGS

Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Minn. Stat. § 626A.02).

Members of the Department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee.

420.5.3 EXPLOSIVE DEVICE

Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

420.6 IDENTIFICATION AND PRESERVATION OF RECORDINGS

To assist with identifying and preserving data and recordings, members should download, tag or mark the recordings in accordance with procedure and document the existence of the recording in any related case report.

A member should transfer, tag or mark recordings when the member reasonably believes:

- (a) The recording contains evidence relevant to potential criminal, civil or administrative matters.
- (b) A complainant, victim or witness has requested non-disclosure.
- (c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person.
- (d) Disclosure may be an unreasonable violation of someone's privacy.
- (e) Medical or mental health information is contained.
- (f) Disclosure may compromise an under-cover officer or confidential informant.
- (g) The recording or portions of the recording may be protected under the Minnesota Data Practices Act.

Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g., a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

420.7 REVIEW OF RECORDED MEDIA FILES

When preparing written reports, members should review their recordings as a resource (see the Officer-Involved Shootings and Deaths Policy for guidance in those cases). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Portable Audio/Video Recorders

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

- (a) By a supervisor as part of internal audits and reviews as required by Minn. Stat. § 626.8473.
- (b) Upon approval by a supervisor, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation.
- (c) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.
- (d) By media personnel with permission of the Chief of Police or the authorized designee.
- (e) In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Custodian of Records prior to public release (see the Records Maintenance and Release Policy). Recordings that are clearly offensive to common sensibilities should not be publicly released unless disclosure is required by law or order of the court (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).

420.8 COORDINATOR

The Chief of Police or the authorized designee should designate a coordinator responsible for (Minn. Stat. § 626.8473; Minn. Stat. § 13.825):

- (a) Establishing procedures for the security, storage, and maintenance of data and recordings.
 - 1. The coordinator should work with the Custodian of Records and the member assigned to coordinate the use, access, and release of protected information to ensure that procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) and other applicable laws (Minn. Stat. § 13.01 et seq.) (see the Protected Information and the Records Maintenance and Release policies).
 - 2. The coordinator should work with the Custodian of Records to identify recordings that must be retained for a specific time frame under Minnesota law (e.g., firearm discharges, certain use of force incidents, formal complaints).
- (b) Establishing procedures for accessing data and recordings.
 - 1. These procedures should include the process to obtain written authorization for access to non-public data by SSP PD members and members of other governmental entities and agencies.
- (c) Establishing procedures for logging or auditing access.
- (d) Establishing procedures for transferring, downloading, tagging, or marking events.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Portable Audio/Video Recorders

- (e) Establishing an inventory of portable recorders including:
 - 1. Total number of devices owned or maintained by the South Saint Paul Police Department.
 - 2. Daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used.
 - 3. Total amount of recorded audio and video data collected by the devices and maintained by the South Saint Paul Police Department.
- (f) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.
- (g) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the South Saint Paul Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.
- (h) Ensuring that this Portable Audio/Video Recorders Policy is posted on the Department website.

420.9 PROHIBITED USE OF AUDIO/VIDEO RECORDERS

Members are prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity.

Members are also prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with department-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department.

Members are prohibited from using personally owned recording devices while on-duty without the express consent of the Sergeant. Any member who uses a personally owned recorder for department-related activities shall comply with the provisions of this policy, including retention and release requirements and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

Members are prohibited from using a personally owned portable recording system while on duty.

420.10 RETENTION OF RECORDINGS

All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 180 days.

If an individual captured in a recording submits a written request, the recording shall be retained for an additional time period. The coordinator should be responsible for notifying the individual prior to destruction of the recording (Minn. Stat. § 13.825).

Members shall not alter, erase, or destroy any recordings before the end of the applicable records retention period (Minn. Stat. § 626.8473).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Portable Audio/Video Recorders

420.10.1 RELEASE OF AUDIO/VIDEO RECORDINGS

Requests for the release of audio/video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

420.10.2 ACCESS TO RECORDINGS

Except as provided by Minn. Stat. § 13.825, Subd. 2, audio/video recordings are considered private or nonpublic data.

Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have the consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the subject unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17.

420.11 ACCOUNTABILITY

Any member who accesses or releases recordings without authorization may be subject to discipline (see the Standards of Conduct and the Protected Information policies) (Minn. Stat. § 626.8473).

420.12 EXPANSION OF TECHNOLOGY

Notification will be made to the MN Bureau of Criminal Apprehension within ten days of obtaining new surveillance technology that expands the type or scope of the agency's portable recording system.

420.13 BIENNIAL AUDIT

An independent, biennial audit of the portable recording system will be conducted and a summary forwarded to the City Council and Legislative Commission on Data Practices and Personal Data Privacy.

Foot Pursuits

421.1 PURPOSE AND SCOPE

This policy provides guidelines to assist officers in making the decision to initiate or continue the pursuit of suspects on foot.

421.2 DECISION TO PURSUE

The safety of department members and the public should be the primary consideration when determining whether a foot pursuit should be initiated or continued. Officers must be mindful that immediate apprehension of a suspect is rarely more important than the safety of the public and department members.

Officers may be justified in initiating a foot pursuit of any individual the officer reasonably believes is about to engage in, is engaging in or has engaged in criminal activity. The decision to initiate or continue such a foot pursuit, however, must be continuously re-evaluated in light of the circumstances presented at the time.

Mere flight by a person who is not suspected of criminal activity shall not serve as the sole justification for engaging in an extended foot pursuit without the development of reasonable suspicion regarding the individual's involvement in criminal activity or being wanted by law enforcement.

Deciding to initiate or continue a foot pursuit is a decision that an officer must make quickly and under unpredictable and dynamic circumstances. It is recognized that foot pursuits potentially place department members and the public at significant risk. Therefore, no officer or supervisor shall be criticized or disciplined for deciding not to engage in a foot pursuit because of the perceived risk involved.

If circumstances permit, surveillance and containment are generally the safest tactics for apprehending fleeing persons. In deciding whether to initiate or continue a foot pursuit, an officer should continuously consider reasonable alternatives to a foot pursuit based upon the circumstances and resources available, such as the following:

- (a) Containment of the area.
- (b) Saturation of the area with law enforcement personnel, including assistance from other agencies.
- (c) A canine search.
- (d) Thermal imaging or other sensing technology.
- (e) Air support.
- (f) Apprehension at another time, when the identity of the suspect is known or there is information available that would likely allow for later apprehension, and the need to immediately apprehend the suspect does not reasonably appear to outweigh the risk of continuing the foot pursuit.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Foot Pursuits

421.3 GENERAL GUIDELINES

When reasonably practicable, officers should consider alternatives to engaging in or continuing a foot pursuit when:

- (a) Directed by a supervisor to terminate the foot pursuit; such an order shall be considered mandatory.
- (b) The officer is acting alone.
- (c) Two or more officers become separated, lose visual contact with one another or obstacles separate them to the degree that they cannot immediately assist each other should a confrontation take place. In such circumstances, it is generally recommended that a single officer keep the suspect in sight from a safe distance and coordinate the containment effort.
- (d) The officer is unsure of his/her location and direction of travel.
- (e) The officer is pursuing multiple suspects and it is not reasonable to believe that the officer would be able to control the suspect should a confrontation occur.
- (f) The physical condition of the officers renders him/her incapable of controlling the suspect if apprehended.
- (g) The officer loses radio contact with Dispatch or with assisting or backup officers.
- (h) The suspect enters a building, structure, confined space, isolated area or dense or difficult terrain, and there are insufficient officers to provide backup and containment. The primary officer should consider discontinuing the foot pursuit and coordinating containment pending the arrival of sufficient resources.
- (i) The officer becomes aware of unanticipated or unforeseen circumstances that unreasonably increase the risk to officers or the public.
- (j) The officer reasonably believes that the danger to the pursuing officers or public outweighs the objective of immediate apprehension.
- (k) The officer loses possession of his/her firearm or other essential equipment.
- (l) The officer or a third party is injured during the foot pursuit, requiring immediate assistance, and there are no other emergency personnel available to render assistance.
- (m) The suspect's location is no longer known.
- (n) The identity of the suspect is established or other information exists that will allow for the suspect's apprehension at a later time, and it reasonably appears that there is no immediate threat to Department personnel or the public if the suspect is not immediately apprehended.
- (o) The officer's ability to safely continue the pursuit is impaired by inclement weather, darkness or other environmental conditions.

421.4 RESPONSIBILITIES IN FOOT PURSUITS

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Foot Pursuits

421.4.1 INITIATING OFFICER RESPONSIBILITIES

Unless relieved by another officer or a supervisor, the initiating officer shall be responsible for coordinating the progress of the pursuit. When acting alone and when practicable, the initiating officer should consider whether it is appropriate to overtake and confront the suspect or, rather, attempt to keep the suspect in sight until sufficient officers are present to safely apprehend the suspect.

Pursuing officers should consider the following variables when deciding to continue the pursuit:

- (a) Size / physical conditioning / skill level of the officer -vs- the suspect
- (b) Is the suspect armed
- (c) Is the suspect under the influence and / or suffering a psychotic episode
- (d) Does the suspect's violation or conduct warrant the pursuit.

Early communication of available information from the involved officers is essential so that adequate resources can be coordinated and deployed to bring a foot pursuit to a safe conclusion. Officers initiating a foot pursuit should broadcast the following information as soon as it becomes practicable and available:

- (a) Location and direction of travel
- (b) Call sign identifier
- (c) Reason for the foot pursuit, such as the crime classification
- (d) Number of suspects and description, to include name if known
- (e) Whether the suspect is known or believed to be armed with a dangerous weapon

Officers should be mindful that radio transmissions made while running may be difficult to understand and may need to be repeated.

Absent extenuating circumstances, any officer unable to promptly and effectively broadcast this information should terminate the foot pursuit. If the foot pursuit is discontinued for any reason, immediate efforts for containment should be established and alternatives considered based upon the circumstances and available resources.

When a foot pursuit terminates, the officer will notify Dispatch of his/her location and the status of the foot pursuit termination (e.g., suspect in custody, lost sight of suspect), and will direct further actions as reasonably appear necessary, to include requesting medical aid as needed for officers, suspects or members of the public.

421.4.2 ASSISTING OFFICER RESPONSIBILITIES

Whenever any officer announces that he/she is engaged in a foot pursuit, all other officers should minimize nonessential radio traffic to permit the involved officers maximum access to the radio frequency.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Foot Pursuits

421.4.3 SUPERVISOR RESPONSIBILITIES

Upon becoming aware of a foot pursuit, the supervisor shall make every reasonable effort to ascertain sufficient information to direct responding resources and to take command, control and coordination of the foot pursuit. The supervisor should respond to the area whenever reasonably possible. The supervisor does not, however, need to be physically present to exercise control over the foot pursuit. The supervisor should continuously assess the situation in order to ensure the foot pursuit is conducted within established department guidelines.

The supervisor shall terminate the foot pursuit when the danger to pursuing officers or the public appears to unreasonably outweigh the objective of immediate apprehension of the suspect.

Upon apprehension of the suspect, the supervisor should promptly proceed to the termination point to direct the post-pursuit activity.

421.5 REPORTING

The initiating officer shall complete the appropriate crime/arrest reports documenting, at minimum:

- (a) Date and time of the foot pursuit.
- (b) Initial reason and circumstances surrounding the foot pursuit.
- (c) Course and approximate distance of the foot pursuit.
- (d) Alleged offenses.
- (e) Involved vehicles and officers.
- (f) Whether a suspect was apprehended as well as the means and methods used.
 - 1. Any use of force shall be reported and documented in compliance with the Use of Force Policy.
- (g) Arrestee information, if applicable.
- (h) Any injuries and/or medical treatment.
- (i) Any property or equipment damage.
- (j) Name of the supervisor at the scene or who handled the incident.

Assisting officers taking an active role in the apprehension of the suspect shall complete supplemental reports as necessary or as directed.

The supervisor reviewing the report will make a preliminary determination that the pursuit appears to be in compliance with this policy or that additional review and/or follow-up is warranted.

In any case in which a suspect is not apprehended and there is insufficient information to warrant further investigation, a supervisor may authorize that the initiating officer need not complete a formal report.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Foot Pursuits

421.6 POLICY

It is the policy of this department that officers, when deciding to initiate or continue a foot pursuit, must continuously balance the objective of apprehending the suspect with the risk and potential for injury to department members, the public or the suspect.

Officers are expected to act reasonably, based on the totality of the circumstances.

Automated License Plate Readers (ALPR)

422.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology (Minn. Stat. § 626.8472).

422.2 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the South Saint Paul Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Operations Commander, who will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

422.3 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

- (a) An ALPR shall only be used for official law enforcement business.
- (b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not necessary before using an ALPR.
- (c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents.
- (d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.
- (e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.
- (f) If practicable, the officer should verify an ALPR response through the Minnesota Justice Information Services (MNJIS) and National Law Enforcement Telecommunications System (NLETS) databases before taking enforcement action that is based solely upon an ALPR alert.

422.3.1 RESTRICTIONS, NOTIFICATIONS AND AUDITS

The South Saint Paul Police Department will observe the following guidelines regarding ALPR use (Minn. Stat. § 13.824):

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Automated License Plate Readers (ALPR)

- (a) Data collected by an ALPR will be limited to:
 - 1. License plate numbers.
 - 2. Date, time and location of data captured.
 - 3. Pictures of license plates, vehicles and areas surrounding the vehicle captured.
- (b) ALPR data may only be matched with the Minnesota license plate data file, unless additional sources are needed for an active criminal investigation.
- (c) ALPRs shall not be used to monitor or track an individual unless done so under a search warrant or because of exigent circumstances.
- (d) The Bureau of Criminal Apprehension shall be notified within 10 days of any installation or use and of any fixed location of an ALPR.

422.4 DATA COLLECTION AND RETENTION

The Operations Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

ALPR data received from another agency shall be maintained securely and released in the same manner as ALPR data collected by this department (Minn. Stat. § 13.824).

ALPR data not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection with the following exceptions (Minn. Stat. § 13.824):

- (a) Exculpatory evidence - Data must be retained until a criminal matter is resolved if a written request is made from a person who is the subject of a criminal investigation asserting that ALPR data may be used as exculpatory evidence.
- (b) Address Confidentiality Program - Data related to a participant of the Address Confidentiality Program must be destroyed upon the written request of the participant. ALPR data already collected at the time of the request shall be destroyed and future related ALPR data must be destroyed at the time of collection. Destruction can be deferred if it relates to an active criminal investigation.

All other ALPR data should be retained in accordance with the established records retention schedule.

422.4.1 LOG OF USE

A public log of ALPR use will be maintained that includes (Minn. Stat. § 13.824):

- (a) Specific times of day that the ALPR collected data.
- (b) The aggregate number of vehicles or license plates on which data are collected for each period of active use and a list of all state and federal public databases with which the data were compared.
- (c) For each period of active use, the number of vehicles or license plates related to:
 - 1. A vehicle or license plate that has been stolen.
 - 2. A warrant for the arrest of the owner of the vehicle.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Automated License Plate Readers (ALPR)

3. An owner with a suspended or revoked driver's license or similar category.
 4. Active investigative data.
- (d) For an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

A publicly accessible list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance devices with ALPR capability shall be maintained. The list may be kept from the public if the data is security information as provided in Minn. Stat. § 13.37, Subd. 2.

422.5 ACCOUNTABILITY

All saved data will be closely safeguarded and protected by both procedural and technological means. The South Saint Paul Police Department will observe the following safeguards regarding access to and use of stored data (Minn. Stat. § 13.824; Minn. Stat. § 13.05):

- (a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.
- (b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.
- (c) Biennial audits and reports shall be completed pursuant to Minn. Stat. § 13.824, Subd. 6.
- (d) Breaches of personal data are addressed as set forth in the Protected Information Policy (Minn. Stat. § 13.055).
- (e) All queries and responses, and all actions, in which data are entered, updated, accessed, shared or disseminated, must be recorded in a data audit trail.
- (f) Any member who violates Minn. Stat. § 13.09 through the unauthorized acquisition or use of ALPR data will face discipline and possible criminal prosecution (Minn. Stat. § 626.8472).

422.6 POLICY

The policy of the South Saint Paul Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Automated License Plate Readers (ALPR)

422.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures (Minn. Stat. § 13.824):

- (a) The agency makes a written request for the ALPR data that includes:
 - 1. The name of the agency.
 - 2. The name of the person requesting.
 - 3. The intended purpose of obtaining the information.
 - 4. A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
 - 5. A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.
- (b) The request is reviewed by the Operations Commander or the authorized designee and approved before the request is fulfilled.
 - 1. A release must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation.
- (c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Criminal Conduct on School Buses

423.1 PURPOSE AND SCOPE

Criminal conduct on school buses has been identified by the legislature as a critical component for the safety and security of the community. The primary purpose of this policy is to provide officers guidance in responding to reports of alleged criminal conduct on school buses. This department, in cooperation with any other law enforcement agency that may have concurrent jurisdiction over the alleged offense, is responsible for responding to all reports of criminal misconduct on school buses in this jurisdiction.

This policy is not intended to interfere with or replace school disciplinary policies that relate to student misconduct on school buses (Minn. Stat. § 169.4581).

423.2 COMMUNITY COOPERATION

The South Saint Paul Police Department shall work with and consult with school officials, transportation personnel, parents and students to respond to these incidents to protect student safety and deal appropriately with those who violate the law.

423.3 PROCEDURE

This department shall respond to all criminal misconduct on school buses within the jurisdiction of this department regardless of the source of the report. Officers should take reasonable actions to complete the following:

- (a) Provide for the safety of any person involved in the incident or present at the incident.
- (b) Coordinate any appropriate care.
- (c) Investigate reports of crimes committed on school buses using the same procedures as followed in other criminal investigations as appropriate for juveniles and/or adults.
- (d) Issue citations, release pending further investigation, or apprehend and transport individuals committing crimes on school buses to the extent authorized by law.
- (e) Submit reports regarding the incident for review, approval and consideration for prosecution.
- (f) Complete follow-up and additional investigation as reasonably necessary to prepare a case pertaining to criminal conduct on school buses as required for prosecution.
- (g) Provide information to the relevant school regarding the incident as required or authorized by law.

Public Recording of Law Enforcement Activity

424.1 PURPOSE AND SCOPE

This policy provides guidelines for handling situations in which members of the public photograph or audio/video record law enforcement actions and other public activities that involve members of this department. In addition, this policy provides guidelines for situations where the recordings may be evidence.

424.2 POLICY

The South Saint Paul Police Department recognizes the right of persons to lawfully record members of this department who are performing their official duties. Members of this department will not prohibit or intentionally interfere with such lawful recordings. Any recordings that are deemed to be evidence of a crime or relevant to an investigation will only be collected or seized lawfully.

Officers should exercise restraint and should not resort to highly discretionary arrests for offenses such as interference, failure to comply or disorderly conduct as a means of preventing someone from exercising the right to record members performing their official duties.

424.3 RECORDING LAW ENFORCEMENT ACTIVITY

Members of the public who wish to record law enforcement activities are limited only in certain aspects.

- (a) Recordings may be made from any public place or any private property where the individual has the legal right to be present.
- (b) Beyond the act of photographing or recording, individuals may not interfere with the law enforcement activity. Examples of interference include, but are not limited to:
 - 1. Tampering with a witness or suspect.
 - 2. Inciting others to violate the law.
 - 3. Being so close to the activity as to present a clear safety hazard to the officers.
 - 4. Being so close to the activity as to interfere with an officer's effective communication with a suspect or witness.
- (c) The individual may not present an undue safety risk to the officers, him/herself or others.

424.4 OFFICER RESPONSE

Officers should promptly request that a supervisor respond to the scene whenever it appears that anyone recording activities may be interfering with an investigation or it is believed that the recording may be evidence. If practicable, officers should wait for the supervisor to arrive before taking enforcement action or seizing any cameras or recording media.

Whenever practicable, officers or supervisors should give clear and concise warnings to individuals who are conducting themselves in a manner that would cause their recording or

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Public Recording of Law Enforcement Activity

behavior to be unlawful. Accompanying the warnings should be clear directions on what an individual can do to be compliant; directions should be specific enough to allow compliance. For example, rather than directing an individual to clear the area, an officer could advise the person that he/she may continue observing and recording from the sidewalk across the street.

If an arrest or other significant enforcement activity is taken as the result of a recording that interferes with law enforcement activity, officers shall document in a report the nature and extent of the interference or other unlawful behavior and the warnings that were issued.

424.5 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to the scene when requested or any time the circumstances indicate a likelihood of interference or other unlawful behavior.

The supervisor should review the situation with the officer and:

- (a) Request any additional assistance as needed to ensure a safe environment.
- (b) Take a lead role in communicating with individuals who are observing or recording regarding any appropriate limitations on their location or behavior. When practical, the encounter should be recorded.
- (c) When practicable, allow adequate time for individuals to respond to requests for a change of location or behavior.
- (d) Ensure that any enforcement, seizure or other actions are consistent with this policy and constitutional and state law.
- (e) Explain alternatives for individuals who wish to express concern about the conduct of department members, such as how and where to file a complaint.

424.6 SEIZING RECORDINGS AS EVIDENCE

Officers should not seize recording devices or media unless (42 USC § 2000aa):

- (a) There is probable cause to believe the person recording has committed or is committing a crime to which the recording relates, and the recording is reasonably necessary for prosecution of the person.
 - 1. Absent exigency or consent, a warrant should be sought before seizing or viewing such recordings. Reasonable steps may be taken to prevent erasure of the recording.
- (b) There is reason to believe that the immediate seizure of such recordings is necessary to prevent serious bodily injury or death of any person.
- (c) The person consents.
 - 1. To ensure that the consent is voluntary, the request should not be made in a threatening or coercive manner.
 - 2. If the original recording is provided, a copy of the recording should be provided to the recording party, if practicable. The recording party should be permitted to be present while the copy is being made, if feasible. Another way to obtain the

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Public Recording of Law Enforcement Activity

evidence is to transmit a copy of the recording from a device to a department-owned device.

Recording devices and media that are seized will be submitted within the guidelines of the Property and Evidence Policy.

Medical Aid and Response

425.1 PURPOSE AND SCOPE

This policy recognizes that members often encounter persons in need of medical aid and establishes a law enforcement response to such situations.

425.2 POLICY

It is the policy of the South Saint Paul Police Department that all officers and other designated members be trained to provide emergency medical aid and to facilitate an emergency medical response.

425.3 FIRST RESPONDING MEMBER RESPONSIBILITIES

Whenever practicable, members should take appropriate steps to provide initial medical aid (e.g., first aid, CPR, use of an automated external defibrillator (AED)) in accordance with their training and current certification levels. This should be done for those in need of immediate care and only when the member can safely do so.

Prior to initiating medical aid, the member should contact Dispatch and request response by Emergency Medical Services (EMS) as the member deems appropriate.

Members should follow universal precautions when providing medical aid, such as wearing gloves and avoiding contact with bodily fluids, consistent with the Communicable Diseases Policy. Members should use a barrier or bag device to perform rescue breathing.

When requesting EMS, the member should provide Dispatch with information for relay to EMS personnel in order to enable an appropriate response, including:

- (a) The location where EMS is needed.
- (b) The nature of the incident.
- (c) Any known scene hazards.
- (d) Information on the person in need of EMS, such as:
 - 1. Signs and symptoms as observed by the member.
 - 2. Changes in apparent condition.
 - 3. Number of patients, sex, and age, if known.
 - 4. Whether the person is conscious, breathing, and alert, or is believed to have consumed drugs or alcohol.
 - 5. Whether the person is showing signs of extreme agitation or is engaging in violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics, and imperviousness to pain.

Members should stabilize the scene whenever practicable while awaiting the arrival of EMS.

Members should not direct EMS personnel whether to transport the person for treatment.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Medical Aid and Response

425.4 TRANSPORTING ILL AND INJURED PERSONS

Except in extraordinary cases where alternatives are not reasonably available, members should not transport persons who are unconscious, who have serious injuries or who may be seriously ill. EMS personnel should be called to handle patient transportation.

Officers should search any person who is in custody before releasing that person to EMS for transport.

An officer should accompany any person in custody during transport in an ambulance when requested by EMS personnel, when it reasonably appears necessary to provide security, when it is necessary for investigative purposes or when so directed by a supervisor.

Members should not provide emergency escort for medical transport or civilian vehicles.

425.5 PERSONS REFUSING EMS CARE

If a person who is not in custody refuses EMS care or refuses to be transported to a medical facility, an officer shall not force that person to receive care or be transported. However, members may assist EMS personnel when EMS personnel determine the person lacks mental capacity to understand the consequences of refusing medical care or to make an informed decision and the lack of immediate medical attention may result in serious bodily injury or the death of the person.

In cases where mental illness may be a factor, the officer should consider proceeding with a 72-hour hold in accordance with the Civil Commitments Policy.

If an officer believes that a person who is in custody requires EMS care and the person refuses, he/she should encourage the person to receive medical treatment. The officer may also consider contacting a family member to help persuade the person to agree to treatment or who may be able to authorize treatment for the person.

If the person who is in custody still refuses, the officer will require the person to be transported to the nearest medical facility. In such cases, the officer should consult with a supervisor prior to the transport.

Members shall not sign refusal-for-treatment forms or forms accepting financial responsibility for treatment.

425.6 MEDICAL ATTENTION RELATED TO USE OF FORCE

Specific guidelines for medical attention for injuries sustained from a use of force may be found in the Use of Force, Handcuffing and Restraints, Control Devices and Conducted Energy Device policies.

425.7 SICK OR INJURED ARRESTEE

If an arrestee appears ill or injured, or claims illness or injury, he/she should be medically cleared prior to booking. If the officer has reason to believe the arrestee is feigning injury or illness, the officer should contact a supervisor, who will determine whether medical clearance will be obtained prior to booking.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Medical Aid and Response

If the jail or detention facility refuses to accept custody of an arrestee based on medical screening, the officer should note the name of the facility person refusing to accept custody and the reason for refusal, and should notify a supervisor to determine the appropriate action.

Arrestees who appear to have a serious medical issue should be transported by ambulance. Officers shall not transport an arrestee to a hospital without a supervisor's approval.

Nothing in this section should delay an officer from requesting EMS when an arrestee reasonably appears to be exhibiting symptoms that appear to be life threatening, including breathing problems or an altered level of consciousness, or is claiming an illness or injury that reasonably warrants an EMS response in accordance with the officer's training.

425.8 ADMINISTRATION OF EPINEPHRINE

The department may obtain epinephrine auto-injectors from licensed pharmacies to be administered by trained members in accordance with Minn. Stat. § 144.999.

425.8.1 EPINEPHRINE USER RESPONSIBILITIES

Members who are qualified to administer epinephrine should handle, store, and administer the medication consistent with their training. Members should check the medication and associated administration equipment at the beginning of their shift to ensure they are serviceable and not expired. Any expired medication or unserviceable administration equipment should be removed from service and given to the Support Services Commander.

Any member who administers epinephrine should contact Dispatch as soon as possible and request response by EMS.

425.8.2 EPINEPHRINE REPORTING

Any member administering epinephrine should detail its use in an appropriate report.

425.8.3 EPINEPHRINE TRAINING

The Support Services Commander should ensure that training is provided to members authorized to administer epinephrine.

Training shall be conducted by an authorized provider and be completed every two years (Minn. Stat. § 144.999).

425.9 FIRST AID TRAINING

Subject to available resources, the Support Services Commander should ensure officers receive periodic first aid training appropriate for their position.

First Amendment Assemblies

426.1 PURPOSE AND SCOPE

This policy provides guidance for responding to public assemblies or demonstrations.

426.2 POLICY

The South Saint Paul Police Department respects the rights of people to peaceably assemble. It is the policy of this department not to unreasonably interfere with, harass, intimidate or discriminate against persons engaged in the lawful exercise of their rights, while also preserving the peace, protecting life and preventing the destruction of property.

426.3 GENERAL CONSIDERATIONS

Individuals or groups present on the public way, such as public facilities, streets or walkways, generally have the right to assemble, rally, demonstrate, protest or otherwise express their views and opinions through varying forms of communication, including the distribution of printed matter. These rights may be limited by laws or ordinances regulating such matters as the obstruction of individual or vehicle access or egress, trespass, noise, picketing, distribution of handbills, leafleting and loitering. However, officers shall not take action or fail to take action based on the opinions being expressed.

Participant behavior during a demonstration or other public assembly can vary. This may include, but is not limited to:

- Lawful, constitutionally protected actions and speech.
- Civil disobedience (typically involving minor criminal acts).
- Rioting.

All of these behaviors may be present during the same event. Therefore, it is imperative that law enforcement actions are measured and appropriate for the behaviors officers may encounter. This is particularly critical if force is being used. Adaptable strategies and tactics are essential. The purpose of a law enforcement presence at the scene of public assemblies and demonstrations should be to preserve the peace, to protect life and prevent the destruction of property.

Officers should not:

- (a) Engage in assembly or demonstration-related discussion with participants.
- (b) Harass, confront or intimidate participants.
- (c) Seize the cameras, cell phones or materials of participants or observers unless an officer is placing a person under lawful arrest.

Supervisors should continually observe department members under their commands to ensure that members' interaction with participants and their response to crowd dynamics is appropriate.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

First Amendment Assemblies

426.3.1 PHOTOGRAPHS AND VIDEO RECORDINGS

Photographs and video recording, when appropriate, can serve a number of purposes, including support of criminal prosecutions by documenting criminal acts; assistance in evaluating department performance; serving as training material; recording the use of dispersal orders; and facilitating a response to allegations of improper law enforcement conduct.

Photographs and videos will not be used or retained for the sole purpose of collecting or maintaining information about the political, religious or social views of associations, or the activities of any individual, group, association, organization, corporation, business or partnership, unless such information directly relates to an investigation of criminal activities and there is reasonable suspicion that the subject of the information is involved in criminal conduct.

426.4 UNPLANNED EVENTS

When responding to an unplanned or spontaneous public gathering, the first responding officer should conduct an assessment of conditions, including, but not limited to, the following:

- Location
- Number of participants
- Apparent purpose of the event
- Leadership (whether it is apparent and/or whether it is effective)
- Any initial indicators of unlawful or disruptive activity
- Indicators that lawful use of public facilities, streets or walkways will be impacted
- Ability and/or need to continue monitoring the incident

Initial assessment information should be promptly communicated to Dispatch, and the assignment of a supervisor should be requested. Additional resources should be requested as appropriate. The responding supervisor shall assume command of the incident until command is expressly assumed by another, and the assumption of command is communicated to the involved members. A clearly defined command structure that is consistent with the Incident Command System (ICS) should be established as resources are deployed.

426.5 PLANNED EVENT PREPARATION

For planned events, comprehensive, incident-specific operational plans should be developed. The ICS should be considered for such events.

426.5.1 INFORMATION GATHERING AND ASSESSMENT

In order to properly assess the potential impact of a public assembly or demonstration on public safety and order, relevant information should be collected and vetted. This may include:

- Information obtained from outreach to group organizers or leaders.
- Information about past and potential unlawful conduct associated with the event or similar events.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

First Amendment Assemblies

- The potential time, duration, scope, and type of planned activities.
- Any other information related to the goal of providing a balanced response to criminal activity and the protection of public safety interests.

Information should be obtained in a transparent manner, and the sources documented. Relevant information should be communicated to the appropriate parties in a timely manner.

Information will be obtained in a lawful manner and will not be based solely on the purpose or content of the assembly or demonstration, or actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability of the participants (or any other characteristic that is unrelated to criminal conduct or the identification of a criminal subject).

426.5.2 OPERATIONAL PLANS

An operational planning team with responsibility for event planning and management should be established. The planning team should develop an operational plan for the event.

The operational plan will minimally provide for the following:

- (a) Command assignments, chain of command structure, roles, and responsibilities
- (b) Staffing and resource allocation
- (c) Management of criminal investigations
- (d) Designation of uniform of the day and related safety equipment (e.g., helmets, shields)
 1. Uniforms must display the Department name and a unique personal identifier.
 2. A protocol for keeping record of any officers on scene who are not in compliance with uniform requirements due to exigent circumstances.
- (e) Deployment of specialized resources
- (f) Event communications and interoperability in a multijurisdictional event
- (g) Liaison with demonstration leaders and external agencies
- (h) Liaison with City government and legal staff
- (i) Media relations
- (j) Logistics: food, fuel, replacement equipment, duty hours, relief, and transportation
- (k) Traffic management plans
- (l) First aid and emergency medical service provider availability
- (m) Prisoner transport and detention
- (n) Review of policies regarding public assemblies and use of force in crowd control
- (o) Parameters for declaring an unlawful assembly (as defined by Minn. Stat. § 609.705)
- (p) Arrest protocol, including management of mass arrests
- (q) Protocol for recording information flow and decisions

South Saint Paul Police Department

S Saint Paul PD Policy Manual

First Amendment Assemblies

- (r) Rules of engagement, including rules of conduct, protocols for field force extraction and arrests, and any authorization required for the use of force
- (s) Protocol for handling complaints during the event
- (t) Parameters for the use of body-worn cameras and other portable recording devices

426.5.3 MUTUAL AID AND EXTERNAL RESOURCES

The magnitude and anticipated duration of an event may necessitate interagency cooperation and coordination. The assigned Incident Commander should ensure that any required memorandums of understanding or other agreements are properly executed, and that any anticipated mutual aid is requested and facilitated (see the Outside Agency Assistance Policy).

426.6 UNLAWFUL ASSEMBLY DISPERSAL ORDERS

If a public gathering or demonstration remains peaceful and nonviolent, and there is no reasonably imminent threat to persons or property, the Incident Commander should generally authorize continued monitoring of the event.

Should the Incident Commander make a determination that public safety is presently or is about to be jeopardized, the Incident Commander or the authorized designee should attempt to verbally persuade event organizers or participants to disperse of their own accord. Warnings and advisements may be communicated through established communications links with leaders and/or participants or to the group.

When initial attempts at verbal persuasion are unsuccessful, the Incident Commander or the authorized designee should make a clear standardized announcement to the gathering that the event is an unlawful assembly, and should order the dispersal of the participants. The announcement should be communicated by whatever methods are reasonably available to ensure that the content of the message is clear and that it has been heard by the participants. The announcement should be amplified, made in different languages as appropriate, made from multiple locations in the affected area and documented by audio and video. The announcement should provide information about what law enforcement actions will take place if illegal behavior continues and should identify routes for egress (at least two routes when possible). A reasonable time to disperse should be allowed following a dispersal order.

Additionally, the dispersal order must include:

- (a) The name and rank of the person and the agency giving the order.
- (b) The reasons for the declaration.
- (c) How long the participants have to comply.

The dispersal announcements should be repeated after commencement of the initial dispersal order so that participants understand that they must leave the area.

If, after a crowd disperses pursuant to a declaration of unlawful assembly and subsequently participants assemble at a different geographic location where the participants are engaged in non-violent and lawful First Amendment activity, such an assembly cannot be dispersed unless it

South Saint Paul Police Department

S Saint Paul PD Policy Manual

First Amendment Assemblies

has been determined that it is an unlawful assembly, and a new declaration of unlawful assembly has been made.

426.6.1 MINNESOTA POST GUIDELINES ON UNLAWFUL ASSEMBLY

The mere failure to obtain a permit, such as a parade permit or sound permit, is not a sufficient basis to declare an unlawful assembly.

The fact that some of the demonstrators or organizing groups have engaged in violent or unlawful acts on prior occasions or demonstrations is not grounds for declaring an assembly unlawful.

Whenever possible, the unlawful behavior of a few participants must not result in the majority of peaceful protestors being deprived of their First Amendment rights, unless other participants or officers are threatened with dangerous circumstances.

426.7 USE OF FORCE

Use of force is governed by current department policy and applicable law (see the Use of Force, Handcuffing and Restraints, Control Devices, and Conducted Energy Device policies).

Individuals refusing to comply with lawful orders (e.g., nonviolent refusal to disperse) should be given a clear verbal warning and a reasonable opportunity to comply. If an individual refuses to comply with lawful orders, the Incident Commander shall evaluate the type of resistance and adopt a reasonable response in order to accomplish the law enforcement mission (such as dispersal or arrest of those acting in violation of the law). Control devices and conducted energy devices should be considered only when the participants' conduct reasonably appears to present the potential to harm officers, themselves or others, or will result in substantial property loss or damage (see the Control Devices and the Conducted Energy Device policies).

Force or control devices, including oleoresin capsaicin (OC), should be directed toward individuals and not toward groups or crowds, unless specific individuals cannot reasonably be targeted due to extreme circumstances, such as a riotous crowd.

Any use of force by a member of this department shall be documented promptly, completely, and accurately in an appropriate report. The type of report required may depend on the nature of the incident.

426.8 ARRESTS

The South Saint Paul Police Department should respond to unlawful behavior in a manner that is consistent with the operational plan. If practicable, warnings or advisements should be communicated prior to arrest.

Mass arrests should be employed only when alternate tactics and strategies have been, or reasonably appear likely to be, unsuccessful. Mass arrests shall only be undertaken upon the order of the Incident Commander or the authorized designee. There must be probable cause for each arrest.

If employed, mass arrest protocols should fully integrate:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

First Amendment Assemblies

- (a) Reasonable measures to address the safety of officers and arrestees.
- (b) Dedicated arrest, booking and report writing teams.
- (c) Timely access to medical care.
- (d) Timely access to legal resources.
- (e) Timely processing of arrestees.
- (f) Full accountability for arrestees and evidence.
- (g) Coordination and cooperation with the prosecuting authority, jail and courts (see the Citation Releases Policy).

426.9 MEDIA RELATIONS

The Police Chief should use all available avenues of communication, including press releases, briefings, press conferences and social media to maintain open channels of communication with media representatives and the public about the status and progress of the event, taking all opportunities to reassure the public about the professional management of the event (see the Media Relations Policy).

- (a) Media personnel have a right to observe, document and disseminate information to the public regarding government activities that are conducted in public. Law enforcement shall never prevent, deter or otherwise intimidate media from lawfully capturing and providing this information to the public. Media shall be permitted to observe and shall be permitted close enough access during arrests to document the contact with the arrestees. Even after a dispersal order has been given, clearly documented and identified media shall be permitted to carry out their professional duties in any area where arrests are being made. However, if their presence would unduly interfere with the enforcement action, they shall be instructed to relocate to an area near the arrest location. Law enforcement shall ensure this policy is consistent with any court or state executive order such as a curfew order. This identified area must be made clear to the media personnel so that they understand where they need to relocate or what actions they must take. If after several requests have been made to the media to relocate due to their interference and individual media personnel fail to do so causing additional interference, those individuals may be arrested. A decision to arrest should be a last resort and the reasons for the arrest and why relocation was not successful must be fully documented. Media shall never be targeted for dispersal or enforcement action merely because of their status. Individuals claiming to be media personnel should provide credentials identifying who they are and the media outlet to which they are associated. If you are unable to identify who they are after credentials have been provided, efforts should be made to further identify them by whatever means is available.

426.10 DEMOBILIZATION

When appropriate, the Incident Commander or the authorized designee should implement a phased and orderly withdrawal of law enforcement resources. All relieved personnel should promptly complete any required reports, including use of force reports, and account for all issued equipment and vehicles to their supervisors prior to returning to normal operational duties.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

First Amendment Assemblies

426.11 POST EVENT

The Incident Commander should designate a member to assemble full documentation of the event, to include the following:

- (a) Operational plan
- (b) Any incident logs
- (c) Any assignment logs
- (d) Vehicle, fuel, equipment, and supply records
- (e) Incident, arrest, use of force, injury, and property damage reports
- (f) Photographs, audio/video recordings, Dispatch records/tapes
- (g) Media accounts (print and broadcast media)
- (h) Record of any unlawful assembly declarations

426.11.1 AFTER-ACTION REPORTING

The Incident Commander should work with City legal counsel, as appropriate, to prepare a comprehensive after-action report of the event, explaining all incidents where force was used including the following:

- (a) Date, time and description of the event
- (b) Actions taken and outcomes (e.g., injuries, property damage, arrests)
- (c) Problems identified
- (d) Significant events
- (e) Recommendations for improvement; opportunities for training should be documented in a generic manner, without identifying individuals or specific incidents, facts or circumstances.

426.12 TRAINING

Department members should receive periodic training regarding this policy, as well as the dynamics of crowd control and incident management. The Department should, when practicable, train with its external and mutual aid partners.

426.13 ADDITIONAL INCIDENT COMMANDER RESPONSIBILITIES

The Incident Commander is responsible for maintaining familiarity with the Minnesota model policy on Public Assembly and First Amendment Activity and incorporating additional protocols as appropriate for the department's preparedness in addressing:

- (a) Approved devices, tactics, and munitions.
- (b) Accessibility to the public assembly or demonstration by media representatives and other observers.
- (c) Additional documentation requirements, if any.

[See attachment: MN Public Assembly - First Amendment Rights Model Policy.pdf](#)

Crisis Intervention Incidents

427.1 SECTION TITLE

427.2 PURPOSE AND SCOPE

This policy provides guidelines for interacting with those who may be experiencing a mental health or emotional crisis. Interaction with such individuals has the potential for miscommunication and violence. It often requires an officer to make difficult judgments about a person's mental state and intent in order to effectively and legally interact with the individual.

427.2.1 DEFINITIONS

Definitions related to this policy include:

Person in crisis - A person whose level of distress or mental health symptoms have exceeded the person's internal ability to manage his/her behavior or emotions. A crisis can be precipitated by any number of things, including an increase in the symptoms of mental illness despite treatment compliance; non-compliance with treatment, including a failure to take prescribed medications appropriately; or any other circumstance or event that causes the person to engage in erratic, disruptive or dangerous behavior that may be accompanied by impaired judgment.

Mental Health Crisis Data (MHCD) - Data on individual clients or patients that is sought and received from community health centers, mental health divisions of counties and providers under contract with them, or private sector mental health providers for the purpose of safely responding to a mental health crisis.

427.3 POLICY

The South Saint Paul Police Department is committed to providing a consistently high level of service to all members of the community and recognizes that persons in crisis may benefit from intervention. The Department will collaborate, where feasible, with mental health professionals to develop an overall intervention strategy to guide its members' interactions with those experiencing a mental health crisis. This is to ensure equitable and safe treatment of all involved.

427.4 SIGNS

Members should be alert to any of the following possible signs of mental health issues or crises:

- (a) A known history of mental illness
- (b) Threats of or attempted suicide
- (c) Loss of memory
- (d) Incoherence, disorientation or slow response
- (e) Delusions, hallucinations, perceptions unrelated to reality or grandiose ideas
- (f) Depression, pronounced feelings of hopelessness or uselessness, extreme sadness or guilt
- (g) Social withdrawal

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Crisis Intervention Incidents

- (h) Manic or impulsive behavior, extreme agitation, lack of control
- (i) Lack of fear
- (j) Anxiety, aggression, rigidity, inflexibility or paranoia

Members should be aware that this list is not exhaustive. The presence or absence of any of these should not be treated as proof of the presence or absence of a mental health issue or crisis.

427.5 COORDINATION WITH MENTAL HEALTH PROFESSIONALS

The Chief of Police should designate an appropriate Division Commander to collaborate with mental health professionals to develop an education and response protocol. It should include a list of community resources to guide department interaction with those who may be suffering from mental illness or who appear to be in a mental health crisis.

427.5.1 OBTAINING MENTAL HEALTH INFORMATION

The Chief of Police should designate a member of the Department to develop access procedures, retention guidelines, data security safeguards, notification procedures, and any other applicable standards for obtained mental health information (Minn. Stat. § 626.8477).

Officers may seek information from a mental health professional during a crisis situation pursuant to department procedures. When information is requested, officers should provide an explanation why disclosure of mental health information is necessary to protect the health or safety of the individual in crisis or of another person (Minn. Stat. § 13.46; Minn. Stat. § 144.294).

Information obtained from mental health professionals in crisis incidents should generally be limited to that necessary to safely respond. Officers obtaining mental health information to address crisis incidents should document the following in the associated reports (Minn. Stat. § 13.46; Minn. Stat. § 144.294):

- (a) The name of the officer who requested the information
- (b) The name of the health professional who provided the information
- (c) The name of the individual experiencing the crisis

Mental health information obtained in these circumstances should not be used for any purpose beyond addressing the crisis. The subject of the information should be advised of the information obtained (Minn. Stat. § 13.46; Minn. Stat. § 144.294).

427.6 FIRST RESPONDERS

Safety is a priority for first responders. It is important to recognize that individuals under the influence of alcohol, drugs or both may exhibit symptoms that are similar to those of a person in a mental health crisis. These individuals may still present a serious threat to officers; such a threat should be addressed with reasonable tactics. Nothing in this policy shall be construed to limit an officer's authority to use reasonable force when interacting with a person in crisis.

Officers are reminded that mental health issues, mental health crises and unusual behavior alone are not criminal offenses. Individuals may benefit from treatment as opposed to incarceration.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Crisis Intervention Incidents

An officer responding to a call involving a person in crisis should:

- (a) Promptly assess the situation independent of reported information and make a preliminary determination regarding whether a mental health crisis may be a factor.
- (b) Request available backup officers and specialized resources as deemed necessary and, if it is reasonably believed that the person is in a crisis situation use conflict resolution and de-escalation techniques to stabilize the incident as appropriate.
- (c) If feasible, and without compromising safety, turn off flashing lights, bright lights or sirens.
- (d) Attempt to determine if weapons are present or available.
- (e) Take into account the person's mental and emotional state and potential inability to understand commands or to appreciate the consequences of his/her action or inaction, as perceived by the officer.
- (f) Secure the scene and clear the immediate area as necessary.
- (g) Employ tactics to preserve the safety of all participants.
- (h) Determine the nature of any crime.
- (i) Request a supervisor, as warranted.
- (j) Evaluate any available information that might assist in determining cause or motivation for the person's actions or stated intentions.
- (k) If circumstances reasonably permit, consider and employ alternatives to force.

427.7 DE-ESCALATION

Officers should consider that taking no action or passively monitoring the situation may be the most reasonable response to a mental health crisis.

Once it is determined that a situation is a mental health crisis and immediate safety concerns have been addressed responding members should be aware of the following considerations and should generally:

- Evaluate safety conditions.
- Introduce themselves and attempt to obtain the person's name.
- Be patient, polite, calm, courteous and avoid overreacting.
- Speak and move slowly and in a non-threatening manner.
- Moderate the level of direct eye contact.
- Remove distractions or disruptive people from the area.
- Demonstrate active listening skills (e.g., summarize the person's verbal communication).
- Provide for sufficient avenues of retreat or escape should the situation become volatile.

Responding officers generally should not:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Crisis Intervention Incidents

- Use stances or tactics that can be interpreted as aggressive.
- Allow others to interrupt or engage the person.
- Corner a person who is not believed to be armed, violent or suicidal.
- Argue, speak with a raised voice or use threats to obtain compliance.

427.8 INCIDENT ORIENTATION

When responding to an incident that may involve mental illness or a mental health crisis, the officer should request that the dispatcher provide critical information as it becomes available. This includes:

- (a) Whether the person relies on drugs or medication, or may have failed to take his/her medication.
- (b) Whether there have been prior incidents, suicide threats/attempts, and whether there has been previous police response.
- (c) Contact information for a treating physician or mental health professional.

Additional resources and a supervisor should be requested as warranted.

427.9 SUPERVISOR RESPONSIBILITIES

A supervisor should respond to the scene of any interaction with a person in crisis. Responding supervisors should:

- (a) Attempt to secure appropriate and sufficient resources.
- (b) Closely monitor any use of force, including the use of restraints, and ensure that those subjected to the use of force are provided with timely access to medical care (see the Handcuffing and Restraints Policy).
- (c) Consider strategic disengagement. Absent an imminent threat to the public and, as circumstances dictate, this may include removing or reducing law enforcement resources or engaging in passive monitoring.
- (d) Ensure that all reports are completed and that incident documentation uses appropriate terminology and language.
- (e) Conduct an after-action tactical and operational debriefing, and prepare an after-action evaluation of the incident to be forwarded to the Division Commander.
- (f) Evaluate whether a critical incident stress management debriefing for involved members is warranted.

427.10 INCIDENT REPORTING

Members engaging in any oral or written communication associated with a mental health crisis should be mindful of the sensitive nature of such communications and should exercise appropriate discretion when referring to or describing persons and circumstances.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Crisis Intervention Incidents

Members having contact with a person in crisis should keep related information confidential, except to the extent that revealing information is necessary to conform to department reporting procedures or other official mental health or medical proceedings.

427.10.1 DIVERSION

Individuals who are not being arrested should be processed in accordance with the Civil Commitments Policy.

427.11 CIVILIAN INTERACTION WITH PEOPLE IN CRISIS

Civilian members may be required to interact with persons in crisis in an administrative capacity, such as dispatching, records request, and animal control issues.

- (a) Members should treat all individuals equally and with dignity and respect.
- (b) If a member believes that he/she is interacting with a person in crisis, he/she should proceed patiently and in a calm manner.
- (c) Members should be aware and understand that the person may make unusual or bizarre claims or requests.

If a person's behavior makes the member feel unsafe, if the person is or becomes disruptive or violent, or if the person acts in such a manner as to cause the member to believe that the person may be harmful to him/herself or others, an officer should be promptly summoned to provide assistance.

427.12 EVALUATION

The Division Commander designated to coordinate the crisis intervention strategy for this department should ensure that a thorough review and analysis of the department response to these incidents is conducted annually. The report will not include identifying information pertaining to any involved individuals, officers or incidents and will be submitted to the Chief of Police through the chain of command.

427.13 TRAINING

In coordination with the mental health community and appropriate stakeholders, the Department will develop and provide comprehensive education and training to all department members to enable them to effectively interact with persons in crisis.

Additionally, the Support Services Commander will provide officers, including part-time officers, with in-service training in crisis intervention and mental illness crisis as required by Minn. Stat. § 626.8469 and Minn. Stat. § 626.8474.

Civil Disputes

428.1 PURPOSE AND SCOPE

This policy provides members of the South Saint Paul Police Department with guidance for addressing conflicts between persons when no criminal investigation or enforcement action is warranted (e.g., civil matters), with the goal of minimizing any potential for violence or criminal acts.

The Domestic Abuse Policy will address specific legal mandates related to domestic violence court orders. References in this policy to “court orders” apply to any order of a court that does not require arrest or enforcement by the terms of the order or by Minnesota law.

428.2 POLICY

The South Saint Paul Police Department recognizes that a law enforcement presence at a civil dispute can play an important role in the peace and safety of the community. Subject to available resources, members of this department will assist at the scene of civil disputes with the primary goal of safeguarding persons and property, preventing criminal activity and maintaining the peace. When handling civil disputes, members will remain impartial, maintain a calm presence, give consideration to all sides and refrain from giving legal or inappropriate advice.

428.3 GENERAL CONSIDERATIONS

When appropriate, members handling a civil dispute should encourage the involved parties to seek the assistance of resolution services or take the matter to the civil courts. Members must not become personally involved in disputes and shall at all times remain impartial.

While not intended to be an exhaustive list, members should give considerations to the following when handling civil disputes:

- (a) Civil disputes tend to be confrontational and members should be alert that they can escalate to violence very quickly. De-escalation techniques should be used when appropriate.
- (b) Members should not dismiss alleged or observed criminal violations as a civil matter and should initiate the appropriate investigation and report when criminal activity is apparent.
- (c) Members shall not provide legal advice, however, when appropriate, members should inform the parties when they are at risk of violating criminal laws.
- (d) Members are reminded that they shall not enter a residence or other non-public location without legal authority including valid consent.
- (e) Members should not take an unreasonable amount of time assisting in these matters and generally should contact a supervisor if it appears that peacekeeping efforts longer than 30 minutes are warranted.

428.4 COURT ORDERS

Disputes involving court orders can be complex. Where no mandate exists for an officer to make an arrest for a violation of a court order, the matter should be addressed by documenting any apparent

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Civil Disputes

court order violation in a report. If there appears to be a more immediate need for enforcement action, the investigating officer should consult a supervisor prior to making any arrest.

If a person appears to be violating the terms of a court order but is disputing the validity of the order or its applicability, the investigating officer should document the following:

- (a) The person's knowledge of the court order or whether proof of service exists.
- (b) Any specific reason or rationale the involved person offers for not complying with the terms of the order.

A copy of the court order should be attached to the report when available. The report should be forwarded to the appropriate prosecutor. The report should also be forwarded to the court issuing the order with a notice that the report was also forwarded to the prosecutor for review.

428.4.1 STANDBY REQUESTS

Officers responding to a call for standby assistance to retrieve property should meet the person requesting assistance at a neutral location to discuss the process. The person should be advised that items that are disputed will not be allowed to be removed. The member may advise the person to seek private legal advice as to the distribution of disputed property.

Members should accompany the person to the location of the property. Members should ask if the other party will allow removal of the property or whether the other party would remove the property.

If the other party is uncooperative, the person requesting standby assistance should be instructed to seek private legal advice and obtain a court order to obtain the items. Officers should not order the other party to allow entry or the removal of any items. If there is a restraining or similar order against the person requesting standby assistance, that person should be asked to leave the scene or they may be subject to arrest for violation of the order.

If the other party is not present at the location, the member will not allow entry into the location or the removal of property from the location.

428.5 VEHICLES AND PERSONAL PROPERTY

Officers may be faced with disputes regarding possession or ownership of vehicles or other personal property. Officers may review documents provided by parties or available databases (e.g., vehicle registration), but should be aware that legal possession of vehicles or personal property can be complex. Generally, officers should not take any enforcement action unless a crime is apparent. The people and the vehicle or personal property involved should be identified and the incident documented.

428.6 REAL PROPERTY

Disputes over possession or occupancy of real property (e.g., land, homes, apartments) should generally be handled through a person seeking a court order.

Medical Cannabis

429.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of this department with guidelines for investigating the possession, transportation, or use of medical cannabis under Minnesota's medical cannabis laws.

429.1.1 DEFINITIONS

Definitions related to this policy include (Minn. Stat. § 152.22):

Medical cannabis - Any species of the genus cannabis plant, or any mixture or preparation of them, including whole plant extracts and resins in the form of a liquid, oil, pill, or dried raw cannabis that is properly packaged and labeled with:

- (a) The name and address of the authorized manufacturer.
- (b) The patient's registry identification number, name, date of birth, and address.
- (c) The chemical composition of medical cannabis.
- (d) Recommended dosage.
- (e) Directions for use.
- (f) Batch number.
- (g) Date of manufacture.

Patient - A Minnesota resident who has been diagnosed with a qualifying medical condition by a health care practitioner and who has met any other requirements for patients under Minn. Stat. § 152.22 et seq.

Caregiver - A person who has been approved by the Minnesota Office of Cannabis Management to assist a patient who is unable to self-administer medication or acquire medical cannabis from a distribution facility, and who is authorized to assist the patient with the use of medical cannabis.

429.2 POLICY

It is the policy of the South Saint Paul Police Department to prioritize resources to avoid making arrests related to medical cannabis that the arresting officer reasonably believes would not be prosecuted by state or federal authorities.

Minnesota medical cannabis laws are intended to provide protection from prosecution to those who use or possess medical cannabis for medical purposes. The South Saint Paul Police Department will exercise discretion to ensure laws are appropriately enforced without unreasonably burdening both those individuals protected under Minnesota law and the resources of the Department.

429.3 INVESTIGATION

Investigations involving the possession or use of cannabis generally fall into one of the following categories:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Medical Cannabis

- (a) Investigations when no person makes a medicinal claim.
- (b) Investigations when a person claims to be a patient or caregiver.
- (c) Investigations when the person is otherwise authorized.

429.3.1 INVESTIGATIONS WITH NO MEDICAL CLAIM

In any investigation involving the possession, delivery, production, or use of a cannabis product or drug paraphernalia where no person claims that the cannabis is used for medicinal purposes, the officer should proceed with a criminal investigation if the amount is greater than permitted for personal use under Minn. Stat. § 342.09. A medicinal claim may be raised at any time, so officers should document any statements and observations that may be relevant to whether the cannabis was possessed or produced for medicinal purposes.

429.3.2 INVESTIGATIONS INVOLVING A PATIENT OR CAREGIVER

Generally, arrests should not be made for the possession of medical cannabis by a patient, a caregiver or the parent or legal guardian of a patient (Minn. Stat. § 152.32).

Possession of medical cannabis properly packaged and labeled by an authorized manufacturer should suffice for verification of a person's status as a patient. The possession of medical cannabis registry verification from the Minnesota Department of Health should also suffice for verification a person's status as a patient or caregiver (Minn. Stat. § 152.22; Minn. Stat. § 152.27).

429.3.3 EXCEPTIONS

This policy does not apply to the following offenses. Officers may take enforcement action if the person (Minn. Stat. § 152.23):

- (a) Possesses or engages in the use of medical cannabis on a school bus or van, on the grounds of any preschool or primary or secondary school, in any correctional facility, or on the grounds of any child care facility or home daycare.
- (b) Vaporizes or smokes medical cannabis on any form of public transportation, where the vapor or smoke would be inhaled by a non-patient minor child, or in any public place or a place of employment.
- (c) Operates any motor vehicle, aircraft, train, or motorboat, or works on transportation property, equipment, or facilities while under the influence of medical cannabis.

429.3.4 INVESTIGATIONS INVOLVING OTHER AUTHORIZED INDIVIDUALS

Any person falling into the following category shall not be arrested for the authorized possession of cannabis (Minn. Stat. § 342.515):

- (a) An otherwise authorized individual transporting cannabis plants or products between business facilities pursuant to state law.

429.4 FEDERAL LAW ENFORCEMENT

Officers should provide information regarding a medical cannabis investigation to federal law enforcement authorities when it is requested by federal law enforcement authorities or whenever the officer believes those authorities would have a particular interest in the information.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Medical Cannabis

429.5 EVIDENCE ROOM SUPERVISOR RESPONSIBILITIES

The Evidence Room supervisor shall ensure that medical cannabis, drug paraphernalia or other related property seized from a person engaged or assisting in the use of medical cannabis is not destroyed. Upon the prosecutor's decision to forgo prosecution, or the dismissal of charges or an acquittal, the Evidence Room supervisor shall as soon as practicable return to the person from whom it was seized any medical cannabis, drug paraphernalia or other related property.

The Evidence Room supervisor may not destroy medical cannabis except upon receipt of a court order.

The Evidence Room supervisor may release medical cannabis to federal law enforcement authorities upon presentation of a valid court order or by a written order of the Investigations supervisor.

429.6 REPORTING

Officers aware of a person experiencing a negative medical condition or a death related to a cannabis overdose, including as a result of an unauthorized access to medical cannabis, must contact the Minnesota Department of Health's Office of Medical Cannabis within five business days. If discovered as part of an ongoing investigation, the report must be made within 72 hours of the conclusion of the investigation (Minn. R. 4770.4002; Minn. R. 4770.4004).

Officers having reasonable suspicion of unauthorized possession of medical cannabis or of violations of cannabis laws by individuals authorized to possess medical cannabis, must report to the Office of Medical Cannabis using the designated online form. Reports related to unauthorized possession must be submitted within 72 hours, unless discovered as part of an ongoing investigation, in which case reporting must be made within 72 hours of the conclusion of the investigation. Reports of violations by persons authorized to possess medical cannabis must be submitted within 15 days (Minn. R. 4770.4010).

Suspicious Activity Reporting

430.1 PURPOSE AND SCOPE

This policy provides guidelines for reporting and investigating suspicious and criminal activity.

430.1.1 DEFINITIONS

Definitions related to this policy include:

Involved party - An individual who has been observed engaging in suspicious activity, as defined in this policy, when no definitive criminal activity can be identified, thus precluding the person's identification as a suspect.

Suspicious activity - Any reported or observed activity that a member reasonably believes may have a nexus to any criminal act or attempted criminal act, or to foreign or domestic terrorism. Actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions). Examples of suspicious activity may include but are not limited to:

- Suspected pre-operational surveillance or intelligence gathering (e.g., photographing security features, asking questions about sensitive security-related subjects).
- Tests of security measures and response to incidents (e.g., "dry run," creating false alarms, attempts to enter secure areas without authorization).
- Suspicious purchases (e.g., purchasing large quantities of otherwise legal items, such as fertilizer, that could be used to create an explosive or other dangerous device).
- An individual in possession of such things as a hoax explosive or dispersal device, sensitive materials (e.g., passwords, access codes, classified government information), or coded or ciphered literature or correspondence.

Suspicious Activity Report (SAR) - An incident report used to document suspicious activity.

430.2 POLICY

The South Saint Paul Police Department recognizes the need to protect the public from criminal conduct and acts of terrorism and shall lawfully collect, maintain and disseminate information regarding suspicious activities, while safeguarding civil liberties and privacy protections.

430.3 RESPONSIBILITIES

The Investigation Division Commander and authorized designees will manage SAR activities. Authorized designees should include supervisors who are responsible for department participation in criminal intelligence systems as outlined in the Criminal Organizations Policy.

The responsibilities of the Investigation Division Commander include, but are not limited to:

- (a) Remaining familiar with those databases available to the Department that would facilitate the purpose of this policy.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Suspicious Activity Reporting

- (b) Maintaining adequate training in the area of intelligence gathering to ensure no information is being maintained that would violate the law or civil rights of any individual.
- (c) Ensuring a process is available that would allow members to report relevant information. The process should be designed to promote efficient and quick reporting, and should not be cumbersome, duplicative or complicated.
- (d) Ensuring that members are made aware of the purpose and value of documenting information regarding suspicious activity, as well as the databases and other information resources that are available to the Department.
- (e) Ensuring that SAR information is appropriately disseminated to members in accordance with their job responsibilities.
- (f) Coordinating investigative follow-up, if appropriate.
- (g) Coordinating with any appropriate agency or fusion center.
- (h) Ensuring that, as resources are available, the Department conducts outreach that is designed to encourage members of the community to report suspicious activity and that outlines what they should look for and how they should report it (e.g., website, public service announcements).

430.4 REPORTING AND INVESTIGATION

Any department member receiving information regarding suspicious activity should take any necessary immediate and appropriate action, including a request for tactical response or immediate notification of specialized entities, when applicable. Any civilian member who receives such information should ensure that it is passed on to an officer in a timely manner.

If the suspicious activity is not directly related to a reportable crime, the member should prepare a SAR and include information about involved parties and the circumstances of the incident. If, during any investigation, an officer becomes aware of suspicious activity that is unrelated to the current investigation, the information should be documented separately in a SAR and not included in the original incident report. The report number of the original incident should be included in the SAR as a cross reference. A SAR should be processed as any other incident report.

430.5 HANDLING INFORMATION

The Records Section will forward copies of SARs, in a timely manner, to the following:

- Investigations supervisor
- Crime Analysis Unit
- Other authorized designees

Body-Worn Cameras

432.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of a body-worn camera (BWC) by members of this department and for the access, use, and retention of department BWC media (Minn. Stat. § 626.8473).

The provisions of this policy, including notice, documentation, access, and retention, also apply to other portable audio/video recording devices used by members, where applicable.

This policy does not apply to undercover operations, wiretaps, or eavesdropping (concealed listening devices).

432.1.1 DEFINITIONS

Definitions related to this policy include:

Activate - To place a BWC in active mode (also called event mode). In active mode, the BWC records both video and audio.

BWC media - The video, audio, and images captured by department BWCs and the associated metadata.

BWC media systems - Any software, including web-based programs and mobile applications, used by the Department to upload/download, store, view, transfer, and otherwise maintain BWC media.

Deactivate - To place a BWC in buffering mode (also called ready or pre-event mode). In buffering mode, the BWC records video (without audio) in short, predetermined intervals that are retained only temporarily. However, when a BWC is activated, the interval recorded immediately prior to activation is then stored as part of the BWC media. Deactivate does not mean powering off the BWC.

Event - A general term referring to a set of circumstances that may, but does not necessarily, correlate directly to a single public safety incident.

432.2 POLICY

It is the policy of the Department to use BWCs and BWC media for evidence collection and to accurately document events in a way that promotes member safety and department accountability and transparency while also protecting the privacy of members of the public.

432.3 RESPONSIBILITIES

432.3.1 BWC COORDINATOR RESPONSIBILITIES

The Chief of Police or the authorized designee should delegate certain responsibilities to a BWC coordinator (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

The responsibilities of the coordinator include:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

- (a) Serving as a liaison between the Department and the BWC manufacturer/distributor and any third-party media storage vendor.
- (b) Developing inventory and documentation procedures for issuing and tracking BWC equipment, including properly marking BWCs as property of the Department, recording the date each BWC is placed into or taken out of service, and maintaining the following information:
 - 1. The total number of devices owned or maintained by the South Saint Paul Police Department
 - 2. The daily record of the total number deployed and used by members and, if applicable, the precinct or district in which the devices were used
 - 3. The total amount of recorded audio and video data collected by the BWC media systems and maintained by the South Saint Paul Police Department
- (c) Assisting with troubleshooting and maintenance of BWC equipment and media systems and, when necessary, coordinating the repair or replacement of BWCs.
 - 1. All equipment and system malfunctions and their resolutions should be documented, and maintenance and repair records should be maintained for all BWCs.
- (d) Managing BWC media systems so that:
 - 1. Access is limited to the minimum necessary authorized users and user privileges are restricted to those necessary for the member to conduct assigned department duties.
 - 2. Security requirements, such as two-factor authentication and appropriate password parameters, are in place for user credentials.
 - 3. Procedures include a process to obtain written authorization for access to non-public data by SSP PD members and members of other governmental entities and agencies for a legitimate, specified law enforcement purpose (Minn. Stat. § 13.825, Subd. 7; Minn. Stat. § 13.825, Subd. 8).
- (e) Configuring BWC media systems, or developing manual procedures, so that media is appropriately categorized and retained according to the event type tagged by members.
- (f) Retaining audit logs or records of all access, alteration, and deletion of BWC media and media systems, and conducting periodic audits to ensure compliance with applicable laws, regulations, and department policy.
- (g) Developing and updating BWC training for members who are assigned a BWC or given access to BWC media systems.
- (h) Coordinating with the community relations coordinator to (see the Community Relations Policy):
 - 1. Provide the public with notice of the department's use of BWCs (e.g., posting on the department website or social media pages) (Minn. Stat. § 626.8473, Subd. 3).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

2. Gain insight into community expectations regarding BWC use.
- (i) Coordinating with the Records Supervisor to (see the Records Section, Records Maintenance and Release, and Protected Information policies):
 1. Determine and apply proper retention periods to BWC media (e.g., firearm discharges, certain use of force incidents, formal complaints) (Minn. Stat. § 13.825, Subd. 3).
 2. Develop procedures for the appropriate release of BWC media.
 3. Ensure procedures comply with the requirements of the Minnesota Government Data Practices Act and other applicable laws (Minn. Stat. § 13.01 et seq.).
- (j) Coordinating with the Evidence Room to develop procedures for the transfer, storage, and backup of evidentiary BWC media (see the Evidence Room Policy).
- (k) Completing an annual administrative review of the BWC program and providing it to the Chief of Police for review.
- (l) Preparing the biennial audit required by Minn. Stat. § 13.825, Subd. 9.
- (m) Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the South Saint Paul Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders (Minn. Stat. § 13.825, Subd. 10).

432.3.2 MEMBER RESPONSIBILITIES

Every member issued a BWC is responsible for its proper use, safekeeping, and maintenance.

At the beginning of each shift or period of BWC use, the member should inspect their assigned BWC to confirm it is charged and in good working order. As part of the inspection, the member should perform a function test by activating the BWC and recording a brief video stating their name, identification number, assignment, and the date and time (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

Members should wear their assigned BWC on their outermost garment positioned at or above the mid-line of the waist (Minn. Stat. § 626.8473). Members are responsible for ensuring there are no obstructions and that the BWC remains in a position suitable for recording.

When a BWC is not in the physical possession of the member to which it is assigned, it should be placed on the charging dock and stored in a secure location.

Members shall report any malfunction or damage to the BWC coordinator or on-duty supervisor as soon as practicable and, if possible, obtain a functioning BWC to use either temporarily while repairs are being made to the member's BWC or as a permanent replacement (Minn. Stat. § 626.8473).

Members shall comply with this policy's provisions while performing law enforcement activities under the command and control of another law enforcement agency (Minn. Stat. § 626.8473).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

432.4 BWC USE

The following guidelines apply to the use of BWCs:

- (a) Only department-issued BWCs should be used (Minn. Stat. § 13.825, Subd. 6).
- (b) BWCs should only be used by the member or members to whom it was issued unless otherwise authorized by a supervisor.
- (c) The use of department-issued BWCs shall be strictly limited to department-related activities.
- (d) Members shall not use BWCs or BWC media systems for which they have not received prior authorization and appropriate training.
- (e) Members shall immediately report unauthorized access or use of BWCs or BWC media systems by another member to their supervisor or the Chief of Police.

432.4.1 PROHIBITIONS

BWCs should not be used to record:

- (a) Routine administrative activities of the Department that do not involve interactions with the public. Care should be taken to avoid incidentally recording confidential documents that the Department has a duty to keep secure (i.e., criminal justice information).
- (b) Areas within the department facilities where members have a reasonable expectation of privacy (e.g., locker rooms or dressing areas, breakrooms) unless responding to a call for service or conducting an investigation.
- (c) Conversations of other members without their knowledge.
- (d) When a member is taking an authorized break or otherwise engaged in personal activities.
- (e) In a courtroom unless responding to a call for service or emergency situation.
- (f) Interactions with undercover officers or confidential informants.
- (g) Strip searches.

BWCs shall not be used for the purpose of embarrassment, harassment, or ridicule of any individual or group.

432.5 ACTIVATION OF BWC

Members should activate their BWC during all calls for service and the performance of law enforcement-related functions. Members are not required to activate their BWC during casual or informal contacts with members of the public that are not part of or related to law enforcement functions. However, members should activate their BWC any time a contact with an individual becomes hostile or adversarial.

Unless otherwise authorized by this policy or approved by a supervisor, BWCs should remain activated until the call for service or law enforcement-related function has concluded. A member may cease recording if they are simply waiting for a tow truck or a family member to arrive, or in other similar situations.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

At no time is a member expected to jeopardize their safety to activate their BWC. However, the BWC should be activated as soon as reasonably practicable in required situations.

If a member attempts to activate their BWC but the BWC fails to record an event, the member should notify their supervisor as soon as practicable.

432.5.1 NOTICE OF RECORDING

Unless otherwise approved based on unique circumstances, a member should wear the BWC in a manner that is conspicuous and shall answer truthfully if asked whether they are equipped with a BWC or if their BWC is activated.

432.5.2 PRIVACY CONSIDERATIONS

Members should remain sensitive to the dignity of individuals being recorded and should exercise sound discretion with respect to privacy concerns.

When responding to a place where individuals have an expectation of privacy (e.g., private residences, medical or mental health facilities, restrooms) or to a sensitive situation (e.g., individuals partially or fully unclothed), members are permitted to mute or deactivate their BWC if it reasonably appears that the privacy concern outweighs any legitimate department interest in recording the event. Members may also mute or deactivate their BWC:

- (a) To protect the privacy of a victim or witness.
- (b) When an individual wishes to provide information anonymously.
- (c) To avoid recording a confidential informant or undercover officer.
- (d) When discussing case tactics or strategy.
- (e) During private conversations with other members or emergency responders.

Members should choose to mute rather than deactivate BWCs when practicable. Deactivation should only be used when muting the BWC will not accomplish the level of privacy necessary for the situation.

Before muting or deactivating their BWC, the member should verbally narrate the reason on the recording. As soon as possible once the privacy concern is no longer an issue, or when circumstances change so that the privacy concern no longer outweighs the department's interest in recording the event (e.g., the individual becomes combative, the conversation ends), the member should unmute or reactivate their BWC and verbally note that recording has resumed.

432.5.3 LIVESTREAMING

Livestreaming enables authorized individuals to remotely view the audio and video captured by a member's BWC in real time. Only supervisors and dispatchers approved by the Chief of Police or the authorized designee shall have access to livestreaming capabilities.

Livestreaming should only be activated:

- (a) For purposes of member safety when the member is not responding to their radio or there is some other indication of distress.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

- (b) To assist with situational awareness or tactical decisions during a significant incident.
- (c) When requested by the member.

432.5.4 DOCUMENTATION

Members are encouraged to provide narration while using a BWC when it would be useful to provide context or clarification of the events being recorded. However, the use of a BWC is not a replacement for written reports and should not be referred to in a written report in place of detailing the event.

Every report prepared by a member who is issued a BWC should state "BWC available" or "BWC unavailable," as applicable, and should document:

- (a) To the extent practicable and relevant, the identity of individuals appearing in the BWC media.
- (b) An explanation of why BWC media is unavailable including any malfunction, damage, or battery issue that resulted in the failure of the BWC to capture all or part of the event.
- (c) Any exigency or other circumstances that prevented the member from immediately activating the recording at the beginning of the event.
- (d) Any period of the event in which the member deactivated or muted their BWC and the reason for such action.
- (e) If livestreaming was activated during the event, the reason for livestreaming and the members who communicated or participated in the event through BWC livestreaming.

432.6 UPLOADING BWC MEDIA

Unless otherwise authorized by a supervisor, all media from a member's BWC should be properly uploaded and tagged before the end of their shift. BWC media related to a serious or high-profile event (e.g., search for a missing child, active shooter situation) should be uploaded and tagged as soon as practicable upon returning to the Department.

Following an officer involved shooting or death or other event deemed necessary, a supervisor should take possession of the BWC for each member present and upload and tag the BWC media.

432.6.1 TAGGING BWC MEDIA

Members should tag all media captured by their BWC with their name and/or identification number, the case or incident number, and the event type. BWC media should be tagged upon uploading or, if capabilities permit tagging in the field, as close to the time of the event as possible. If more than one event type applies to BWC media, it should be tagged with each event type. If BWC media can only be tagged with a single event type, the media should be tagged using the event type with the longest retention period.

BWC media depicting sensitive circumstances or events should be tagged as restricted. BWC media should be flagged for supervisor review when it pertains to a significant event such as:

- (a) An incident that is the basis of a formal or informal complaint or is likely to result in a complaint.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

- (b) When a member has sustained a serious injury or a line-of-duty death has occurred.
- (c) When a firearm discharge or use of force incident has occurred.
- (d) An event that has attracted or is likely to attract significant media attention.

Supervisors should conduct audits at regular intervals to confirm BWC media is being properly uploaded and tagged by their subordinates.

432.7 BWC MEDIA

All BWC media is the sole property of the Department. Members shall have no expectation of privacy or ownership interest in the content of BWC media.

All BWC media shall be stored and transferred in a manner that is physically and digitally secure with appropriate safeguards to prevent unauthorized modification, use, release, or transfer. Contracts with any third-party vendors for the storage of BWC media should include provisions specifying that all BWC media remains the property of the Department and shall not be used by the vendor for any purpose without explicit approval of the Chief of Police or the authorized designee.

Members shall not alter, copy, delete, release, or permit access to BWC media other than as permitted in this policy without the express consent of the Chief of Police or the authorized designee.

BWC media systems should not be accessed using personal devices unless authorized by the Chief of Police or the authorized designee.

432.7.1 ACCESS AND USE OF BWC MEDIA

BWC media systems shall only be accessed by authorized members using the member's own login credentials and in accordance with the Information Technology Use Policy.

BWC media shall only be accessed and viewed for legitimate department-related purposes in accordance with the following guidelines:

- (a) BWC media tagged as restricted should only be accessible by those designated by the Chief of Police or the authorized designee.
- (b) Members may review their own BWC media for department-related purposes. Members should document in their report if they reviewed BWC media before completing the report.
- (c) Investigators may review BWC media pertaining to their assigned cases.
- (d) A member testifying regarding a department-related event may review the pertinent BWC media before testifying.
- (e) Supervisors are permitted to access and view BWC media of their subordinates.
 - 1. Supervisors should review BWC media that is tagged as a significant event or that the supervisor is aware pertains to a significant event.
 - 2. Supervisors should conduct documented reviews of their subordinate's BWC media at least annually to evaluate the member's performance, verify compliance with department procedures, and determine the need for additional

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

training. The review should include a variety of event types when possible. Supervisors should review BWC media with the recording member when it would be beneficial to provide guidance or to conduct one-on-one informal training for the member (Minn. Stat. § 626.8473).

3. Supervisors should conduct periodic reviews of a sample of each subordinate's BWC media to evaluate BWC use and ensure compliance with this policy.
- (f) The Support Services Commander is permitted to access and view BWC media for training purposes.
1. The Support Services Commander should conduct a quarterly review of a random sampling of BWC media to evaluate department performance and effectiveness and to identify specific areas where additional training or changes to protocols would be beneficial. Training Committee members may review BWC media as part of their review to identify training needs.
 2. The Support Services Commander may use BWC media for training purposes with the approval of the Chief of Police or the authorized designee. The Support Services Commander should use caution to avoid embarrassing or singling out a member and, to the extent practicable, should seek consent from the members appearing in the BWC media before its use for training. When practicable, sensitive issues depicted in BWC media should be redacted before being used for training.
- (g) The Records Supervisor may access BWC media when necessary to conduct department-related duties.
- (h) The BWC coordinator may access BWC media and the BWC media system as needed to ensure the system is functioning properly, provide troubleshooting assistance, conduct audits, and fulfill other responsibilities related to their role.
- (i) Any member who accesses or releases BWC media without authorization may be subject to discipline (see the Standards of Conduct and the Protected Information policies for additional guidance) (Minn. Stat. § 626.8473, Subd. 3).
- (j) Members may be subject to criminal penalties for the misuse of BWC media pursuant to Minn. Stat. § 13.09 (Minn. Stat. § 626.8473, Subd. 3).

432.7.2 PUBLIC ACCESS

Unless disclosure is required by law or a court order, BWC media should not be released to the public if:

- (a) It is clearly offensive to common sensibilities (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2; Minn. Stat. § 13.825, Subd. 4).
- (b) It unreasonably violates a person's privacy or depicts the interior of:
 1. A private residence.
 2. A facility that offers health care, mental health or substance abuse treatment, or social services.
 3. A school building.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

4. Any other building in which public access is restricted or which implicates heightened security concerns.

Except as provided by Minn. Stat. § 13.825, Subd. 2 or pursuant to Minn. Stat. § 13.82, Subd. 15, BWC media is considered private or nonpublic data.

432.7.3 ACCESS BY OTHER LAW ENFORCEMENT AGENCIES AND GOVERNMENT ENTITIES

Other law enforcement agencies and government entities (e.g., prosecutors, criminal justice agencies) may obtain access to not public BWC media for a legitimate, specified law enforcement purpose upon written authorization from the Chief of Police or the authorized designee and pursuant to department protocols (Minn. Stat. § 13.825, Subd. 8).

432.7.4 ACCESS BY PERSONS CAPTURED ON BWC MEDIA

Any person captured on BWC media may have access to the BWC media. If the individual requests a copy of the BWC media and does not have the consent of other non-law enforcement individuals captured on the BWC media, the identity of those individuals must be blurred or obscured sufficiently to render the person unidentifiable prior to release unless otherwise provided by law. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17 (Minn. Stat. § 13.825, Subd. 4).

432.7.5 ACCESS TO BWC MEDIA USED IN COLLISION INVESTIGATIONS

Individuals shall be provided with unredacted BWC media used in a collision investigation if the individual (Minn. Stat. § 13.825, Subd. 4):

- (a) Is entitled to a collision report under Minn. Stat. § 169.09
- (b) Submits a written request accompanied by the related collision report

The Department may deny access to unredacted data as provided in Minn. Stat. § 13.825, Subd. 4.

432.7.6 BWC MEDIA REGARDING USE OF FORCE INCIDENTS RESULTING IN DEATH

When a person dies as a result of the use of force by an officer, the Department shall (Minn. Stat. § 13.825, Subd. 2; Minn. Stat. § 626.8473, Subd. 3):

- (a) Allow certain individuals as identified in Minn. Stat. § 13.825, upon request, to inspect all portable recording system data that documents the incident within five days of the request pursuant to the provisions of Minn. Stat. § 13.825.
- (b) Release all portable recording system data that documents the incident within 14 days of the incident pursuant to the provisions of Minn. Stat. § 13.825.

432.7.7 DENIALS, REDACTIONS, AND NOTICES

Requests for the release of BWC media shall be processed in accordance with the Records Maintenance and Release Policy. The Records Supervisor should review BWC media before public release.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

The Chief of Police should work with the Custodian of Records when redactions, denials, or notices (e.g., reason for denial, potential penalties for misuse, seeking court relief) are necessary (Minn. Stat. § 13.825, Subd. 2; Minn. Stat. § 13.825, Subd. 4; Minn. Stat. § 626.8473, Subd. 3).

432.8 RETENTION OF BWC MEDIA

Non-evidentiary BWC media should be retained in accordance with state records retention laws but in no event for a period less than 90 days (Minn. Stat. § 13.825).

Unless circumstances justify continued retention, BWC media should be permanently deleted upon the expiration of the retention period in a way that it cannot be retrieved. BWC media shall not otherwise be deleted by any person without the authorization of the Chief of Police or the authorized designee.

If an individual captured on BWC media submits a written request, the BWC media shall be retained for an additional time period up to 180 days. The BWC coordinator should be responsible for notifying the individual that the BWC media will then be destroyed unless a new request is made (Minn. Stat. § 13.825, Subd. 3).

Members shall not alter, erase, or destroy any BWC media, before the end of the applicable retention period (Minn. Stat. § 626.8473).

432.8.1 EVIDENTIARY BWC MEDIA

BWC media relevant to a criminal prosecution should be exported from the BWC media system and securely transferred to digital evidence storage according to established department procedures. Evidentiary BWC media is subject to the same laws, policies, and procedures as all other evidence, including chain of custody, accessibility, and retention periods (see the Evidence Room Policy).

432.8.2 EVIDENTIARY RETENTION REQUIREMENTS

BWC media documenting the following incidents must be retained for a minimum of one year and destroyed according to the department's records retention schedule (Minn. Stat. § 13.825, Subd. 3):

- (a) Any reportable firearms discharge
- (b) Any use of force by an officer resulting in substantial bodily harm
- (c) Any incident that results in a formal complaint against an officer

Evidentiary BWC media that documents an officer's use of deadly force must be maintained indefinitely (Minn. Stat. § 13.825; Minn. Stat. § 626.8473).

432.9 TRAINING

The BWC coordinator should ensure that each member issued a BWC receives initial training before use, and periodic refresher training thereafter. Training should include:

- (a) Proper use of the BWC device and accessories.
- (b) When BWC activation is required, permitted, and prohibited.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body-Worn Cameras

- (c) How to respond to an individual's request to stop recording.
- (d) Proper use of the BWC media systems, including uploading and tagging procedures.
- (e) Security procedures for BWC media, including appropriate access and use.

Members who are not issued a BWC but who have access to BWC media systems shall receive training on the BWC media system, including appropriate access, use, and security procedures.

School Resource Officers

433.1 PURPOSE AND SCOPE

This policy describes the South Saint Paul Police Department School Resource Officer (SRO) program (Minn. Stat. § 626.8482).

433.2 POLICY

The South Saint Paul Police Department is committed to enhancing the safety of students and faculty on campuses located in the department's jurisdiction by forming a partnership with school administrators, faculty members, and students.

433.3 SCHOOL RESOURCE OFFICER PROGRAM

The Chief of Police should appoint SROs to serve in elementary, middle, and secondary schools upon contract with local school districts or charter schools. The goals and objectives of the SRO program are to provide a safe learning environment, provide valuable resources to school staff members, foster a positive relationship with students, and develop strategies to resolve problems. Methods to achieve these goals and objectives include but are not limited to:

- (a) Assisting with the development and implementation of a school safety plan.
- (b) Protecting the school against external threats by preventing unauthorized access to school property, and securing the school against a natural disaster or other violence.
- (c) Creating respect for law and order in the public school system and minimizing criminal activity.
- (d) Identifying students at risk of becoming involved in the criminal justice system and guiding them toward more positive and socially acceptable ways to behave.
- (e) Reducing criminal activity on or near a school campus.
- (f) Enhancing communication and understanding between students, their families, district staff, and the Department.
- (g) Assisting with the coordination of security measures for school activities such as sports events, dances, and other large gatherings, if applicable.
- (h) Auditing security measures, at least annually, throughout the school and making recommendations to enhance safety and reduce risk.

433.3.1 SRO CONTRACT

The contract between the school district or charter school and the Department shall:

- (a) Include the SRO's duties set forth in Minn. Stat. 626.8482, Subd. 2.
- (b) Address a mutually agreed upon policy regarding the use of plain clothes, modified uniforms, and other changes to SRO attire.
- (c) Articulate the role, if any, of the school district or charter school in the selection, vetting, and retention of the SRO.
- (d) Establish a public notification process that an SRO will be present in the schools.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

School Resource Officers

- (e) Address data practices policies and procedures.

A school district or charter school may contract with the Department for the SRO to perform additional duties (Minn. Stat. § 626.8482, Subd. 2). The contract should cover paid services, where applicable. The contract should also address how the SRO will be informed of school district resources available to school staff to assist with de-escalation of conflicts in school (e.g., specialized crisis teams, mediation opportunities).

433.4 SCHOOL RESOURCE OFFICER DUTIES

The SRO duties and responsibilities include (Minn. Stat. § 626.8482, Subd. 2):

- (a) Fostering a positive school climate through relationship building and open communication.
- (b) Protecting students, staff, and visitors to the school grounds from criminal activity.
- (c) Serving as a liaison from law enforcement to school officials.
- (d) Providing advice on safety drills.
- (e) Identifying vulnerabilities in school facilities and safety protocols.
- (f) Educating and advising students and staff on law enforcement topics.
- (g) Enforcing criminal laws.

433.5 USE OF FORCE

SROs should exercise age-appropriate and developmentally appropriate practices when interacting with students.

SROs shall not use force or their authority solely to enforce school rules or policies or participate in the enforcement of discipline for violations of school rules (Minn. Stat. § 626.8482, Subd. 2).

SROs should employ de-escalation techniques and physical intervention strategies consistent with their training, using only that amount of force that reasonably appears necessary given the facts and circumstances perceived by the SRO at the time of the event to accomplish a legitimate law enforcement purpose. See the Use of Force Policy for additional guidance.

433.6 ARREST CONSIDERATIONS

When a criminal incident also involves a violation of school rules, SROs should consider referral of the matter to school authorities in lieu of formal criminal referral, as appropriate for the incident.

Custodial arrests in school should be avoided if reasonably practical. If a custodial arrest is necessary because of exigency or public safety considerations, the arrest should be made in a non-communal area away from the view of other students if practicable.

When reasonably practicable, appropriate school staff should be notified prior to and/or present during the custodial arrest of a student.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

School Resource Officers

433.7 STUDENT AND PARENT DATA

Department records containing student and parent data shall be maintained pursuant to state law and the Records Maintenance and Release Policy.

433.8 TRAINING

SROs shall complete required initial and ongoing POST-approved training within the required timeframes. The SRO's most recent training documents shall be maintained in the SRO's training file (Minn. Stat. § 626.8482, Subd. 3) (See the Personnel Records Policy for additional guidance).

433.9 POLICY REVIEW

The SRO shall review this policy prior to assuming SRO duties (Minn. Stat. § 626.8482, Subd. 3(c)).

Chapter 5 - Traffic Operations

Traffic Function and Responsibility

500.1 PURPOSE AND SCOPE

The ultimate goal of traffic law enforcement is to reduce traffic collisions. This may be achieved through the application of such techniques as geographic/temporal assignment of personnel and equipment and the establishment of preventative patrols to deal with specific categories of unlawful driving behavior. Traffic enforcement techniques are based on collision data, enforcement activity records, traffic volume and traffic conditions. This department provides enforcement efforts toward violations, not only in proportion to the frequency of their occurrence in collision situations but also in terms of traffic-related needs.

500.3 ENFORCEMENT

Enforcement actions are commensurate with applicable laws and take into account the degree and severity of the violation committed. This department does not establish ticket quotas and the number of citations issued by any officer shall not be used when evaluating officer performance (Minn. Stat. § 169.985; Minn. Stat. § 299D.08). The visibility and quality of an officer's work effort will be commensurate with the philosophy of this policy. Several methods are effective in the reduction of collisions:

500.3.1 WARNINGS

Warnings or other non-punitive enforcement actions should be considered in each situation and substituted for arrests or citations when circumstances warrant.

500.3.2 TRAFFIC CITATIONS

Traffic citations may be issued when an officer believes it is appropriate. It is essential that officers fully explain the rights and requirements imposed on motorists upon issuance of a citation for a traffic violation. Officers should provide the following information at a minimum:

- (a) Explanation of the violation or charge.
- (b) Court appearance procedure, including the optional or mandatory appearance by the motorist.
- (c) Notice of whether the motorist can enter a plea and pay the fine by mail or at the court.
- (d) The court contact information.

500.3.3 TRAFFIC CITATION COURT JURISDICTION

An officer who issues a traffic citation shall ensure that the citation is properly directed to the court having jurisdiction (Minn. Stat. § 169.91 Subd. 3).

500.3.4 PHYSICAL ARREST

Physical arrest can be made on a number of criminal traffic offenses. These physical arrest cases usually deal with, but are not limited to (Minn. Stat. § 169.91):

- (a) Negligent homicide.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Traffic Function and Responsibility

- (b) Driving under the influence of alcohol/drugs.
- (c) Hit-and-run resulting in serious injury or death.
- (d) Hit-and-run resulting in damage to any vehicle or property.

500.3.5 LIMITATION AND DISCLOSURE OF REASON FOR TRAFFIC STOP

Officers conducting a traffic stop for violations of Minnesota Statute Chapters 168 or 169 shall not ask the motorist if they can identify the reason for the traffic stop. Officers shall state a reason for the stop unless it would be unreasonable to do so under the totality of the circumstances (Minn. Stat. § 169.905).

500.3 HIGH-VISIBILITY VESTS

The Department has provided American National Standards Institute (ANSI) Class II high-visibility vests to increase the visibility of department members who may be exposed to hazards presented by passing traffic, maneuvering or operating vehicles, machinery and equipment (23 CFR 655.601; Minn. R. 5205.0030).

Although intended primarily for use while performing traffic-related assignments, high-visibility vests should be worn at any time increased visibility would improve the safety or efficiency of the member.

500.3.1 REQUIRED USE

Except when working in a potentially adversarial or confrontational role, such as during vehicle stops, high-visibility vests should be worn at any time it is anticipated that an employee will be exposed to the hazards of approaching traffic or construction and recovery equipment. Examples of when high-visibility vests should be worn include traffic control duties, collision investigations, lane closures and while at disaster scenes, or any time high visibility is desirable. When emergency conditions preclude the immediate donning of the vest, officers should retrieve and wear the vest as soon as conditions reasonably permit. Use of the vests shall also be mandatory when directed by a supervisor.

Vests maintained in the investigation units may be used any time a plain clothes officer might benefit from being readily identified as an officer.

500.3.2 CARE AND STORAGE OF HIGH-VISIBILITY VESTS

High-visibility vests shall be maintained in the trunk of each patrol and investigation unit, in the side box of each police motorcycle and in the saddlebag or gear bag of each police bicycle. Each vest should be stored inside the resealable plastic bag provided to protect and maintain the vest in a serviceable condition. Before going into service each employee shall ensure a serviceable high-visibility vest is properly stored.

A supply of high-visibility vests will be maintained in the equipment room for replacement of damaged or unserviceable vests. The Support Services Commander should be promptly notified whenever the supply of vests in the equipment room needs replenishing.

Traffic Collisions

501.1 PURPOSE AND SCOPE

This policy provides guidelines for responding to and investigating traffic collisions.

501.2 POLICY

It is the policy of the South Saint Paul Police Department to respond to traffic collisions and render or summon aid to injured victims as needed. The Department will investigate and prepare reports according to the established minimum reporting requirements with the goal of reducing the occurrence of collisions by attempting to identify the cause of the collision and through enforcing applicable laws. Unless restricted by law, traffic collision reports will be made available to the public upon request.

501.3 RESPONSE

Upon arriving at the scene, the responding member should assess the need for additional resources and summon assistance as appropriate. Generally, the member initially dispatched to the scene will be responsible for the investigation and report, if required, unless responsibility is reassigned by a supervisor.

A supervisor should be called to the scene when the incident:

- (a) Is within the jurisdiction of this department and there is:
 - 1. A life-threatening injury.
 - 2. A fatality.
 - 3. A City vehicle involved.
 - 4. A City official or employee involved.
 - 5. Involvement of an on- or off-duty member of this department.
- (b) Is within another jurisdiction and there is:
 - 1. A City of South Saint Paul vehicle involved.
 - 2. A City of South Saint Paul official involved.
 - 3. Involvement of an on-duty member of this department.

501.3.1 MEMBER RESPONSIBILITIES

Upon arriving at the scene, the responding member should consider and appropriately address:

- (a) Traffic direction and control
- (b) Proper placement of emergency vehicles, cones, roadway flares or other devices if available to provide protection for members, the public and the scene.
- (c) First aid for any injured parties if it can be done safely.
- (d) The potential for involvement of hazardous materials.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Traffic Collisions

- (e) The need for additional support as necessary (e.g., traffic control, emergency medical services, fire department, HAZMAT, tow vehicles).
- (f) Clearance and cleanup of the roadway.

501.4 NOTIFICATION

If a traffic collision involves a life-threatening injury or fatality, the responding officer shall notify a supervisor, or if unavailable, a command staff member. The supervisor may assign an investigator or other appropriate personnel to investigate the incident. The supervisor will ensure notification is made in accordance with the Major Incident Notification Policy.

501.4.1 NOTIFICATION OF FAMILY

In the event of a life-threatening injury or fatality, the supervisor responsible for the incident should ensure notification of the victim's immediate family or coordinate such notification with the Medical Examiner, department chaplain or another suitable person. Notification should be made as soon as practicable following positive identification of the victim.

The identity of any person seriously injured or deceased in a traffic collision should not be released until notification is made to the victim's immediate family.

501.5 MINIMUM REPORTING REQUIREMENTS

A collision report shall be taken when:

- (a) A fatality, any injury (including complaint of pain), impaired driving or hit and run is involved.
- (b) An on-duty member of the City of South Saint Paul is involved.
- (c) The collision results in any damage to any City-owned or leased vehicle.
- (d) The collision involves any other public agency driver or vehicle.
- (e) There is damage to public property.
- (f) There is damage to any vehicle to the extent that towing is required.
- (g) Prosecution or follow-up investigation is contemplated.
- (h) Directed by a supervisor.

501.5.1 CITY VEHICLE INVOLVED

A traffic collision report shall be taken when a City vehicle is involved in a traffic collision that results in property damage or injury.

A general information report may be taken in lieu of a traffic collision report at the direction of a supervisor when the incident occurs entirely on private property or does not involve another vehicle.

Whenever there is damage to a City vehicle, a vehicle damage report shall be completed and forwarded to the appropriate Division Commander. The traffic investigator or supervisor at the scene should determine what photographs should be taken of the scene and the vehicle damage.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Traffic Collisions

501.5.2 INJURED ANIMALS

Department members should refer to the [Animal Control] Policy when a traffic collision involves the disposition of an injured animal.

501.6 INVESTIGATION

When a traffic collision meets minimum reporting requirements the investigation should include, at a minimum:

- (a) Identification and interview of all involved parties.
- (b) Identification and interview of any witnesses.
- (c) A determination of whether a violation of law has occurred and the appropriate enforcement action.
- (d) Identification and protection of items of apparent evidentiary value.
- (e) Documentation of the incident as necessary (e.g., statements, measurements, photographs, collection of evidence and reporting) on the appropriate forms.

501.6.1 INVESTIGATION BY OUTSIDE LAW ENFORCEMENT AGENCY

The Operations Commander or on-duty Sergeant should request that the Minnesota Department of Public Safety or other outside law enforcement agency investigate and complete a traffic collision investigation when a life-threatening injury or fatal traffic collision occurs within the jurisdiction of the South Saint Paul Police Department and involves:

- (a) An on- or off-duty member of the Department.
 - (a) The involved member shall complete the department traffic collision report. If the member is unable to complete the report, the supervisor shall complete it.
- (b) An on-or off-duty official or employee of the City of South Saint Paul.

Department members shall promptly notify a supervisor when any department vehicle is involved in a traffic collision. The collision investigation and report shall be completed by the agency having jurisdiction.

501.6.2 COMMERCIAL VEHICLE COLLISIONS

Commercial vehicle collisions additionally require notification to the Minnesota State Patrol if the collision results in (Minn. Stat. § 169.783):

- (a) A fatality.
- (b) Bodily injury to a person who, as a result of the injury, immediately receives medical treatment away from the scene of the collision.
- (c) One or more vehicles incurring disabling damage as a result of the collision, requiring the vehicle to be transported away from the scene by tow truck or other motor vehicle.

A waiver or inspection by a state trooper or other authorized person is required before a person may drive a commercial motor vehicle that was involved in such a collision (Minn. Stat. § 169.783).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Traffic Collisions

501.7 ENFORCEMENT ACTION

After a thorough investigation in which physical evidence or independent witness statements indicate that a violation of a traffic law contributed to the collision, authorized members should issue a citation or arrest the offending driver, as appropriate.

More serious violations, such as driving under the influence of drugs or alcohol, vehicular manslaughter, or other felonies, shall be enforced. If a driver who is subject to enforcement action is admitted to a hospital, a supervisor shall be contacted to determine the best enforcement option.

501.8 REPORTS

Department members shall utilize forms approved by the Minnesota Department of Public Safety as required for the reporting of traffic collisions (Minn. Stat. § 169.09, Subd. 9).

501.8.1 REPORT MODIFICATION

A change or modification of a written report that alters a material fact in the report may be made only by the member who prepared the report, and only prior to its approval and distribution. Once a report has been approved and distributed, corrections shall only be made by way of a written supplemental report. A written supplemental report may be made by any authorized member.

501.8.2 OPERATIONS COMMANDER RESPONSIBILITIES

The responsibilities of the Operations Commander include but are not limited to:

- (a) Ensuring the monthly and quarterly reports on traffic collision information and statistics are forwarded to the Patrol Division Commander or other persons as required.
- (b) Forwarding the traffic collision report to the Department of Public Safety within 10 days of the collision investigation (Minn. Stat. § 169.09, Subd. 8).
- (c) Ensuring the Department of Public Safety is notified within two business days of a collision that results in a fatality (Minn. Stat. § 169.09, Subd. 8).

Vehicle Towing

502.1 PURPOSE AND SCOPE

This policy provides the procedures for towing a vehicle by or at the direction of the South Saint Paul Police Department and under the authority of Minn. Stat. § 168B.035.

502.2 STORAGE AND IMPOUNDS

Vehicles may be towed for violations of Minn. Stat. § 168B.035, including parking, registration and snow emergency violations.

Vehicles may be moved or removed from a highway when in violation of Minn. Stat. § 169.32(a) or when left unattended upon any street or highway or upon any bridge or causeway or in any tunnel where such vehicle constitutes an obstruction to traffic (Minn. Stat. § 169.33).

The responsibilities of those employees storing or impounding a vehicle are as follows:

502.2.1 COMPLETION OF VEHICLE IMPOUND AND INVENTORY REPORT

Department members requesting towing of a vehicle shall complete a Vehicle Impound and Inventory Report, including a description of property within the vehicle. A copy is to be given to the tow truck operator and the original is to be submitted to the Records Section as soon as practicable after the vehicle is stored.

The Records Section shall promptly enter pertinent data from the completed Vehicle Impound and Inventory Report into the Minnesota Justice Information Services (MNJIS).

Approved Vehicle Impound and Inventory Report forms shall be promptly routed to the records section so that they are immediately available for release or for information, should inquiries be made.

Within 48 hours, excluding weekends and holidays, of the towing of any such vehicle, it shall be the responsibility of the towing vendor to determine through MNJIS the names and addresses of any individuals having an interest in the vehicle. Notice to all such individuals shall be sent by certified mail within five business days of impound (Minn. Stat. § 168B.06 Subd. 1).

502.2.2 REMOVAL OF VEHICLE DISABLED IN A TRAFFIC COLLISION

When a vehicle has been involved in a traffic collision and must be removed from the scene, the officer shall have the driver select a towing company, if reasonably possible and accomplished in a timely manner, and shall relay the request for the specified towing company to the dispatcher. When there is no preferred company requested, the Department's towing vendor will be used.

If the owner is incapacitated or for any reason it is necessary for the Department to assume responsibility for a vehicle involved in a collision, the officer shall request the dispatcher to call the Department's towing vendor. The officer will then conduct an inventory and store the vehicle using a Vehicle Impound and Inventory Report.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Towing

502.2.3 DRIVING A NON-CITY VEHICLE

Vehicles that have been towed by or at the direction of the Department should not be driven by police personnel unless it is necessary to move a vehicle a short distance to eliminate a hazard, prevent the obstruction of a fire hydrant or to comply with posted signs.

502.2.4 RECORDSBUREAU RESPONSIBILITIES

Records Section personnel shall promptly enter pertinent data from the completed Vehicle Impound and Inventory Report form into the stolen vehicle system. Approved forms shall be promptly filed so that they are immediately available for release or review should inquiries be made.

Within 48 hours of recovering a stolen vehicle or receiving notification that a vehicle reported stolen through this department has been recovered, the Records Section, or officer fielding the recovery call, shall make a reasonable and good faith effort to notify the victim of the recovery. The notice must specify when the recovering law enforcement agency expects to release the vehicle to the owner and where the owner may pick up the vehicle. Upon recovery of a vehicle reported stolen to another agency, the Records Section, or assigned officer, is to promptly inform the agency that the vehicle is recovered, where it is located and when it can be released to the owner (Minn. Stat. § 169.042 Subd. 1).

502.3 TOWING SERVICES

The City of South Saint Paul periodically selects one or more firms to act as official tow services and awards contracts to those firms. Those firms will be used in the following situations:

- (a) When it is necessary to safeguard a vehicle due to the inability of the owner or operator to take the required action.
- (b) When a vehicle is being held as evidence in connection with an investigation.
- (c) When it is otherwise necessary to store a motor vehicle. This would include situations involving the recovery of stolen or abandoned vehicles and the removal of vehicles obstructing traffic in violation of state or local regulations.

502.4 TOWING AT ARREST SCENES

Whenever a person in charge or in control of a vehicle is arrested, it is the policy of this department to provide reasonable safekeeping by towing the arrestee's vehicle subject to the exceptions described below. However, a vehicle shall be towed whenever it is needed for the furtherance of an investigation or prosecution of the case, or when the community caretaker doctrine would reasonably suggest that the vehicle should be towed. For example, the vehicle would present a traffic hazard if it were not removed, or the vehicle is located in a high-crime area and is susceptible to theft or damage if left at the scene.

502.5 VEHICLE INVENTORY

All property in a stored or impounded vehicle shall be inventoried and listed on the vehicle storage form. This includes the trunk and any compartments or containers, even if they are closed

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Towing

and/or locked. Members conducting inventory searches should be as thorough and accurate as practicable in preparing an itemized inventory. These inventory procedures are for the purpose of protecting an owner's property while the owner is in police custody, to provide for the safety of officers and the public, and to protect the Department against fraudulent claims of lost, stolen or damaged property.

502.6 PRESERVATION OF EVIDENCE

An officer who removes a vehicle pursuant to Minn. Stat. § 168B.035 is required to take reasonable and necessary steps to preserve evidence. If there is probable cause to believe that a vehicle or its contents constitute any evidence which tends to show that a criminal offense has been committed, or that a particular person has committed a criminal offense, officers shall ensure that all legally required and reasonably necessary efforts are taken to preserve the evidence. Such evidence is to be provided safe storage and preserved until released to the owner or otherwise disposed of according to law.

502.7 SECURITY OF VEHICLES AND PROPERTY

Unless it would cause an unreasonable delay in the completion of a vehicle impound/storage or create an issue of officer safety, officer should make reasonable accommodations to permit a driver/owner to retrieve small items of value or personal need (e.g., cash, jewelry, cellular telephone, prescriptions) that are not considered evidence or contraband.

If a search of a vehicle leaves the vehicle or any property contained therein vulnerable to unauthorized entry, theft or damage, personnel conducting the search shall take such steps as are reasonably necessary to secure and/or preserve the vehicle or property from such hazards.

Disabled Vehicles

503.1 PURPOSE AND SCOPE

Law enforcement and other public agencies may develop and adopt a written policy to provide assistance to motorists in disabled vehicles within their primary jurisdiction.

503.2 OFFICER RESPONSIBILITIES

When an on-duty officer observes a disabled vehicle on the roadway, the officer should make a reasonable effort to provide assistance. If that officer is assigned to a call of higher priority, the dispatcher should be advised of the location of the disabled vehicle and the need for assistance. The dispatcher should then assign another available officer to respond for assistance as soon as practicable.

503.3 EXTENT OF ASSISTANCE

In most cases, a disabled motorist will require assistance. After arrangements for assistance are made, continued involvement by Department personnel will be contingent on the time of day, the location, the availability of Department resources and the vulnerability of the disabled motorist.

503.3.1 MECHANICAL REPAIRS

Department personnel shall not make mechanical repairs to a disabled vehicle. The use of push bumpers to relocate vehicles to a position of safety is not considered a mechanical repair.

503.3.2 RELOCATION OF DISABLED VEHICLES

The relocation of disabled vehicles by members of this department by pushing or pulling a vehicle should only occur when the conditions reasonably indicate that immediate movement is necessary to reduce a hazard presented by the disabled vehicle.

Abandoned Vehicle Violations

504.1 PURPOSE AND SCOPE

This policy provides procedures for the removal, recording and storage of vehicles abandoned in violation of abandoned vehicle laws, under the authority of Minn. Stat. § 168B.04.

504.1.1 DEFINITION

Pursuant to Minnesota statutes, a vehicle is abandoned if:

- (a) The motor vehicle has remained illegally for more than 48 hours on any government-owned or -controlled property, or for more than four hours on that property when properly posted (Minn. Stat. § 168B.011 Subd. 2 (1)).
- (b) The motor vehicle has been properly tagged by an officer and abandoned for four hours on any highway (Minn. Stat. § 168B.04, Subd. 2 (b) (1)).
- (c) The motor vehicle has been abandoned and located so as to constitute a collision or traffic hazard (Minn. Stat. § 168B.04 Subd. 2 (b) (1)).
- (d) The motor vehicle is unattended on private residential property, that is a single-family or duplex, without permission of the property caretaker (Minn. Stat. § 168B.04 Subd. 2 (b) (2)).
- (e) The motor vehicle can be immediately removed if on private non-residential property if properly posted or after 24 hours if not posted (Minn. Stat. § 168B.04 Subd. 2 (b) (2)).
- (f) The motor vehicle remains at a service, repair or maintenance establishment of motor vehicles five days after notifying the vehicle owner by certified mail, return receipt requested, of the property owner's intention to have the vehicle removed from the property (Minn. Stat. § 168B.04 Subd. 2 (b) (2)).

504.2 MARKING VEHICLES

Vehicles on public roadways suspected of being abandoned in violation of Minnesota abandoned vehicle laws shall be marked and noted on the computer aided dispatch (CAD) system. No case number is required at this time.

A visible chalk, crayon or paint mark should be placed on the tire tread at the fender level unless the vehicle is missing tires or other vehicle conditions or weather prevent marking.

If a marked vehicle has been moved or the markings have been removed during a four or 24-hour investigation period, the vehicle shall be marked again for either the four or 24-hour abandonment violation and a CAD update completed.

504.2.1 VEHICLE STORAGE

Any vehicle in violation shall be impounded and stored by the authorized towing service and a vehicle impound report shall be completed by the officer authorizing the storage of the vehicle.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Abandoned Vehicle Violations

The impound report form shall be submitted to the Records Section immediately following the storage of the vehicle.

Chapter 6 - Investigation Operations

Investigation and Prosecution

600.1 PURPOSE AND SCOPE

When assigned to a case for initial or follow-up investigation, officers shall proceed with due diligence in evaluating and preparing the case for appropriate clearance or presentation to a prosecutor for filing criminal charges.

600.2 INITIAL INVESTIGATIONS

An officer responsible for an initial investigation shall complete no less than the following:

- (a) Make a preliminary determination if a crime has been committed by completing, at a minimum, the following:
 - 1. Obtain an initial statement from any witnesses or complainants.
 - 2. Conduct a cursory examination for possible evidence.
- (b) If information indicates a crime has occurred:
 - 1. Preserve the scene and any evidence as required to complete the initial and follow-up investigation.
 - 2. Determine if additional investigative resources (e.g., investigators or scene processing) assistance is necessary and request assistance as required.
 - 3. If assistance is warranted, or if the incident is not routine, notify a supervisor.
 - 4. Interview all available victims, informants, complainants, witnesses and suspects.
 - 5. Make reasonable attempts to locate, identify and interview all available victims, complainants, witnesses and suspects.
 - 6. Collect any evidence.
 - 7. Take any appropriate law enforcement action.
 - 8. Complete and submit the appropriate reports and documentation.
- (c) If the preliminary determination is that no crime occurred, determine what other action may be necessary, what other resources may be available and advise the informant or complainant of this information.

600.3 RECORDING OF CUSTODIAL INTERROGATIONS

Any custodial interrogation of a person who is suspected of having committed a criminal offense should be electronically recorded (audio/video or both as available) in its entirety, including any information or discussion about the person's rights and any waiver of those rights. Regardless of where the interrogation occurs, every reasonable effort should be made to secure functional recording equipment to accomplish such recordings.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Investigation and Prosecution

Officers should also consider electronically recording a custodial interrogation, or any investigative interview, for any offense when the officer reasonably believes it would be appropriate and beneficial to the investigation and is otherwise allowed by law.

No recording of an interrogation should be destroyed or altered without written authorization from the prosecuting attorney and the Investigation supervisor or pursuant to the Department records retention policy after closure of the case file. Copies of recorded interrogations or interviews may be made in the same or different format, provided they are true, accurate and complete copies and are made only for authorized and legitimate law enforcement purposes or otherwise authorized or required by law.

Officers should continue to prepare written summaries of custodial questioning and investigative interviews and continue to obtain written statements from suspects when applicable.

600.4 FOLLOW-UP INVESTIGATIONS

Follow-up investigations on all cases are evaluated and assigned by the Investigations supervisor for based upon caseload, case assignment and an evaluation of case solvability factors.

600.4.1 CASE SOLVABILITY FACTORS

Case solvability factors include, but are not limited to, the following:

- (a) Reliability of witnesses.
- (b) Suspect is named.
- (c) Suspect is described.
- (d) Suspect's location is known.
- (e) Suspect is identified.
- (f) Suspect has been previously seen.
- (g) Suspect vehicle is described.
- (h) Suspect vehicle is identified.
- (i) Property is traceable.
- (j) *Modus operandi* is significant.
- (k) There is usable physical evidence.
- (l) There was limited opportunity for anyone other than the suspect to commit the crime.
- (m) The case may be solved with reasonable additional investigative effort.
- (n) Other factors that are applicable only in exceptional circumstances:
 - 1. The case is of significant importance to the community.
 - 2. There is potential imminent danger to victims or witnesses.
 - 3. The seriousness of offense.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Investigation and Prosecution

4. There is a characteristic pattern, frequency or *modus operandi* related to the case.
5. Management decisions to pursue a case regardless of solvability factors.

600.5 MODIFICATION OF CHARGES FILED

Employees are not authorized to recommend to the prosecuting attorney, City Attorney or to any other official of the court that charges on a pending case be altered or the case dismissed. In all cases resulting in court prosecution, any request to modify the charges filed or to recommend dismissal of charges in a pending case shall be made to the prosecuting attorney's office or City Attorney's Office only as authorized by a Division Commander or the Chief of Police or designee.

600.6 TRAINING

Officers shall receive training in preliminary investigations prior to assignment to any investigative duties. Officers assigned to any follow-up or advanced investigations, or upon assignment to investigations, shall have completed training in follow-up investigations.

600.7 ELECTRONIC BENEFIT TRANSFER (EBT) CARDS

Officers shall make a report any time they arrest a person who possesses more than one welfare Electronic Benefit Transfer (EBT) card. The investigating officer shall forward this report to the Minnesota Department of Human Services within 30 days of the arrest. The report shall include all of the following (Minn. Stat. § 626.5533):

- (a) The name, address and driver's license or state identification card number of the suspect
- (b) The number on each EBT card and name, if any
- (c) The date and location of any alleged offense
- (d) Any other information the Minnesota Department of Human Services may require on related state forms

600.8 SCRAP METAL THEFT INVESTIGATION

The Investigations supervisor shall ensure the department complies with the implementation and use of the Automated Property System (APS) as well as the investigative requirements regarding scrap metal dealers (Minn. Stat. § 168; Minn. Stat. § 168A.1501; Minn. Stat. § 325E.21).

Sexual Assault Investigations

601.1 PURPOSE AND SCOPE

The South Saint Paul Police Department adopts the Investigations of Sexual Assault model policy established and published by the Minnesota Board of Peace Officer Standards and Training (MN POST) (Minn. Stat. § 626.8442).

See attachment: [Model Sexual Assault Investigation Policy 03-03-21.pdf](#)

601.2 INVESTIGATION CONSIDERATIONS

601.2.1 VICTIM CONFIDENTIALITY

Officers investigating or receiving a report of an alleged sex offense shall assist in keeping the identity of the victim private by providing the victim with Safe at Home Program information (Minn. R. 8290, et seq. and Minn. Stat. § 5B et seq.). A notation should be made within the incident report that the Safe at Home Program information was provided to the victim.

The Department shall withhold public access to information that would reveal the identity of a victim or alleged victim of criminal sexual conduct (Minn. Stat. § 13.82 Subd. 17 (b) and Minn. Stat. § 611A.021).

601.2.2 OFFICER RESPONSIBILITIES

Officers investigating or receiving a report of an alleged sex offense shall inform the victim of the following: (Minn. Stat. § 611A.02 Subd. 2 (b)):

- (a) Victims have the right to apply for reparations.
- (b) Victims have the right to request that the Department withhold public access to information that would reveal the victim's identity.
- (c) Victims have the right to be informed about the nearest crime victim assistance program or resource.
- (d) Victims have the right to be informed of and participate in the prosecution process if an offender is charged, including the right to request restitution.

Victims have the right should also receive the telephone number to call for a Safe at Home Program application form (Minn. Stat. § 611A.66).

601.3 MEDICAL EXAMINATION FOR SEXUAL ASSAULT VICTIMS

Officers investigating or receiving a report of an alleged sex offense that occurred within 96 hours of the offense shall, with the consent of the victim or a person authorized to act on behalf of the victim, request a medical examination of the victim.

If a sexual assault is not reported within 96 hours of the offense, the Department may still request a medical examination of the victim provided consent is given by the victim or a person authorized to act on behalf of the victim.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Sexual Assault Investigations

601.4 POLYGRAPH EXAMINATION

An officer may not require a sexual assault victim to submit to a polygraph examination as a condition to investigating, charging or prosecuting the offense (Minn. Stat. § 611A.26 Subd. 1 and Minn. Stat. § 611A.26 Subd. 5).

Officers may conduct a polygraph examination of a sexual assault victim only with the victim's written, informed consent and only after the victim has been referred to and had the opportunity to exercise the option of consulting with a sexual assault counselor (Minn. Stat. § 611A.26 Subd. 2 and Minn. Stat. § 611A.26 Subd. 3).

To consent to a polygraph, the officer must inform the victim in writing that (Minn. Stat. § 611A.26 Subd. 4):

- (a) The taking of a polygraph is voluntary and solely at the victim's request.
- (b) The victim may not be asked or required to submit to a polygraph examination.
- (c) The results of the examination are not admissible in court.
- (d) The victim's refusal to submit to a polygraph examination may not be used as a basis not to investigate, charge or prosecute the offender.

601.5 COPY OF SUMMARY

The Investigations supervisor shall ensure that the victim of a sexual assault who reports an incident to this department is provided with a copy of the written summary of the allegation. If the incident occurred outside the jurisdiction of the South Saint Paul Police Department, a copy of the written summary shall also be provided to the law enforcement agency where the incident occurred. If the South Saint Paul Police Department learns that both the victim and the accused are members of the Minnesota National Guard, the Department shall provide a copy of the summary to the Bureau of Criminal Apprehension (Minn. Stat. § 609.3459).

Asset Forfeiture

602.1 PURPOSE AND SCOPE

This policy describes the authority and procedure for the seizure, forfeiture and liquidation of property associated with specified designated offenses and controlled substance offenses (Minn. Stat. § 609.531 to Minn. Stat. § 609.5318).

602.2 POLICY

The South Saint Paul Police Department recognizes that appropriately applied forfeiture laws are helpful to enforce the law, deter crime and reduce the economic incentive of crime. However, the potential of revenue shall not be allowed to jeopardize the effective investigation and prosecution of criminal offenses, officer safety, the integrity of ongoing investigations or the due process rights of citizens.

It is the policy of the South Saint Paul Police Department that all employees of the agency, all employees assigned to another law enforcement agency's task force and all employees assigned to a task force from an outside law enforcement agency, in which this agency serves as the Fiscal Agent, follow all state and federal laws pertaining to forfeiture.

602.3 DEFINITIONS

Definitions related to this policy include:

Cash - Money in the form of bills or coins, traveler's checks, money orders, checks, or other forms of electronic money or stored value cards, including but not limited to gift cards, debit cards, gift cards/certificates, or other negotiable financial instruments.

Conveyance device - A device used for transportation. It includes but is not limited to a motor vehicle, trailer, snowmobile, airplane, and vessel, and any equipment attached to it. The term "conveyance device" does not include property which has been stolen or taken in violation of the law.

Firearms/ammunition/firearm accessories - A device that projects either single or multiple projectiles at high velocity. Ammunition is a term meaning the assembly of a projectile and its propellant. Accessories include but are not limited to holsters, gun cases, firearm optics, suppression devices, and cleaning supplies.

Fiscal Agent - The person designated by the South Saint Paul Police Department to be responsible for securing and maintaining seized assets and distributing any proceeds as a result of any forfeiture proceedings. This includes anytime the South Saint Paul Police Department seizes property for forfeiture or when the South Saint Paul Police Department is acting as the fiscal agent pursuant to a multi-agency agreement.

Forfeiture - The process by which legal ownership of an asset is transferred to a government or other authority.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Asset Forfeiture

Forfeiture Reviewer - The South Saint Paul Police Department employee assigned by the South Saint Paul Police Department responsible for reviewing all forfeiture cases and for acting as the liaison between the Department and the prosecutor's office.

Jewelry/precious metals/precious stones - The term includes items of jewelry, such as rings, necklaces, and watches that reasonably appear to be made of precious metals or precious stones. Precious metals include but are not limited to gold, silver, platinum, iridium, and palladium. Precious stones, often referred to as gemstones, include but are not limited to diamonds, emeralds, and rubies.

Property subject to administrative forfeiture - The following property is subject to administrative forfeiture under Minnesota Law (Minn. Stat. § 609.5314):

- (a) All cash totaling \$1500 or more, precious metals, and precious stones that there is probable cause to believe represent the proceeds of a controlled substance offense, and all cash found in proximity to controlled substances when there is probable cause to believe that the cash was exchanged for the purchase of a controlled substance.
- (b) All conveyance devices containing controlled substances with a retail value of \$100 or more if there is probable cause to believe that the conveyance device was used in the transportation or exchange of a controlled substance intended for distribution or sale.
- (c) All firearms, ammunition, and firearm accessories found:
 - 1. In a conveyance device used or intended for use to commit or facilitate the commission of a felony offense involving a controlled substance.
 - 2. On or in proximity to a person from whom a felony amount of controlled substance is seized.
 - 3. On the premises where a controlled substance is seized and in proximity to the controlled substance, if possession or sale of the controlled substance would be a felony under Minnesota Statutes, Chapter 152.

Seizure - The act of law enforcement officials taking property, including cash and conveyance devices that have been used in connection with or acquired by illegal activities.

602.4 ASSET SEIZURE

Property may be seized for forfeiture as provided in this policy.

602.4.1 PROPERTY SUBJECT TO SEIZURE

The following property is subject to seizure.

- (a) The following property may be seized upon review and approval of a supervisor and in coordination with the Forfeiture Reviewer:
 - 1. Controlled substances and associated property as described in Minn. Stat. § 609.5311.
 - 2. Property intended for use to commit or facilitate the commission of a designated offense, as listed in Minn. Stat. § 169A.63, Subd. 6 and limited by Minn. Stat. §

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Asset Forfeiture

169A.63, Subd. 7, and as listed in Minn. Stat. § 609.531, Subd. 1(f) and limited by Minn. Stat. § 609.5312.

- (b) Property subject to administrative forfeiture may be seized without prior supervisor approval if the item has a retail value of \$50,000 or less (Minn. Stat. § 609.5314).

602.4.2 PROPERTY NOT SUBJECT TO SEIZURE

The following property should not be seized for forfeiture:

- (a) Cash and property that does not meet the prosecuting agency's current minimum forfeiture thresholds.
- (b) Cash totaling less than \$1,500, unless prerecorded buy funds are included in the cash seized.

602.4.3 SEIZURE OF PROPERTY TO BE FORFEITED

An officer may seize property subject to forfeiture based on a court order. An officer may also seize property without a court order under any of the following conditions (Minn. Stat. § 609.531, Subd. 4; Minn. Stat. § 169A.63, Subd. 2):

- (a) The seizure is incident to a lawful arrest or a lawful search.
- (b) The property subject to seizure has been the subject of a prior judgment in favor of the state in a criminal injunction or forfeiture proceeding.
- (c) The officer has probable cause to believe that a delay to obtain a warrant or other process would result in the removal or destruction of the property and that either of the following apply:
 - 1. The property was used or is intended to be used in commission of a felony.
 - 2. The property is dangerous to health or safety.

602.5 PROCESSING SEIZED PROPERTY FOR FORFEITURE PROCEEDINGS

When property or cash subject to this policy is seized, the officer making the seizure should ensure compliance with the following:

- (a) If the retail value of the asset to be seized is \$50,000 or less, completely and accurately prepare the Notice of Seizure and Intent to Forfeit Property Form (seizure form) and present it to the person from whom the property is to be seized for that person's signature. If the person refuses to sign, the officer shall indicate on the seizure form that the person refused. The seizure form is not used when the value of the seized property exceeds \$50,000.
- (b) Prepare and provide a receipt for the items seized to the person from whom the property is being seized.
 - 1. If cash or property is seized from more than one person, a separate property inventory receipt must be completed for each person specifying the amount of cash seized. The receipt shall include a detailed description of all property, checks, money orders, traveler's checks or other financial instruments.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Asset Forfeiture

- (c) Complete and submit a report within 24 hours of the seizure if practicable. The report must include, at minimum, the following:
 - 1. A description of the items seized
 - 2. The location where the property was turned in or stored
 - 3. The name of the individual who was served with the seizure form
 - 4. The date that the seizure form was served
 - 5. The name of the officer making the seizure
 - 6. Whether the individual signed the seizure form
- (d) If property is seized from multiple individuals, a separate seizure form will be completed for each individual. A copy of the receipt and seizure form must be given to the individual from whom the property was seized.
- (e) When property is seized and no one claims possession of the property, the officer must leave a receipt in the place where the property was found if it is reasonably possible to do so.
- (f) The officer will book seized property into the Evidence Room as evidence, with the notation in the comment section of the property form, "Seized Subject to Forfeiture." Property seized subject to forfeiture should be booked on a separate property form. No other evidence from the case should be booked on this form.
- (g) Forward the original and the pink copy of the seizure form, and any seized property processing worksheets, property receipts and reports to the Forfeiture Reviewer within 10 days of seizure.
- (h) Inform the Forfeiture Reviewer of the estimated retail value of drugs found in proximity to the asset seized.

602.5.1 CASH HANDLING

It is the responsibility of the seizing officer to secure and count cash consistent with this policy and the Cash Handling, Security and Management Policy. All cash shall be counted in the presence of another officer and the envelope initialed by both officers. A supervisor shall be contacted for cash in excess of \$1,000. The supervisor shall also witness the count, and will initial and date the property documentation and specify any additional security procedures to be used.

All forfeitable cash seized will be turned over to the Forfeiture Reviewer or property/evidence room as soon as practicable.

Prior to deposit with the Forfeiture Reviewer, officers shall examine all cash seized to determine whether it contains any prerecorded buy funds. Officers shall document the recovery of all buy funds and deposit those funds with the Forfeiture Reviewer to be returned to the appropriate buy fund account.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Asset Forfeiture

602.5.2 JEWELRY/PRECIOUS METALS/PRECIOUS STONES

Officers seizing jewelry, precious metals and/or precious stones will write a detailed description of each item on the property inventory receipt. A copy of the property inventory receipt and any photographs of the jewelry, precious metals and/or precious stones shall be delivered to the Forfeiture Reviewer.

Officers seizing jewelry, precious metals and/or precious stones shall book those items according to current property and evidence procedures as soon as practicable.

602.5.3 VEHICLES

Any conveyance device seized for forfeiture shall be taken to a secure designated area or to a department-approved impound facility as soon as practicable.

Officers shall inventory the conveyance device and its contents in accordance with the Vehicle Towing Policy. Officers shall also complete applicable report forms and distribute them appropriately. A copy of the vehicle storage report shall be included with the seizure documentation that is submitted to the Forfeiture Reviewer.

602.5.4 FIREARMS/AMMUNITION/FIREARM ACCESSORIES

When firearms, ammunition or firearms accessories are seized, they shall be inventoried and delivered to the Evidence Room in accordance with the current booking procedures and the Property and Evidence Policy.

602.6 MAINTAINING SEIZED PROPERTY

The Evidence Room supervisor is responsible for ensuring compliance with the following:

- (a) All property received for forfeiture is reasonably secured and properly stored to prevent waste and preserve its condition (Minn. Stat. § 609.531 Subd. 5).
- (b) All property received for forfeiture is checked to determine if the property has been stolen.
- (c) All property received for forfeiture is retained in the same manner as evidence until forfeiture is finalized or returned to the claimant or person with an ownership interest.
- (d) Property received for forfeiture is not used unless the forfeiture action has been completed.

602.7 FORFEITURE REVIEWER

The Chief of Police will appoint an officer as the Forfeiture Reviewer. Prior to assuming duties, or as soon as practicable thereafter, the Forfeiture Reviewer should attend a department-approved course on asset forfeiture.

The responsibilities of Forfeiture Reviewer include the following:

- (a) Confer regularly with the prosecuting attorney's office to remain familiar with forfeiture laws, particularly Minn. Stat. § 609.531 through Minn. Stat. § 609.5318, Minn. Stat. § 169A.63, and the forfeiture policies of the prosecuting agency.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Asset Forfeiture

- (b) Make reasonable efforts to obtain annual training that includes best practices in pursuing, seizing, and tracking forfeitures.
- (c) Ensure responsibilities, including designation of a Fiscal Agent, are clearly established whenever multiple agencies are cooperating in a forfeiture case.
- (d) Ensure that a seizure form, property inventory receipt, and a forfeited property processing worksheet is available and appropriate for department use. The seizure form will minimally include the following (Minn. Stat. § 609.5314):
 - 1. Space for an itemized list of items seized
 - 2. The location and date of the seizure
 - 3. A place for the name of the individual served with the seizure form
 - 4. The date and signature of the officer conducting the seizure
 - 5. The agency case number
 - 6. A space for the signature of the person from whom property is seized or an appropriate space or check box for the officer to indicate that the person refused to sign
 - 7. At least an original and the pink copy
 - 8. Information in English, Hmong, Somali and Spanish explaining the right to obtain judicial review and the procedure provided by Minn. Stat. § 609.5314.
- (e) Ensure that officers who may be involved in asset forfeiture receive training in the proper use of the seizure form and the forfeiture process. The training should be developed in consultation with the prosecuting attorney and may be accomplished through traditional classroom education, electronic media, Daily Training Bulletins, or department directives. The training should be based on this policy and address any relevant statutory changes and court decisions.
- (f) Review each asset forfeiture case to ensure the following:
 - 1. Written documentation of the seizure and items seized is present in the case file.
 - 2. Independent prosecutorial review of the circumstances and propriety of the seizure is made in a timely manner.
 - 3. A timely notice of seizure has been given to interest holders of seized property.
 - 4. Property is promptly released to those entitled to its return.
- (g) Forward all changes to forfeiture status to any supervisor who initiates a forfeiture case.
- (h) Deposit any cash received with the Fiscal Agent.
- (i) Ensure the current minimum forfeiture thresholds are communicated appropriately to officers.
- (j) Annually review and update this policy and any related policies to reflect current federal and state statutes and case law.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Asset Forfeiture

- (k) Prepare a written plan for the Chief of Police to address any extended absence of the Forfeiture Reviewer to ensure that contact information for other law enforcement officers and attorneys who may assist in these matters is available.
- (l) Ensure the Department disposes of property as provided by law following any forfeiture (Minn. Stat. § 609.5315).
- (m) Ensure that any forfeited property used in an undercover capacity, or that is sold or added to the department inventory is done so according to Minnesota law.
- (n) Ensure that all forfeited property is used or disposed of in a manner consistent with the use and disposition of similar property by this department.
- (o) Upon completion of any forfeiture process, ensure that no property is retained by the South Saint Paul Police Department unless the South Saint Paul Police Department authorizes in writing the retention of the property for official use.
- (p) Ensure that forfeiture proceeds are maintained in a separate fund or account subject to appropriate accounting control with regular reviews or audits of all deposits and expenditures (Minn. Stat. § 609.5315).
- (q) Ensure that records of forfeiture are retained for a minimum of six years.
- (r) Ensure forfeiture reporting is made to the state auditor in the manner prescribed by the auditor (Minn. Stat. § 609.5315, Subd. 6).

602.8 DISPOSITION OF FORFEITED PROPERTY

Legal disposition may include (Minn. Stat. § 609.5315; Minn. Stat. § 169A.63, Subd. 10):

- (a) Retention by the Department and/or prosecuting agency.
 - 1. If a forfeited motor vehicle is kept for Department use, the Department will make a reasonable effort to ensure the vehicle is available for use and adaptation by officers who participate in the Department's Drug Abuse Resistance Education program (Minn. Stat. §609.5315).
- (b) Destruction.
- (c) Sale performed in a commercially reasonable manner.
- (d) Other disposition pursuant to applicable provisions of Minnesota Statutes.

No member of this department may use property that has been seized for forfeiture until the forfeiture action has been completed and the South Saint Paul Police Department has given written authorization to retain the property for official use.

Members of this department or persons related to members of this department by blood or marriage are prohibited from purchasing forfeited items sold by this department (Minn. Stat. § 609.5315, Subd. 1(c)).

Informants

603.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of informants.

603.1.1 DEFINITIONS

Definitions related to this policy include:

Informant - A person who covertly interacts with other individuals or suspects at the direction of, request of, or by agreement with the South Saint Paul Police Department for law enforcement purposes. This also includes a person agreeing to supply information to the South Saint Paul Police Department for a benefit (e.g., a quid pro quo in the form of a reduced criminal penalty, money).

603.2 POLICY

The South Saint Paul Police Department recognizes the value of informants to law enforcement efforts and will strive to protect the integrity of the informant process. It is the policy of this department that all funds related to informant payments will be routinely audited and that payments to informants will be made according to the criteria outlined in this policy.

603.2.1 POST MODEL POLICY

It is the policy of the Department to follow the requirements of the Confidential Informants Model Policy, established and published by the Minnesota Board of Peace Officer Standards and Training (MN POST) (Minn. Stat. § 626.8476).

[See attachment: Confidential Informants Model Policy.pdf](#)

603.3 USE OF INFORMANTS

603.3.1 INITIAL APPROVAL

Before using an individual as an informant, an officer must receive approval from his/her supervisor. The officer shall compile sufficient information through a background investigation and experience with the informant in order to determine the suitability of the individual, including age, maturity and risk of physical harm, as well as any indicators of his/her reliability and credibility.

Members of this department should not guarantee absolute safety or confidentiality to an informant.

603.3.2 JUVENILE INFORMANTS

The use of informants under the age of 13 is prohibited.

Juveniles under the guardianship of the state may not be used as informants.

In all cases, a juvenile 13 years of age or older may only be used as an informant with the written consent of each of the following:

- (a) The juvenile's parents or legal guardians

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Informants

- (b) The juvenile's attorney, if any
- (c) The court in which the juvenile's case is being handled, if applicable
- (d) The Chief of Police or the authorized designee

603.3.3 INFORMANT AGREEMENTS

All informants are required to sign and abide by the provisions of the designated department informant agreement. The officer using the informant shall discuss each of the provisions of the agreement with the informant.

Details of the agreement are to be approved in writing by a supervisor before being finalized with the informant.

603.4 INFORMANT INTEGRITY

To maintain the integrity of the informant process, the following must be adhered to:

- (a) The identity of an informant acting in a confidential capacity shall not be withheld from the Chief of Police, Division Commander, Dakota County Drug Task Force supervisor or their authorized designees.
 - 1. Identities of informants acting in a confidential capacity shall otherwise be kept confidential.
- (b) Criminal activity by informants shall not be condoned.
- (c) Informants shall be told they are not acting as police officers, employees or agents of the South Saint Paul Police Department, and that they shall not represent themselves as such.
- (d) The relationship between department members and informants shall always be ethical and professional.
 - 1. Members shall not become intimately involved with an informant.
 - 2. Social contact shall be avoided unless it is necessary to conduct an official investigation, and only with prior approval of the Dakota County Drug Task Force supervisor.
 - 3. Members shall neither solicit nor accept gratuities or engage in any private business transaction with an informant.
- (e) Officers shall not meet with informants in a private place unless accompanied by at least one additional officer or with prior approval of the Dakota County Drug Task Force supervisor.
 - 1. Officers may meet informants alone in an occupied public place, such as a restaurant.
- (f) When contacting informants for the purpose of making payments, officers shall arrange for the presence of another officer.
- (g) In all instances when department funds are paid to informants, a voucher shall be completed in advance, itemizing the expenses.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Informants

- (h) Since the decision rests with the appropriate prosecutor, officers shall not promise that the informant will receive any form of leniency or immunity from criminal prosecution.

603.4.1 UNSUITABLE INFORMANTS

The suitability of any informant should be considered before engaging him/her in any way in a covert or other investigative process. Members who become aware that an informant may be unsuitable will notify the supervisor, who will initiate a review to determine suitability. Until a determination has been made by a supervisor, the informant should not be used by any member. The supervisor shall determine whether the informant should be used by the Department and, if so, what conditions will be placed on his/her participation or any information the informant provides. The supervisor shall document the decision and conditions in file notes and mark the file "unsuitable" when appropriate.

Considerations for determining whether an informant is unsuitable include, but are not limited to, the following:

- (a) The informant has provided untruthful or unreliable information in the past.
- (b) The informant behaves in a way that may endanger the safety of an officer.
- (c) The informant reveals to suspects the identity of an officer or the existence of an investigation.
- (d) The informant appears to be using his/her affiliation with this department to further criminal objectives.
- (e) The informant creates officer-safety issues by providing information to multiple law enforcement agencies simultaneously, without prior notification and approval of each agency.
- (f) The informant engages in any other behavior that could jeopardize the safety of officers or the integrity of a criminal investigation.
- (g) The informant commits criminal acts subsequent to entering into an informant agreement.

603.5 INFORMANT FILES

Informant files shall be utilized as a source of background information about the informant, to enable review and evaluation of information provided by the informant, and to minimize incidents that could be used to question the integrity of department members or the reliability of the informant.

Informant files shall be maintained in a secure area within the Dakota County Drug Task Force. The Dakota County Drug Task Force supervisor or the authorized designee shall be responsible for maintaining informant files. Access to the informant files shall be restricted to the Chief of Police, Division Commander, Dakota County Drug Task Force supervisor or their authorized designees.

The Investigation Division Commander should arrange for an audit using a representative sample of randomly selected informant files on a periodic basis, but no less than one time per year. If the Dakota County Drug Task Force supervisor is replaced, the files will be audited before

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Informants

the new supervisor takes over management of the files. The purpose of the audit is to ensure compliance with file content and updating provisions of this policy. The audit should be conducted by a supervisor who does not have normal access to the informant files.

603.5.1 FILE SYSTEM PROCEDURE

A separate file shall be maintained on each informant and shall be coded with an assigned informant control number. An informant history that includes the following information shall be prepared for each file:

- (a) Name and aliases
- (b) Date of birth
- (c) Physical description: sex, race, height, weight, hair color, eye color, scars, tattoos, or other distinguishing features
- (d) Photograph
- (e) Current home address and telephone numbers
- (f) Current employers, positions, addresses, and telephone numbers
- (g) Vehicles owned and registration information
- (h) Places frequented
- (i) Briefs of information provided by the informant and the informant's subsequent reliability
 - 1. If an informant is determined to be unsuitable, the informant's file is to be marked "unsuitable" and notations included detailing the issues that caused this classification.
- (j) Name of the officer initiating use of the informant and any subsequent overseeing agents
- (k) Signed informant agreement
- (l) Update on active or inactive status of informant
- (m) Emergency contact information
- (n) Criminal history record
- (o) Residential addresses in the last five years
- (p) Social media accounts
- (q) Marital status and number of children
- (r) Gang affiliations or other organizational affiliations
- (s) Special skills and hobbies
- (t) Special areas of criminal expertise or knowledge

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Informants

603.6 INFORMANT PAYMENTS

No informant will be told in advance or given an exact amount or percentage for his/her service. The amount of funds to be paid to any informant will be evaluated against the following criteria:

- The extent of the informant's personal involvement in the case
- The significance, value or effect on crime
- The value of assets seized
- The quantity of the drugs or other contraband seized
- The informant's previous criminal activity
- The level of risk taken by the informant

The Dakota County Drug Task Force supervisor will discuss the above factors with the Patrol Division Commander and recommend the type and level of payment subject to approval by the Chief of Police.

603.6.1 REPORTING OF PAYMENTS

Each informant receiving a cash payment shall be advised of his/her responsibility to report the cash to the Internal Revenue Service (IRS) as income. If funds distributed exceed \$600 in any reporting year, the informant should be provided IRS Form 1099 (26 CFR 1.6041-1). If such documentation or reporting may reveal the identity of the informant and by doing so jeopardize any investigation, the safety of officers or the safety of the informant (26 CFR 1.6041-3), then IRS Form 1099 should not be issued.

In such cases, the informant shall be provided a letter identifying the amount he/she must report on a tax return as "other income" and shall be required to provide a signed acknowledgement of receipt of the letter. The completed acknowledgement form and a copy of the letter shall be retained in the informant's file.

603.6.2 PAYMENT PROCESS

Approved payments to an informant should be in cash using the following process:

- (a) Payments of \$500 and under may be paid in cash from a Dakota County Drug Task Force buy/expense fund.
 1. The Dakota County Drug Task Force supervisor shall sign the voucher for cash payouts from the buy/expense fund.
- (b) Payments exceeding \$500 shall be made by issuance of a check, payable to the officer who will be delivering the payment.
 1. The check shall list the case numbers related to and supporting the payment.
 2. A written statement of the informant's involvement in the case shall be placed in the informant's file.
 3. The statement shall be signed by the informant verifying the statement as a true summary of the informant's actions in the case.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Informants

4. Authorization signatures from the Chief of Police and the City Administrator are required for disbursement of the funds.
- (c) To complete the payment process for any amount, the officer delivering the payment shall complete a cash transfer form.
 1. The cash transfer form shall include the following:
 - (a) Date
 - (b) Payment amount
 - (c) South Saint Paul Police Department case number
 - (d) A statement that the informant is receiving funds in payment for information voluntarily rendered.
 2. The cash transfer form shall be signed by the informant.
 3. The cash transfer form will be kept in the informant's file.
 4. At least two officers should be present when payments are made.
 5. Any signature by the informant for receipt of payment should not contain the true identity of the informant but should use the informant's control number.

603.6.3 AUDIT OF PAYMENTS

The Dakota County Drug Task Force supervisor or the authorized designee shall be responsible for compliance with any audit requirements associated with grant provisions and applicable state and federal law.

At least once every six months, the Chief of Police or the authorized designee should conduct an audit of all informant funds for the purpose of accountability and security of the funds. The funds and related documents (e.g., buy/expense fund records, cash transfer forms, invoices, receipts and logs) will assist with the audit process.

603.7 TRAINING

The Support Services Commander shall provide in-service training to officers, including part-time officers, in the recruitment, control, and use of confidential informants as required by Minn. Stat. § 626.8476.

603.8 INFORMANT COORDINATOR

The Chief of Police or the authorized designee should designate an informant coordinator responsible for remaining familiar with the requirements and guidelines set forth in Minn. Stat. § 626.8476 and the MN POST Confidential Informants Model Policy.

The coordinator is also responsible for implementing department procedures and protocols concerning the recruitment, control, and use of informants, as adopted by the model policy, including but not limited to:

- (a) Establishing general guidelines related to the oversight of informants such as:
 1. The execution of informant agreements.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Informants

2. The use of informants in exigent circumstances.
 3. Supervisor review of informant files and informant agreements, and attendance at debriefings and meetings.
 4. Communication strategies and plans to address the confidentiality and integrity of the department/informant relationship.
 5. The screening of informants for personal safety or mental health concerns before and after their use.
- (b) Developing procedures for determining initial and continued suitability, and preparing related reports (e.g., Initial Suitability Report, Continuing Suitability Report).
1. Procedures should include a process for forwarding the results of initial and continuing suitability determinations to appropriate department members.
 2. The local prosecutor's office should be consulted before engaging individuals who require special review and approval (e.g., juveniles, government officials, those individuals obligated by legal privilege of confidentiality).
- (c) Creating a process for identifying individuals who may be or who may become unsuitable to serve as informants (e.g., individuals receiving in-patient or partial-hospitalization treatment for a substance use disorder or mental illness, participating in a treatment-based drug court program or treatment court, having overdosed in the last 12 months, having a physical or mental illness that impairs the ability to understand instructions and make informed decisions).
- (d) Working with department members to identify informants who should be referred to prevention or treatment services.
- (e) Addressing jurisdictional issues to ensure proper coordination in the use of informants.
- (f) Working with the Dakota County Drug Task Force supervisor to manage the informant file system, including establishing guidelines regarding access, review, and disclosure.
- (g) Establishing deactivation procedures.
- (h) Making any necessary updates to agency procedures.
- (i) Certifying annually to MN POST that the Department has adopted a policy that complies with the requirements of the model policy as required by Minn. Stat. § 626.8476, Subd. 3.

Eyewitness Identification

604.1 PURPOSE AND SCOPE

This policy sets forth guidelines to be used when members of this department employ eyewitness identification techniques (Minn. Stat. § 626.8433).

604.1.1 DEFINITIONS

Definitions related to the policy include:

Eyewitness identification process - Any field identification, live lineup or photographic identification.

Field identification - A live presentation of a single individual to a witness following the commission of a criminal offense for the purpose of identifying or eliminating the person as the suspect.

Live lineup - A live presentation of individuals to a witness for the purpose of identifying or eliminating an individual as the suspect.

Photographic lineup - Presentation of photographs to a witness for the purpose of identifying or eliminating an individual as the suspect.

604.2 POLICY

The South Saint Paul Police Department will strive to use eyewitness identification techniques, when appropriate, to enhance the investigative process and will emphasize identifying persons responsible for crime and exonerating the innocent.

604.2.1 POST MODEL POLICY

It is the policy of the South Saint Paul Police Department to follow the requirements of the Eyewitness Identification Procedures model policy, established and published by the Minnesota Board of Peace Officer Standards and Training (POST) (Minn. Stat. § 626.8433).

See attachment: [Eyewitness Identification Procedures model policy.pdf](#)

604.3 INTERPRETIVE SERVICES

Members should make a reasonable effort to arrange for an interpreter before proceeding with eyewitness identification if communication with a witness is impeded due to language or hearing barriers.

Before the interpreter is permitted to discuss any matter with the witness, the investigating officer should explain the identification process to the interpreter. Once it is determined that the interpreter comprehends the process and can explain it to the witness, the eyewitness identification may proceed as provided for within this policy.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Eyewitness Identification

604.4 EYEWITNESS IDENTIFICATION PROCESS AND FORM

The Investigations supervisor shall be responsible for the development and maintenance of an eyewitness identification process for use by members when they are conducting eyewitness identifications.

The process should include appropriate forms or reports that provide:

- (a) The date, time, and location of the eyewitness identification procedure.
- (b) The name and identifying information of the witness.
- (c) The name of the person administering the identification procedure.
- (d) If applicable, the names of all individuals present during the identification procedure.
- (e) An instruction to the witness that it is as important to exclude innocent persons as it is to identify a perpetrator.
- (f) An instruction to the witness that the perpetrator may or may not be among those presented and that the witness is not obligated to make an identification.
- (g) If the identification process is a photographic or live lineup, an instruction to the witness that the perpetrator may not appear exactly as he/she did on the date of the incident.
- (h) An instruction to the witness that the investigation will continue regardless of whether an identification is made by the witness.
- (i) A signature line where the witness acknowledges that he/she understands the identification procedures and instructions.
- (j) A statement from the witness in the witness's own words describing how certain he/she is of the identification or non-identification. This statement should be taken at the time of the identification procedure.
- (k) Any other direction to meet the requirements of the POST model policy.

The process and related forms should be reviewed at least annually and modified when necessary.

604.4.1 POST REQUIREMENTS

The Investigations supervisor should remain familiar with the requirements contained in the Eyewitness Identification Procedures model policy issued by POST and incorporate these, as necessary, into the eyewitness identification process for use by members when conducting photographic and live lineups.

604.5 EYEWITNESS IDENTIFICATION

Members are cautioned not to, in any way, influence a witness as to whether any subject or photo presented in a lineup is in any way connected to the case. Members should avoid mentioning that:

- The individual was apprehended near the crime scene.
- The evidence points to the individual as the suspect.
- Other witnesses have identified, or failed to identify, the individual as the suspect.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Eyewitness Identification

In order to avoid undue influence, witnesses should view suspects or a lineup individually and outside the presence of other witnesses. Witnesses should be instructed to avoid discussing details of the incident or of the identification process with other witnesses.

Whenever feasible, the eyewitness identification procedure should be audio and/or video recorded and the recording should be retained according to current evidence procedures.

604.5.1 PHOTOGRAPHIC AND LIVE LINEUP CONSIDERATIONS

When conducting a live lineup, the member presenting the lineup should not be involved in the investigation or know the identity of the suspect (Minn. Stat. § 626.8433).

When conducting a photographic lineup, if practicable, the member presenting the lineup should not be involved in the investigation of the case or know the identity of the suspect. In no case should the member presenting a lineup to a witness know which photograph or person in the lineup is being viewed by the witness.

Individuals in the lineup should reasonably match the description of the perpetrator provided by the witness and should bear similar characteristics to avoid causing any person to unreasonably stand out. In cases involving multiple suspects, a separate lineup should be conducted for each suspect. The suspects should be placed in a different order within each lineup.

The member presenting the lineup to a witness should do so sequentially (i.e., show the witness one person at a time) and not simultaneously. The witness should view all persons in the lineup.

A live lineup should only be used before criminal proceedings have been initiated against the suspect. If there is any question as to whether any criminal proceedings have begun, the investigating officer should contact the appropriate prosecuting attorney before proceeding.

604.5.2 FIELD IDENTIFICATION CONSIDERATIONS

Field identifications, also known as field elimination show-ups or one-on-one identifications, may be helpful in certain cases, where exigent circumstances make it impracticable to conduct a photo or live lineup identification. A field elimination show-up or one-on-one identification should not be used when independent probable cause exists to arrest a suspect. In such cases a live or photo lineup is the preferred course of action if eyewitness identification is contemplated.

When initiating a field identification, the member should observe the following guidelines:

- (a) Obtain and document a complete description of the suspect from the witness.
- (b) Assess whether a witness should be included in a field identification process by considering:
 - 1. The length of time the witness observed the suspect.
 - 2. The distance between the witness and the suspect.
 - 3. Whether the witness could view the suspect's face.
 - 4. The quality of the lighting when the suspect was observed by the witness.
 - 5. Whether there were distracting noises or activity during the observation.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Eyewitness Identification

6. Any other circumstances affecting the witness's opportunity to observe the suspect.
 7. The length of time that has elapsed since the witness observed the suspect.
- (c) If safe and practicable, the person who is the subject of the show-up should not be handcuffed or in a patrol vehicle.
 - (d) When feasible, members should bring the witness to the location of the subject of the show-up, rather than bring the subject of the show-up to the witness.
 - (e) The person who is the subject of the show-up should not be shown to the same witness more than once.
 - (f) In cases involving multiple suspects, witnesses should only be permitted to view the subjects of the show-up one at a time.
 - (g) The person who is the subject of the show-up should not be required to put on clothing worn by the suspect, to speak words uttered by the suspect, or to perform other actions mimicking those of the suspect.
 - (h) If a witness positively identifies a subject of the show-up as the suspect, members should not conduct any further field identifications with other witnesses for that suspect. In such instances members should document the contact information for any additional witnesses for follow up, if necessary.

604.6 DOCUMENTATION

A thorough description of the eyewitness process and the results of any eyewitness identification should be documented in the case report. Witness comments of how certain he/she is of the identification or non-identification should be quoted in the report.

If a photographic lineup is utilized, a copy of the photographic lineup presented to the witness should be included in the case report. In addition, the order in which the photographs were presented to the witness should be documented in the case report.

604.6.1 DOCUMENTATION RELATED TO RECORDINGS

The member conducting the lineup should document the reason that an audio and/or video recording was not obtained, if applicable.

Brady Material Disclosure

605.1 PURPOSE AND SCOPE

This policy establishes guidelines for identifying and releasing potentially exculpatory or impeachment information (so-called “*Brady* information”) to a prosecuting attorney.

605.1.1 DEFINITIONS

Definitions related to this policy include:

Brady information - Information known or possessed by the South Saint Paul Police Department that is both favorable and material to the current prosecution or defense of a criminal defendant.

605.2 POLICY

The South Saint Paul Police Department will conduct fair and impartial criminal investigations and will provide the prosecution with both incriminating and exculpatory evidence as well as information that may adversely affect the credibility of a witness. In addition to reporting all evidence of guilt, the South Saint Paul Police Department will assist the prosecution by complying with its obligation to disclose information that is both favorable and material to the defense. The Department will identify and disclose to the prosecution potentially exculpatory information as provided in this policy.

605.3 DISCLOSURE OF INVESTIGATIVE INFORMATION

Officers must include in their investigative reports adequate investigative information and reference to all material evidence and facts that are reasonably believed to be either incriminating or exculpatory to any individual in the case. If an officer learns of potentially incriminating or exculpatory information any time after submission of a case, the officer or the handling investigator must prepare and submit a supplemental report documenting such information as soon as practicable. Supplemental reports shall be promptly processed and transmitted to the prosecutor’s office.

If information is believed to be privileged or confidential (e.g., informant or attorney-client information, attorney work product), the officer should discuss the matter with a supervisor and/or prosecutor to determine the appropriate manner in which to proceed.

Evidence or facts are considered material if there is a reasonable probability that they would affect the outcome of a criminal proceeding or trial. Determining whether evidence or facts are material often requires legal or even judicial review. If an officer is unsure whether evidence or facts are material, the officer should address the issue with a supervisor.

Supervisors who are uncertain about whether evidence or facts are material should address the issue in a written memo to an appropriate prosecutor. A copy of the memo should be retained in the Department case file.

605.4 DISCLOSURE OF REQUESTED INFORMATION

If *Brady* information is located, the following procedure shall apply:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Brady Material Disclosure

- (a) In the event that a motion has not already been filed by the criminal defendant or other party, the prosecuting attorney and department member shall be notified of the potential presence of *Brady* material in the member's personnel file.
- (b) The prosecuting attorney or City Attorney should then be requested to file a motion in order to initiate an in-camera review by the court.
 - 1. If no motion is filed, the Custodian of Records should work with the appropriate counsel to determine whether the records should be disclosed to the prosecutor.
- (c) The Custodian of Records shall accompany all relevant personnel files during any in-camera inspection to address any issues or questions raised by the court.
- (d) If the court determines that there is relevant *Brady* material contained in the files, only that data ordered released will be copied and released to the parties filing the motion.
 - 1. Prior to the release of any materials pursuant to this process, the Custodian of Records should request a protective order from the court limiting the use and further dissemination of such materials to the involved case and requiring the return of all copies upon completion of the case.
- (e) If a court has determined that relevant *Brady* information is contained in the member's file in any case, the prosecutor should be notified of that fact in all future cases involving that member.

605.5 INVESTIGATING BRADY ISSUES

If the Department receives information from any source that a member may have issues of credibility, dishonesty or has been engaged in an act of moral turpitude or criminal conduct, the information shall be investigated and processed in accordance with the Personnel Complaints Policy.

605.6 TRAINING

Department personnel should receive periodic training on the requirements of this policy.

605.7 BRADY PROCESS

The Chief of Police shall select a member of the Department to coordinate requests for *Brady* information. This person shall be directly responsible to the Administration Division Commander or the authorized designee.

The responsibilities of the coordinator include but are not limited to:

- (a) Working with the appropriate prosecutors' offices and the City Attorney's office to establish systems and processes to determine what constitutes *Brady* information and the method for notification and disclosure.
- (b) Maintaining a current list of members who have *Brady* information in their files or backgrounds.
 - 1. Updating this list whenever potential *Brady* information concerning any department member becomes known to the Department or is placed into a personnel or internal affairs file.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Brady Material Disclosure

605.8 SUBPOENA PROCESSING

The individual processing subpoenas (or the supervisor of the subpoenaed member) shall check the subpoenaed member's name against the current list of those who are known to have *Brady* information in their files or background, and shall alert the coordinator if a person on the list is subpoenaed.

Chapter 7 - Equipment

Department-Owned and Personal Property

700.1 PURPOSE AND SCOPE

Department employees are expected to properly care for Department property assigned or entrusted to them. Employees may also suffer occasional loss or damage to personal or department property while performing their assigned duties. Certain procedures are required depending on the loss and ownership of the item.

700.2 DOCUMENTATION OF ISSUED PROPERTY

All property issued shall be documented in the appropriate property sheet or equipment log and receipt acknowledged by signature. Upon an employee's separation from the Department, all issued equipment shall be returned and documentation of the return signed by a supervisor.

700.2.1 CARE OF DEPARTMENT PROPERTY

Employees shall be responsible for the safekeeping, serviceable condition, proper care, use and replacement of department property assigned or entrusted to them. An employee's intentional or negligent abuse or misuse of department property may lead to discipline including, but not limited to, the cost of repair or replacement.

- (a) Employees shall promptly report through the chain of command, any loss, damage to or unserviceable condition of any department-issued property or equipment assigned for their use.
 - 1. A supervisor receiving such a report shall make an appropriate investigation and direct a memo to the appropriate Division Commander that shall include the result of his/her investigation and whether the employee followed proper procedures. The supervisor's report shall address whether reasonable care was taken to prevent the loss, damage or unserviceable condition.
 - 2. A review by Staff to determine whether misconduct or negligence was involved should be completed.
- (b) The use of damaged or unserviceable department property should be discontinued as soon as practicable and, if appropriate and approved by staff, replaced with comparable Department property as soon as available and following notice to a supervisor.
- (c) Except when otherwise directed by competent authority or required by exigent circumstances, Department property shall only be used by those to whom it was assigned. Use should be limited to official purposes and in the capacity for which it was designed.
- (d) Department property shall not be thrown away, sold, traded, donated, destroyed or otherwise disposed of without proper authority.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Department-Owned and Personal Property

- (e) In the event that any Department property becomes damaged or unserviceable, no employee shall attempt to repair the property without prior approval of a supervisor.

700.3 LOSS OR DAMAGE OF PROPERTY OF ANOTHER

Officers and other employees intentionally or unintentionally may cause damage to the real or personal property of another while performing their duties. Any employee who damages or causes to be damaged any real or personal property of another while performing any law enforcement function shall report it as provided below.

- (a) A verbal report shall be made to the employee's immediate supervisor as reasonably soon as circumstances permit.
- (b) A written report shall be submitted before the employee goes off-duty or within the time frame directed by the supervisor to whom the verbal report was made.

700.3.1 DAMAGE BY PERSON OF ANOTHER AGENCY

If employees of another jurisdiction cause damage to personal property or property belonging to the City, it shall be the responsibility of the employee present or the employee responsible for the property to make a verbal report to his/her immediate supervisor as reasonably soon as circumstances permit. The employee shall submit a written report before going off-duty or as otherwise directed by the supervisor.

These written reports, accompanied by the supervisor's written report, shall promptly be forwarded to the appropriate Division Commander.

Personal Communication Devices

701.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of mobile telephones and communication devices, whether issued or funded by the Department or personally owned, while on-duty or when used for authorized work-related purposes.

This policy generically refers to all such devices as Personal Communication Devices (PCDs) but is intended to include all mobile telephones, personal digital assistants (PDAs), wireless-capable tablets, and similar wireless two-way communications and/or portable internet-access devices. PCD use includes but is not limited to placing and receiving calls, text messaging, blogging and microblogging, emailing, using video or camera features, playing games, and accessing sites or services on the internet.

701.2 POLICY

The South Saint Paul Police Department allows members to utilize department-issued or funded PCDs and to possess personally owned PCDs in the workplace, subject to certain limitations. Any PCD used while on- or off-duty for business-related purposes, or reasonably associated with work-related misconduct, will be subject to monitoring and inspection consistent with applicable law and this policy.

Additionally, the use of a PCD either on-duty or after duty hours for business-related purposes, or reasonably associated with work-related misconduct, may subject the member and the member's PCD records to civil or criminal discovery or disclosure under applicable data practices laws and rules of civil or criminal procedures.

Members who have questions regarding the application of this policy or the guidelines contained herein are encouraged to seek clarification from supervisory staff.

701.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to any communication accessed, transmitted, received, or reviewed on any PCD issued or funded by the Department and shall have no expectation of privacy in their location should the device be equipped with location-detection capabilities. This includes records of all keystrokes or web-browsing history made on the PCD. The fact that access to a database, service, or website requires a username or password will not create an expectation of privacy if it is accessed through department PCDs or networks (see the Information Technology Use Policy for additional guidance).

Members have no expectation of privacy regarding any communications while using a personally owned PCD for department-related business or when the use reasonably implicates work-related misconduct.

701.4 DEPARTMENT-ISSUED PCD

Depending on a member's assignment and the needs of the position, the Department may, at its discretion, issue or fund a PCD for the member's use to facilitate on-duty performance.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Communication Devices

Department-issued or funded PCDs may not be used for personal business either on- or off-duty unless authorized by the Chief of Police or the authorized designee. Such devices and the associated telephone number, if any, shall remain the sole property of the Department and shall be subject to inspection or monitoring (including all related records and content) at any time without notice and without cause.

701.5 PERSONALLY OWNED PCD

Members may carry a personally owned PCD while on-duty, subject to the following conditions and limitations:

- (a) Permission to carry a personally owned PCD may be revoked if it is used contrary to provisions of this policy.
- (b) The Department accepts no responsibility for loss of or damage to a personally owned PCD.
- (c) The PCD and any associated services shall be purchased, used, and maintained solely at the member's expense.
- (d) The device should not be used for work-related purposes except in exigent circumstances (e.g., unavailability of radio communications) or as otherwise authorized by department procedures.
 - 1. Use of a personally owned PCD for work-related business constitutes consent for the Department to access the PCD to inspect and copy the work-related data (e.g., for litigation purposes, public records retention and release obligations, internal investigations).
 - 2. Use of and data within a personally owned PCD may be discoverable in cases when there is reason to believe it is associated with work-related misconduct.
 - 3. Searches of a personally owned PCD by the Department should be limited to those matters reasonably associated with the work-related business or work-related misconduct.
- (e) The device shall not be utilized to record or disclose any department business-related information, including photographs, video, or the recording or transmittal of any information or material obtained or made accessible as a result of employment or appointment with the Department, without the express authorization of the Chief of Police or the authorized designee.
- (f) If the PCD is carried on-duty, members will provide the Department with the telephone number of the device.
- (g) All work-related documents, emails, photographs, recordings, and other public records created or received on a member's personally owned PCD should be transferred to the South Saint Paul Police Department and deleted from the member's PCD as soon as reasonably practicable but no later than the end of the member's shift.

Except with prior express authorization from their supervisors, members are not obligated or required to carry, access, monitor, or respond to electronic communications using a personally owned PCD while off-duty. If a member is in an authorized status that allows for appropriate

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Communication Devices

compensation consistent with policy or existing collective bargaining agreements, or if the member has prior express authorization from their supervisor, the member may engage in department business-related communications. Should members engage in such approved off-duty communications or work, members entitled to compensation shall promptly document the time worked and communicate the information to their supervisors to ensure appropriate compensation. Members who independently document off-duty department-related business activities in any manner shall promptly provide the Department with a copy of such records to ensure accurate recordkeeping.

701.5.1 PUBLIC RECORDS

Work related information including data created, received, recorded or stored on a personally owned PCD in the course of department duties is considered government data subject to the requirements of the Minnesota Government Data Practices Act and discovery obligations (Minn. Stat. § 13.01 et seq.).

701.6 USE OF PCD

The following protocols shall apply to all PCDs that are carried while on-duty or used to conduct department business:

- (a) A PCD shall not be carried in a manner that allows it to be visible while in uniform unless it is in an approved carrier.
- (b) All PCDs in the workplace shall be set to silent or vibrate mode.
- (c) A PCD may not be used to conduct personal business while on-duty except for brief personal communications (e.g., informing family of extended hours). Members shall endeavor to limit their use of PCDs to authorized break times unless an emergency exists.
- (d) Members may use a PCD to communicate with other personnel in situations where the use of radio communications is either impracticable or not feasible. PCDs should not be used as a substitute for, as a way to avoid, or in lieu of regular radio communications.
- (e) Members are prohibited from taking pictures, audio or video recordings, or making copies of any such picture or recording media unless it is directly related to official department business. Disclosure of any such information to any third party through any means requires the express authorization of the Chief of Police or the authorized designee.
- (f) Members will not access social networking sites for any purpose that is not official department business. This restriction does not apply to a personally owned PCD used during authorized break times.
- (g) Using PCDs to harass, threaten, coerce, or otherwise engage in inappropriate conduct with any third party is prohibited. Any member having knowledge of such conduct shall promptly notify a supervisor.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Communication Devices

701.7 SUPERVISOR RESPONSIBILITIES

The responsibilities of supervisors include but are not limited to:

- (a) Ensuring that members under their command are provided appropriate training on the use of PCDs consistent with this policy.
- (b) Monitoring, to the extent practicable, PCD use in the workplace and taking prompt corrective action if a member is observed or reported to be improperly using a PCD.
 - 1. An investigation into improper conduct should be promptly initiated when circumstances warrant.
 - 2. Before conducting any administrative search of a member's personally owned device, supervisors should consult with the Chief of Police or the authorized designee.

701.8 USE WHILE DRIVING

The use of a PCD while driving can adversely affect safety, cause unnecessary distractions, and present a negative image to the public. Officers operating emergency vehicles should restrict the use of these devices to matters involving official duties and, where practicable, stop the vehicle at an appropriate location to use the PCD (Minn. Stat. § 169.475).

Except in an emergency, members who are operating non-emergency vehicles shall not use a PCD while driving unless the device is specifically designed and configured to allow hands-free use (Minn. Stat. § 169.475). Hands-free use should be restricted to business-related calls or calls of an urgent nature.

701.9 OFFICIAL USE

Members are reminded that PCDs are not secure devices and conversations may be intercepted or overheard. Caution should be exercised while utilizing PCDs to ensure that sensitive information is not inadvertently transmitted. As soon as reasonably possible, members shall conduct sensitive or private communications on a land-based or other department communications network.

Vehicle Maintenance

702.1 PURPOSE AND SCOPE

Employees are responsible for assisting in maintaining Department vehicles so that they are properly equipped, maintained, refueled and present a clean appearance.

702.2 DEFECTIVE VEHICLES

When a department vehicle becomes inoperative or in need of repair that affects the safety of the vehicle, that vehicle shall be removed from service for repair. Proper documentation shall be promptly completed by the employee who becomes aware of the defective condition. Paperwork, describing the correction needed, shall be promptly forwarded to vehicle maintenance for repair.

702.2.1 SUSPECTED DAMAGE OR POOR PERFORMANCE

Vehicles that may have suffered damage, perform poorly or whose control or safety features has been diminished shall be immediately removed from service for inspection and repair.

702.2.2 SEVERE USE INSPECTION

Vehicles operated under severe use conditions, including rough roadway or off-road operation, hard or extended braking, pursuits or prolonged high-speed operation, should be removed from service and subjected to a safety inspection as soon as reasonably possible.

702.3 VEHICLE EQUIPMENT

Certain items shall be maintained in all Department vehicles for emergency purposes and to perform routine duties.

702.3.1 PATROL VEHICLES

Officers shall inspect the patrol vehicle at the beginning of the shift and ensure that the following equipment, at a minimum, is present in the vehicle:

- Emergency road flares
- Crime scene barricade tape
- First aid kit, CPR mask, and other medical supplies
- Blanket
- Fire extinguisher
- Blood borne pathogen kit, including all personal protective equipment
- Sharps container
- Hazardous waste disposal bag
- Traffic safety vest
- 1 hazardous materials emergency response handbook

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Maintenance

- Evidence collection items to include: bags, boxes, markers etc.
- 1 camera
- Portable Breath Test apparatus

702.3.2 UNMARKED VEHICLES

An employee driving an unmarked department vehicle shall ensure that, at minimum, the equipment listed below is present in the vehicle:

- Crime scene barricade tape
- First aid kit, CPR mask and other medical supplies
- Blanket
- Blood borne pathogen kit, including personal protective equipment
- Sharps container
- Hazardous waste disposal bag
- Traffic safety vest
- Hazardous materials emergency response handbook
- Evidence collection kit
- Camera

702.4 VEHICLE REFUELING

Absent emergency conditions or supervisor approval, officers driving department vehicles shall not place a vehicle in service that has less than one-quarter tank of fuel. Whenever practicable, vehicles should be fully fueled when placed into service and refueled before the level falls below one-quarter tank.

702.5 WASHING OF VEHICLES

All units shall be kept clean at all times and, weather conditions permitting, shall be washed as necessary to enhance their appearance.

Employees using a vehicle shall remove any trash or debris at the end of the shift. No public data should be placed in a designated receptacle provided for the shredding of this matter.

702.6 CIVILIAN EMPLOYEE USE

Civilian employees shall not operate the emergency lights or siren of any vehicle unless expressly authorized by a supervisor.

Vehicle Use

703.1 PURPOSE AND SCOPE

The purpose of this policy is to establish a system of accountability to ensure department vehicles are used appropriately. This policy provides guidelines for on- and off-duty use of department vehicles and shall not be construed to create or imply any contractual obligation by the City of South Saint Paul to provide assigned take-home vehicles.

Additional guidelines for member responsibilities when transporting persons in custody may be found in the Transporting Persons in Custody Policy.

703.2 POLICY

The South Saint Paul Police Department provides vehicles for department-related business and may assign patrol and unmarked vehicles based on a determination of operational efficiency, economic impact to the Department, requirements for tactical deployments and other considerations.

703.3 USE OF VEHICLES

703.3.1 SHIFT ASSIGNED VEHICLES

The Sergeant shall ensure a copy of the shift assignment roster, indicating member assignments and vehicle numbers, is completed for each shift and retained in accordance with the established records retention schedule. If a member exchanges vehicles during his/her shift, the new vehicle number shall be documented on the roster.

703.3.2 OTHER USE OF VEHICLES

Members utilizing a vehicle for any purpose other than their normally assigned duties or normal vehicle assignment (e.g., transportation to training, community event) shall first notify the Sergeant. A notation will be made on the shift assignment roster indicating the member's name and vehicle number.

This subsection does not apply to those who are assigned to transport vehicles to and from the maintenance yard or car wash.

703.3.3 INSPECTIONS

Members shall be responsible for inspecting the interior and exterior of any assigned vehicle before taking the vehicle into service and at the conclusion of their shifts. Any previously unreported damage, mechanical problems, unauthorized contents, or other problems with the vehicle shall be promptly reported to a supervisor and documented as appropriate.

The interior of any vehicle that has been used to transport any person other than a member of this department should be inspected prior to placing another person in the vehicle and again after the person is removed. This is to ensure that unauthorized or personal items have not been left in the vehicle.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Use

All department vehicles are subject to inspection and/or search at any time by a supervisor without notice and without cause. No member assigned to or operating such vehicle shall be entitled to any expectation of privacy with respect to the vehicle or its contents.

703.3.4 SECURITY AND UNATTENDED VEHICLES

Unattended vehicles should be locked and secured at all times. No key should be left in the vehicle except when it is necessary that the vehicle be left running (e.g., continued activation of emergency lights, canine safety, equipment charging). Officers who exit a vehicle rapidly in an emergency situation or to engage in a foot pursuit must carefully balance the need to exit the vehicle quickly with the need to secure the vehicle.

Members shall ensure all weapons are secured while the vehicle is unattended.

703.3.5 MOBILE DIGITAL COMPUTER

Members assigned to vehicles equipped with a Mobile Digital Computer (MDC) shall log onto the MDC with the required information when going on-duty. If the vehicle is not equipped with a working MDC, the member shall notify Dispatch. Use of the MDC is governed by the Mobile Digital Computer Use Policy.

703.3.6 VEHICLE LOCATION SYSTEM

Patrol and other vehicles, at the discretion of the Chief of Police, may be equipped with a system designed to track the vehicle's location. While the system may provide vehicle location and other information, members are not relieved of their responsibility to use required communication practices to report their location and status.

Members shall not make any unauthorized modifications to the system. At the start of each shift, members shall verify that the system is on and report any malfunctions to their supervisor. If the member finds that the system is not functioning properly at any time during the shift, he/she should exchange the vehicle for one with a working system, if available.

System data may be accessed by supervisors at any time. However, access to historical data by personnel other than supervisors will require Division Commander approval.

All data captured by the system shall be retained in accordance with the established records retention schedule.

703.3.7 KEYS

Members approved to operate marked patrol vehicles should be issued a copy of the key as part of their initial equipment distribution. Members who are assigned a specific vehicle should be issued keys for that vehicle.

Members shall not duplicate keys. The loss of a key shall be promptly reported in writing through the member's chain of command.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Use

703.3.8 AUTHORIZED PASSENGERS

Members operating department vehicles shall not permit persons other than City personnel or persons required to be conveyed in the performance of duty, or as otherwise authorized, to ride as passengers in the vehicle, except as stated in the Ride-Along Policy.

703.3.9 ALCOHOL

Members who have consumed alcohol are prohibited from operating any department vehicle unless it is required by the duty assignment (e.g., task force, undercover work). Regardless of assignment, members may not violate state law regarding vehicle operation while intoxicated.

703.3.10 PARKING

Except when responding to an emergency or when urgent department-related business requires otherwise, members driving department vehicles should obey all parking regulations at all times.

Department vehicles should be parked in assigned stalls. Members shall not park privately owned vehicles in stalls assigned to department vehicles or in other areas of the parking lot that are not so designated unless authorized by a supervisor. Privately owned motorcycles shall be parked in designated areas.

703.3.11 ACCESSORIES AND/OR MODIFICATIONS

There shall be no modifications, additions or removal of any equipment or accessories without written permission from the assigned vehicle program manager.

703.3.12 CIVILIAN MEMBER USE

Civilian members using marked emergency vehicles shall ensure that all weapons have been removed before going into service. Civilian members shall prominently display the "out of service" placards or light bar covers at all times. Civilian members shall not operate the emergency lights or siren of any vehicle unless expressly authorized by a supervisor.

703.4 INDIVIDUAL MEMBER ASSIGNMENT TO VEHICLES

Department vehicles may be assigned to individual members at the discretion of the Chief of Police. Vehicles may be assigned for on-duty and/or take-home use. Assigned vehicles may be changed at any time. Permission to take home a vehicle may be withdrawn at any time.

The assignment of vehicles may be suspended when the member is unable to perform his/her regular assignment.

703.4.1 ON-DUTY USE

Vehicle assignments shall be based on the nature of the member's duties, job description and essential functions, and employment or appointment status. Vehicles may be reassigned or utilized by other department members at the discretion of the Chief of Police or the authorized designee.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Use

703.4.2 UNSCHEDULED TAKE-HOME USE

Circumstances may arise where department vehicles must be used by members to commute to and from a work assignment. Members may take home department vehicles only with prior approval of a supervisor and shall meet the following criteria:

- (a) The circumstances are unplanned and were created by the needs of the Department.
- (b) Other reasonable transportation options are not available.
- (c) The member lives within a reasonable distance (generally not to exceed a 60-minute drive time) of the South Saint Paul City limits.
- (d) Off-street parking will be available at the member's residence.
- (e) Vehicles will be locked when not attended.
- (f) All firearms, weapons and control devices will be removed from the interior of the vehicle and properly secured in the residence when the vehicle is not attended, unless the vehicle is parked in a locked garage.

703.4.3 ASSIGNED VEHICLES

Assignment of take-home vehicles shall be based on the location of the member's residence; the nature of the member's duties, job description and essential functions; and the member's employment or appointment status. Residence in the City of South Saint Paul is a prime consideration for assignment of a take-home vehicle. Members who reside outside the City of South Saint Paul may be required to secure the vehicle at a designated location or the Department at the discretion of the Chief of Police.

Members are cautioned that under federal and local tax rules, personal use of a City vehicle may create an income tax liability for the member. Questions regarding tax rules should be directed to the member's tax adviser.

Criteria for use of take-home vehicles include the following:

- (a) Vehicles shall only be used for work-related purposes and shall not be used for personal errands or transports, unless special circumstances exist and the Chief of Police or a Division Commander gives authorization.
- (b) Vehicles may be used to transport the member to and from the member's residence for work-related purposes.
- (c) Vehicles will not be used when off-duty except:
 - 1. In circumstances when a member has been placed on call by the Chief of Police or Division Commanders and there is a high probability that the member will be called back to duty.
 - 2. When the member is performing a work-related function during what normally would be an off-duty period, including vehicle maintenance or traveling to or from a work-related activity or function.
 - 3. When the member has received permission from the Chief of Police or Division Commanders.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Use

4. When the vehicle is being used by the Chief of Police, Division Commanders or members who are in on-call administrative positions.
5. When the vehicle is being used by on-call investigators.
- (d) While operating the vehicle, authorized members will carry and have accessible their duty firearms and be prepared to perform any function they would be expected to perform while on-duty.
- (e) The two-way communications radio, MDC and global positioning satellite device, if equipped, must be on and set to an audible volume when the vehicle is in operation.
- (f) Unattended vehicles are to be locked and secured at all times.
 1. No key should be left in the vehicle except when it is necessary that the vehicle be left running (e.g., continued activation of emergency lights, canine safety, equipment charging).
 2. All weapons shall be secured while the vehicle is unattended.
 3. All department identification, portable radios and equipment should be secured.
- (g) Vehicles are to be parked off-street at the member's residence unless prior arrangements have been made with the Chief of Police or the authorized designee. If the vehicle is not secured inside a locked garage, all firearms and kinetic impact weapons shall be removed and properly secured in the residence (see the Firearms Policy regarding safe storage of firearms at home).
- (h) Vehicles are to be secured at the member's residence or the appropriate department facility, at the discretion of the Department when a member will be away (e.g., on vacation) for periods exceeding one week.
 1. If the vehicle remains at the residence of the member, the Department shall have access to the vehicle.
 2. If the member is unable to provide access to the vehicle, it shall be parked at the Department.
- (i) The member is responsible for the care and maintenance of the vehicle.

703.4.4 ENFORCEMENT ACTIONS

When driving a take-home vehicle to and from work outside of the jurisdiction of the South Saint Paul Police Department or while off-duty, an officer shall not initiate enforcement actions except in those circumstances where a potential threat to life or serious property damage exists (see the Off-Duty Law Enforcement Actions and Law Enforcement Authority policies).

Officers may render public assistance when it is deemed prudent (e.g., to a stranded motorist).

Officers driving take-home vehicles shall be armed, appropriately attired and carry their department-issued identification. Officers should also ensure that department radio communication capabilities are maintained to the extent feasible.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Use

703.4.5 MAINTENANCE

Members are responsible for the cleanliness (exterior and interior) and overall maintenance of their assigned vehicles. Cleaning and maintenance supplies will be provided by the Department. Failure to adhere to these requirements may result in discipline and loss of vehicle assignment. The following should be performed as outlined below:

- (a) Members shall make daily inspections of their assigned vehicles for service/maintenance requirements and damage.
- (b) It is the member's responsibility to ensure that his/her assigned vehicle is maintained according to the established service and maintenance schedule.
- (c) All scheduled vehicle maintenance and car washes shall be performed as necessary at a facility approved by the department supervisor in charge of vehicle maintenance.
- (d) The Department shall be notified of problems with the vehicle and approve any major repairs before they are performed.
- (e) When leaving the vehicle at the maintenance facility, the member will complete a vehicle repair card explaining the service or repair, and leave it on the seat or dash.
- (f) All weapons shall be removed from any vehicle left for maintenance.
- (g) Supervisors shall make, at a minimum, monthly inspections of vehicles assigned to members under their command to ensure the vehicles are being maintained in accordance with this policy.

703.5 DAMAGE, ABUSE AND MISUSE

When any department vehicle is involved in a traffic collision or otherwise incurs damage, the involved member shall promptly notify a supervisor. Any collision report shall be filed with the agency having jurisdiction (see the Traffic Collisions Policy).

Damage to any department vehicle that was not caused by a traffic collision shall be immediately reported during the shift in which the damage was discovered, documented in memorandum format and forwarded to the Sergeant. An administrative investigation should be initiated to determine if there has been any vehicle abuse or misuse.

703.6 MAINTENANCE

Members are responsible for the cleanliness (exterior and interior) and overall maintenance of the assigned vehicles.

Members shall make daily inspections of their assigned vehicles for service/maintenance requirements and damage. It is the assigned member's responsibility to ensure that his/her assigned vehicle is maintained according to the established service and maintenance schedule.

Supervisors shall make, at a minimum, monthly inspections of vehicles assigned to members under their command to ensure the vehicles are being maintained in accordance with policy.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Vehicle Use

703.7 ATTIRE AND APPEARANCE

When operating any department vehicle while off-duty, members may dress in a manner appropriate for their intended activity. Whenever in view of or in contact with the public, attire and appearance, regardless of the activity, should be suitable to reflect positively upon the Department.

Personal Protective Equipment

704.1 PURPOSE AND SCOPE

This policy identifies the different types of personal protective equipment (PPE) provided by the Department as well the requirements and guidelines for the use of PPE.

This policy does not address ballistic vests or protection from communicable disease, as those issues are addressed in the Body Armor and Communicable Diseases policies.

704.1.1 DEFINITIONS

Definitions related to this policy include:

Personal protective equipment (PPE) - Equipment that protects a person from serious workplace injuries or illnesses resulting from contact with chemical, radiological, physical, electrical, mechanical, or other workplace hazards.

Respiratory PPE - Any device that is worn by the user to protect from exposure to atmospheres where there is smoke, low levels of oxygen, high levels of carbon monoxide, or the presence of toxic gases or other respiratory hazards. For purposes of this policy, respiratory PPE does not include particulate-filtering masks such as N95 or N100 masks.

704.2 POLICY

The South Saint Paul Police Department endeavors to protect members by supplying certain PPE to members as provided in this policy.

704.3 OFFICER RESPONSIBILITIES

Members are required to use PPE as provided in this policy and pursuant to their training.

Members are responsible for proper maintenance and storage of issued PPE. PPE should be stored in an appropriate location so that it is available when needed.

Any member who identifies hazards in the workplace is encouraged to utilize the procedures in the Workplace Accident and Injury Reduction Policy to recommend new or improved PPE or additional needs for PPE.

704.4 HEARING PROTECTION

Approved hearing protection shall be used by members during firearms training.

Hearing protection shall meet or exceed industry standards for use at firing ranges (29 CFR 1910.95; Minn. R. 5205.0010).

704.5 EYE PROTECTION

Approved eye protection, including side protection, shall be used by members during firearms training. Eye protection for members who wear prescription lenses shall incorporate the prescription (e.g., eye protection that can be worn over prescription lenses). Members shall ensure their eye protection does not interfere with the fit of their hearing protection.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Protective Equipment

The Operations Commander shall ensure eye protection meets or exceeds consensus standards set by the American National Standards Institute (29 CFR 1910.133; Minn. R. 5205.0010).

704.6 HEAD AND BODY PROTECTION

Members who make arrests or control crowds should be provided ballistic head protection with an attachable face shield.

Padded body protection consisting of chest, arm, leg, and groin protection should be provided as required by any collective bargaining agreement.

704.7 RESPIRATORY PROTECTION

The Administration Division Commander is responsible for ensuring a respiratory protection plan is developed and maintained by a trained and qualified member. The plan shall include procedures for (29 CFR 1910.134; Minn. R. 5205.0010):

- (a) Selecting appropriate respiratory PPE based on hazards and risks associated with functions or positions.
- (b) Fit testing, including identification of members or contractors qualified to conduct fit testing.
- (c) Medical evaluations.
- (d) PPE inventory control.
- (e) PPE issuance and replacement.
- (f) Cleaning, disinfecting, storing, inspecting, repairing, discarding, and otherwise maintaining respiratory PPE, including schedules for these activities.
- (g) Regularly reviewing the PPE plan.
- (h) Remaining current with applicable National Institute for Occupational Safety and Health (NIOSH), American National Standards Institute (ANSI), Occupational Safety and Health Administration (OSHA), Environmental Protective Agency (EPA), and state PPE standards and guidelines.

704.7.1 RESPIRATORY PROTECTION USE

Designated members may be issued respiratory PPE based on the member's assignment (e.g., a narcotics investigator who is involved in clandestine lab investigations).

Respiratory PPE may be worn when authorized by a scene commander who will determine the type and level of protection appropriate at a scene based upon an evaluation of the hazards present.

Scene commanders are responsible for monitoring members using respiratory PPE and their degree of exposure or stress. When there is a change in work area conditions or when a member's degree of exposure or stress may affect respirator effectiveness, the scene commander shall reevaluate the continued effectiveness of the respirator and direct the member to leave the respirator use area when the scene commander reasonably believes (29 CFR 1910.134; Minn. R. 5205.0010):

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Protective Equipment

- (a) It is necessary for the member to wash his/her face and the respirator facepiece to prevent eye or skin irritation associated with respirator use.
- (b) The member detects vapor or gas breakthrough, or there is a change in breathing resistance or leakage of the facepiece.
- (c) The member needs to replace the respirator, filter, cartridge, or canister.

704.7.2 MEMBER RESPONSIBILITIES FOR RESPIRATORY PROTECTION

Members shall not use self-contained breathing apparatus (SCBA), full-face respirators, or cartridge respirators unless they have completed training requirements for the equipment.

Members exposed to environments that are reasonably known to be harmful due to gases, smoke, or vapors shall use respiratory PPE.

Members using respiratory PPE shall (29 CFR 1910.134; Minn. R. 5205.0010):

- (a) Ensure that they have no facial hair between the sealing surface of the facepiece and the face that could interfere with the seal or the valve function. Members also shall ensure that they have no other condition that will interfere with the face-to-facepiece seal or the valve function.
- (b) Not wear corrective glasses, goggles, or other PPE that interferes with the seal of the facepiece to the face, or that has not been previously tested for use with that respiratory equipment.
- (c) Perform a user seal check per department-approved procedures recommended by the respirator manufacturer each time they put on a tight-fitting respirator.
- (d) Leave a respiratory use area whenever they detect vapor or gas breakthrough, changes in breathing resistance or leakage of their facepiece and ensure that the respirator is replaced or repaired before returning to the affected area.

704.7.3 GAS MASK

Full-face air-purifying respirators, commonly referred to as gas masks, may be fitted with mechanical pre-filters or combination cartridge/filter assemblies for use in areas where gases, vapors, dusts, fumes, or mists are present. Members must identify and use the correct cartridge based on the circumstances (29 CFR 1910.134; Minn. R. 5205.0010).

A scene commander may order the use of gas masks in situations where the use of an SCBA is not necessary. These incidents may include areas where tear gas has or will be used or where a vegetation fire is burning. Gas masks shall not be used if there is a potential for an oxygen-deficient atmosphere.

Members shall ensure their gas mask filters are replaced whenever:

- (a) They smell, taste, or are irritated by a contaminant.
- (b) They experience difficulty breathing due to filter loading.
- (c) The cartridges or filters become wet.
- (d) The expiration date on the cartridges or canisters has been reached.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Protective Equipment

704.7.4 RESPIRATOR FIT TESTING

No member shall be issued respiratory PPE until a proper fit testing has been completed by a designated member or contractor (29 CFR 1910.134; Minn. R. 5205.0010).

After initial testing, fit testing for respiratory PPE shall be repeated (29 CFR 1910.134; Minn. R. 5205.0010):

- (a) At least once every 12 months.
- (b) Whenever there are changes in the type of SCBA or facepiece used.
- (c) Whenever there are significant physical changes in the user (e.g., obvious change in body weight, scarring of the face seal area, dental changes, cosmetic surgery, or any other condition that may affect the fit of the facepiece seal).

All respirator fit testing shall be conducted in negative-pressure mode.

704.7.5 RESPIRATORY MEDICAL EVALUATION QUESTIONNAIRE

No member shall be issued respiratory protection that forms a complete seal around the face until (29 CFR 1910.134; Minn. R. 5205.0010):

- (a) The member has completed a medical evaluation that includes a medical evaluation questionnaire.
- (b) A physician or other licensed health care professional has reviewed the questionnaire.
- (c) The member has completed any physical examination recommended by the reviewing physician or health care professional.

704.8 RECORDS

The is Operations Commander is responsible for maintaining records of all:

- (a) PPE training.
- (b) Initial fit testing for respiratory protection equipment.
- (c) Annual fit testing.
- (d) Respirator medical evaluation questionnaires and any subsequent physical examination results.

1. These records shall be maintained in a separate confidential medical file.

The records shall be maintained in accordance with the department records retention schedule, 29 CFR 1910.1020 and Minn. R. 5205.0010.

704.9 TRAINING

Members should be trained in the respiratory and other hazards to which they may be potentially exposed during routine and emergency situations.

All members shall be trained in the proper use and maintenance of PPE issued to them, including when the use is appropriate; how to put on, remove, and adjust PPE; how to care for the PPE; and the limitations (29 CFR 1910.132; Minn. R. 5205.0010).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Protective Equipment

Members issued respiratory PPE shall attend annual training on the proper use of respiratory protection devices (29 CFR 1910.134; Minn. R. 5205.0010).

Chapter 8 - Support Services

Evidence Room

800.1 PURPOSE AND SCOPE

This policy provides for the proper collection, storage and security of evidence and other property. Additionally, this policy provides for the protection of the chain of evidence and those persons authorized to remove and/or destroy property. Property belonging to persons in custody should be handled pursuant to policies guiding Juvenile Temporary Custody, Temporary Holding Facility, Jail Operations, and the operations procedures for each facility or operation.

800.1.1 EVIDENCE ROOM SECURITY

The Evidence Room shall maintain secure storage and control of all property necessitating custody by the Department. The property officers report to the Investigation Division supervisor and are responsible for the security of the Evidence Room. Evidence Room access is maintained only by the property officers and the Investigation Division supervisor. The property officers and the Investigation Division supervisor shall not loan Evidence Room access cards to anyone and shall maintain access cards in a secure manner.

Any individual entering the Evidence Room other than the property officers must be accompanied by the property officers or the Investigation Division supervisor.

800.2 DEFINITIONS

Property - Includes all items of evidence, items taken for safekeeping and found property.

Evidence - Includes items taken or recovered in the course of an investigation that may be used in the prosecution of a case. This includes photographs and latent fingerprints.

Safekeeping - Includes the following types of property:

- Property obtained by the Department for safekeeping, such as a firearm.
- Personal property of an arrestee not taken as evidence.
- Property taken for safekeeping under authority of a law.

Found Property - Includes property found by an employee or citizen that has no apparent evidentiary value and where the owner cannot be readily identified or contacted.

800.3 PROPERTY HANDLING

Any employee who first comes into possession of any property shall retain such property in their possession until it is properly tagged and placed in the designated property locker or storage room, along with the property form. Care shall be taken to maintain the chain of custody for all evidence.

Any property seized by an officer with or without a warrant shall be safely kept for as long as necessary for the purpose of being produced as evidence (Minn. Stat. § 626.04 (a)). Seized property held as evidence shall be returned to its rightful owner unless subject to lawful detention or ordered destroyed or otherwise disposed of by the court (Minn. Stat. § 626.04 (b) and Minn. Stat. § 629.361).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

An officer arresting a person for committing or aiding in committing a robbery, carjacking, or theft offense shall use reasonable diligence to secure the property that was alleged to have been stolen and shall be answerable for it while it remains in the officer's custody (Minn. Stat. § 629.361).

Where ownership can be established as to found property that has no apparent evidentiary value, such property may be released to the owner without the need for booking. The property documentation must be completed to document the release of property not booked. The owner shall sign the documentation acknowledging receipt of the items.

800.3.1 PROPERTY BOOKING PROCEDURE

All property must be booked prior to the employee going off-duty. Employees booking property shall observe the following guidelines:

- (a) Complete the property form describing each item of property separately, listing all serial numbers, owner's name, finder's name and other identifying information or markings.
- (b) The employee shall mark each item of evidence with initials and date.
- (c) Items too small to mark, or that will be damaged or degraded or devalued by marking, should be individually packaged, labeled and the package marked with initials and date.
- (d) Complete an evidence/property tag and attach it to each package or envelope in which the property is stored.
- (e) Place the case number in the upper right hand corner or in the appropriate field of the evidence/property tag.
- (f) The original property documentation shall be submitted with the case report. A copy shall be placed with the property in the temporary property locker or with the property if it is stored somewhere other than a property locker.
- (g) When the property is too large to be placed in a temporary property locker, the item may be temporarily stored in any department supply room or other location that can be secured from unauthorized entry. The location shall be secured to prevent entry and a completed property form placed into a numbered property locker indicating the location of the property.

800.3.2 CONTROLLED SUBSTANCES

All controlled substances shall be booked separately using a separate property record. Drug paraphernalia shall also be booked separately.

The officer seizing the narcotics and dangerous drugs shall place them in the designated temporary property locker accompanied by the property documentation form. A copy of the original form will be detached and submitted with the case report.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

800.3.3 EXPLOSIVES

Officers who encounter a suspected explosive device shall promptly notify the immediate supervisor. The Bomb Squad will be called to handle explosive-related incidents and will be responsible for the handling, storage, sampling and disposal of all suspected explosives.

Explosives will not be retained in the police facility. Only fireworks that are considered stable and safe and road flares or similar signaling devices may be booked into property. All such items shall be stored in proper containers and in an area designated for the storage of flammable materials.

800.3.4 EXCEPTIONAL HANDLING

Certain property items require a separate process. The following items shall be processed in the described manner:

- (a) Bodily fluids such as blood or semen stains shall be air-dried prior to booking.
- (b) License plates found not to be stolen or connected with a known crime, should be released directly to the property officer or placed in the designated container for return to the Minnesota Department of Driver and Vehicle Services. No formal property booking process is required.
- (c) All bicycles and bicycle frames require a property record. Property tags will be securely attached to each bicycle or bicycle frame. The property may be released directly to the property officer, or placed in the bicycle storage area until a property officer can log the property.
- (d) All cash shall be counted in the presence of another officer and the envelope initialed by both officers. A supervisor shall be contacted for cash in excess of \$1,000. The supervisor shall also witness the count, and will initial and date the property documentation and specify any additional security procedures to be used.
- (e) All evidence collected by personnel processing a crime scene requiring specific storage requirements pursuant to laboratory procedures should clearly indicate storage requirements on the property form.

City property, unless connected to a known criminal case, should be released directly to the appropriate City department. No formal booking is required. In cases where no responsible person can be located, the property should be booked for safekeeping in the normal manner.

800.3.5 COURT-ORDERED FIREARM SURRENDERS

- (a) Although not required, this department generally will accept firearms surrendered by an abusing party or defendant pursuant to a court order. A decision to refuse a surrendered firearm should be approved by a supervisor (Minn. Stat. § 260C.201, Subd. 3; Minn. Stat. § 518B.01, Subd. 6; Minn. Stat. § 609.2242, Subd. 3; Minn. Stat. § 609.749, Subd. 8; Minn. Stat. § 624.7175).
- (b) Members accepting surrendered firearms should complete a standardized Firearms Proof of Transfer form, if available. If the surrender relates to an extreme risk protection order, the individual should be provided with a copy of the Proof of Transfer form

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

(Minn. Stat. § 624.7175). If a standard form is not available, an evidence/property form should be used and include the following information:

1. Whether the firearm is being transferred temporarily or permanently
 2. The abusing party or defendant's name
 3. The date and time of the transfer
 4. Complete description of all firearms surrendered (e.g., make, model, serial number, color, identifying marks)
- (c) In certain circumstances, a court may issue an order for the immediate transfer of firearms of an abusing party or defendant.
1. The Department may serve the court order either by assignment or when an officer comes into contact with an abusing party or defendant for which a court order has been issued but has not been served, or for which they are in violation. In such cases, if there are firearms that may be lawfully seized, they should be seized and submitted to the Evidence Room pursuant to standard protocol.
 2. If the abusing party or defendant is not cooperative, seek guidance from legal counsel to ensure that firearms are seized lawfully.
 3. Permits possessed by the abusing party or defendant should be returned to the Sheriff where the person resides.
- (d) The Evidence Room shall develop and maintain a process to store, transfer, or release firearms ordered surrendered by a court. The procedures shall:
1. Provide for adequate storage and protection so as to preserve the condition of the firearms.
 2. Require a valid court order or written notice from the abusing party or defendant to be presented before any transfer of the firearms.
 3. Ensure that recipients of transferred firearms are not legally prohibited from possession of firearms under state or federal law.
 4. Ensure that proper affidavits or proof of transfer are obtained from any designated firearms dealer or third party.
 5. Ensure that prior to disposition of unclaimed firearms, abusing parties or defendants are notified via certified mail.

800.4 PACKAGING OF PROPERTY

Packaging will conform to the Property Packaging Procedures. Certain items require special consideration and shall be booked separately as follows:

- (a) Controlled substances
- (b) Firearms (ensure they are unloaded and booked separately from ammunition)
- (c) Property with more than one known owner
- (d) Drug paraphernalia

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

- (e) Fireworks
- (f) Contraband

800.4.1 PACKAGING CONTAINER

Employees shall package all property, except controlled substances in a suitable container available for its size. Knife boxes should be used to package knives, handgun boxes should be used for handguns and syringe tubes should be used to package syringes and needles.

A property tag shall be securely attached to the outside of all items or group of items packaged together.

800.4.2 PACKAGING CONTROLLED SUBSTANCES

The officer seizing controlled substances shall retain such property in his/her possession until it is properly packaged, tagged and placed in a locker, accompanied by the property record.

Controlled substances shall be packaged, available in the property processing room. The booking officer shall initial the sealed envelope and the initials covered with evidence tape. Controlled substances shall not be packaged with other property.

800.5 RECORDING OF PROPERTY

The property officer receiving custody of evidence or property shall create a property control entry for each piece of property received. The property control entry will be the permanent record of the property in the Evidence Room. The property officer will record the date and time the property was received and where the property will be stored on the property control entry.

A property database shall be maintained and a unique property number created for each piece of property received. The database shall record by property number, the date received, case number, tag number, item description, item location and date disposed. A unique property number shall be obtained for each item or group of items from the database. This number shall be recorded on the property tag and the database entry.

Any changes in the location of property held by the South Saint Paul Police Department shall be noted in the property database.

800.6 PROPERTY CONTROL

Each time the property officer receives property or releases property to another person, he/she shall enter this information in the property control database. Officers desiring property for court shall contact the property officer at least one day prior to the court day.

800.6.1 RESPONSIBILITIES OF OTHER PERSONNEL

Every time property is released or received, an appropriate entry on the evidence package shall be completed to maintain the chain of possession. No property or evidence is to be released without first receiving written authorization from a supervisor or investigator.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

Request for analysis for items other than controlled substances shall be completed on the appropriate forms and submitted to the property officer. This request may be filled out any time after booking of the property or evidence.

800.6.2 TRANSFER OF EVIDENCE TO CRIME LABORATORY

The transporting employee will check the evidence out of property, indicating the date and time in the property database and the request for laboratory analysis.

The property officer releasing the evidence must complete the required information in the property database. The lab forms will be transported with the property to the examining laboratory. Upon delivering the item involved, the officer will record the delivery time on both copies and indicate the locker in which the item was placed or the employee to whom it was delivered. The original copy of the lab form will remain with the evidence and the copy will be returned to the Records Section for filing with the case.

800.6.3 STATUS OF PROPERTY

Each person receiving property will make the appropriate entry to document the chain of evidence. Temporary release of property to officers for investigative purposes, or for court, shall be noted on the property control card, stating the date, time and to whom it was released.

The property officer shall obtain the signature of the person to whom property was released, and the reason for release. Any employee receiving property shall be responsible for such property until it is properly returned to property or properly released to another authorized person or entity.

The return of the property should be recorded in the property database, indicating date, time and the person who returned the property.

800.6.4 AUTHORITY TO RELEASE PROPERTY

The property officer shall not release any property without authorization from an appropriate authorized member of the Department. The property room officer(s) and / or supervisor shall authorize the disposition or release of all evidence and property coming into the care and custody of the Department.

Property held as evidence for a pending criminal investigation or proceeding shall be retained for a period of time no less than that required pursuant to Minn. Stat. § 628.26.

For property in custody of the Department for investigatory or prosecutorial purposes and owned by a victim or witness, a property officer shall, upon the request of the owner:

- (a) Provide a list describing the property unless such release would seriously impede an investigation.
- (b) Return the property expeditiously unless the property is required as evidence.

Upon the direction of a prosecuting attorney, property held as evidence of a crime may be photographed and released to the owner of the property in accordance with the requirements of Minn. Stat. 609.523.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

800.6.5 RELEASE OF PROPERTY

All reasonable attempts shall be made to identify the rightful owner of found property or evidence not needed for an investigation.

Release of property shall be made upon receipt of an authorized release form, listing the name and address of the person to whom the property is to be released. Receiving individuals must present a valid photo ID which will be photocopied and placed in the file.

With the exception of firearms and other property specifically regulated by statute, found property and property held for safekeeping shall be held for a minimum of 90 days. During such period, property personnel shall attempt to contact the rightful owner by telephone and/or mail when sufficient identifying information is available. Property not held for any other purpose and not claimed within 60 days after notification (or receipt, if notification is not feasible) may be auctioned to the highest bidder at a properly published public auction, which may be conducted as an Internet-based auction. If such property is not sold at auction or otherwise lawfully claimed, it may thereafter be destroyed.

A property officer shall release the property upon proper identification being presented by the owner for which an authorized release has been received. The owner shall also pay any costs incurred by the agency, including costs for advertising or storage. A signature of the person receiving the property shall be recorded on the original property documentation. After release of all property entered in the property database. If some items of property have not been released, the property card will remain with the Evidence Room.

Upon release or other form of disposal, the proper entry shall be recorded in all property documentation and logs.

800.6.6 STOLEN OR EMBEZZLED PROPERTY

Stolen or embezzled property or property believed to be stolen or embezzled that is in the custody of this department may be restored to the owner (Minn. Stat. § 609.523 Subd. 3). Such property may be released from law enforcement custody when the following are satisfied:

- (a) Photographs of the property are filed and retained by the Evidence Room.
- (b) Satisfactory proof of ownership of the property is shown by the owner.
- (c) A declaration of ownership is signed under penalty of perjury.
- (d) A receipt for the property is obtained from the owner upon delivery.

800.6.7 DISPUTED CLAIMS TO PROPERTY

Occasionally more than one party may claim an interest in property being held by the department, and the legal rights of the parties cannot be clearly established. Such property shall not be released until one party has obtained a court order or other proof of the undisputed right to the involved property.

All parties should be advised that their claims are civil. In extreme situations, legal counsel for the Department may be asked to file an interpleader in court to resolve the disputed claim.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

800.6.8 RELEASE AND DISPOSAL OF FIREARMS

A firearm may not be released until it has been verified that the person receiving the weapon is not prohibited from receiving or possessing the weapon by 18 USC § 922.

The Department shall make best efforts for a period of 90 days after the seizure of an abandoned or stolen firearm to protect the firearm from harm and return it to the lawful owner (Minn. Stat. § 609.5315 Subd. 7). At the expiration of such period, the firearm or other deadly weapon may be processed for disposal consistent with this policy.

800.7 DISPOSITION OF PROPERTY

All property not held for evidence in a pending criminal investigation or proceeding, and held for six months or longer where the owner has not been located or fails to claim the property, may be disposed of in compliance with existing laws upon receipt of proper authorization for disposal.

800.7.1 EXCEPTIONAL DISPOSITIONS

The following types of property shall be destroyed or disposed of in the manner and at the time prescribed by law, unless a different disposition is ordered by a court of competent jurisdiction:

- Weapons declared by law to be nuisances.
- Animals, birds and equipment related to their care and containment that have been ordered forfeited by the court.
- Counterfeiting equipment.
- Gaming devices.
- Obscene matter ordered to be destroyed by the court.
- Altered vehicles or component parts.
- Controlled substances.
- Unclaimed, stolen or embezzled property.
- Destructive devices.

Money found in gambling devices by any peace officer, other than a municipal police officer, shall be paid into the county treasury. Money found in gambling devices by a municipal police officer shall be paid into the treasury of the municipality (Minn. Stat. § 626.04 (b)).

800.7.2 UNCLAIMED MONEY

If found or seized money is no longer required as evidence and remains unclaimed after three years, the money is presumed abandoned property and is reportable as specified in this policy (Minn. Stat. § 345.38 and Minn. Stat. § 345.75).

800.7.3 RETENTION OF BIOLOGICAL EVIDENCE

The Evidence Room Supervisor shall ensure that no biological evidence held by the Department is destroyed without adequate notification to the following persons, when applicable:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Evidence Room

- (a) The defendant
- (b) The defendant's attorney
- (c) The appropriate prosecutor
- (d) Any sexual assault victim
- (e) The Investigation Division Supervisor

Biological evidence shall be retained for a minimum period established by law, the Evidence Room Supervisor or the expiration of any sentence imposed related to the evidence (Minn. Stat. § 590.10), whichever time period is greater. Following the retention period, notifications should be made by certified mail and should inform the recipient that the evidence will be destroyed after a date specified in the notice unless a motion seeking an order to retain the sample is filed and served on the Department within 90 days of the date of the notification. A record of all certified mail receipts shall be retained in the appropriate file. Any objection to, or motion regarding, the destruction of the biological evidence should be retained in the appropriate file and a copy forwarded to the Investigation Division Supervisor.

Biological evidence related to a homicide shall be retained indefinitely and may only be destroyed with the written approval of the Chief of Police and the head of the applicable prosecutor's office.

Bulk evidence may be destroyed prior to these minimum retention periods only pursuant to a court order or if the Evidence Room Supervisor determines that such destruction is consistent with Minn. Stat. § 590.10 and the above notices have been made.

800.8 INSPECTIONS OF THE EVIDENCE ROOM

- (a) Unannounced inspections of evidence storage areas shall be conducted annually as directed by the Chief of Police.
- (b) An annual audit of evidence held by the Department shall be conducted by a Division Commander who is not routinely or directly connected with evidence control, as assigned by the Chief of Police.

Records Section

801.1 PURPOSE AND SCOPE

This policy establishes the guidelines for the operational functions of the South Saint Paul Police Department Records Section. The policy addresses department file access and internal requests for case reports.

801.2 FILE ACCESS AND SECURITY

The security of files in the Records Section must be a high priority and shall be maintained as mandated by state or federal law. All case reports including but not limited to initial, supplemental, follow-up, evidence, and any other reports related to a police department case, including field interview (FI) cards, criminal history records, and publicly accessible logs, shall be maintained in a secure area within the Records Section, accessible only by authorized members of the Records Section. Access to case reports or files when Records Section staff is not available may be obtained through the Sergeant.

The Records Section will also maintain a secure file for case reports deemed by the Chief of Police as sensitive or otherwise requiring extraordinary access restrictions.

801.2.1 ORIGINAL CASE REPORTS

Generally, original case reports shall not be removed from the Records Section.

801.3 RECORDS MANAGER TRAINING

The Records Supervisor shall receive training in records management, including proper maintenance, retention and disposal of records and the proper release of records under the Minnesota Government Data Practices Act (MGDPA).

801.4 POLICY

It is the policy of the South Saint Paul Police Department to maintain department records securely, professionally, and efficiently.

801.5 RESPONSIBILITIES

801.5.1 RECORDS SUPERVISOR

The Chief of Police shall appoint and delegate certain responsibilities to a Records Supervisor. The Records Supervisor shall be directly responsible to the Administration Division Commander or the authorized designee.

The responsibilities of the Records Supervisor include, but are not limited to:

- (a) Overseeing the efficient and effective operation of the Records Section.
- (b) Scheduling and maintaining Records Section time records.
- (c) Supervising, training, and evaluating Records Section staff.
- (d) Maintaining and updating a Records Section procedure manual.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Section

- (e) Ensuring compliance with established policies and procedures.
- (f) Supervising the access, use, and release of protected information (see the Protected Information Policy).
- (g) Establishing security and access protocols for case reports designated as sensitive, where additional restrictions to access have been implemented. Sensitive reports may include but are not limited to:
 - 1. Homicides
 - 2. Cases involving department members or public officials
 - 3. Any case where restricted access is prudent

801.5.2 RECORDS SECTION

The responsibilities of the Records Section include but are not limited to:

- (a) Maintaining a records management system for case reports.
 - 1. The records management system should include a process for numbering, identifying, tracking, and retrieving case reports.
- (b) Entering case report information into the records management system.
 - 1. Modification of case reports shall only be made when authorized by a supervisor.
- (c) Providing members of the Department with access to case reports when needed for investigation or court proceedings.
- (d) Maintaining compliance with federal, state, and local regulations regarding reporting requirements of crime statistics.
- (e) Maintaining compliance with federal, state, and local regulations regarding criminal history reports and auditing.
- (f) Identifying missing case reports and notifying the responsible member's supervisor.
- (g) Establishing a process for collecting and submitting data to appropriate federal data collection authorities (e.g., FBI National Use-of-Force Data Collection, U.S. Department of Justice's National Law Enforcement Accountability Database), as applicable, for the following types of occurrences:
 - 1. Officer suicides
 - 2. Officer misconduct
 - 3. Uses of force
 - 4. Officer deaths or assaults
 - 5. Crime incidents
 - 6. Deaths in custody
- (h) Transmitting data annually to the superintendent of the Bureau of Criminal Apprehension on the number of mobile tracking device search warrants obtained by the Department as provided in Minn. Stat. § 626A.35.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Section

- (i) Transmitting carjacking information annually to the Commissioner of Public Safety as provided in Minn. Stat. § 626.5535.

801.6 CONFIDENTIALITY

Records Section staff has access to information that may be confidential or sensitive in nature. Records Section staff shall not access, view, or distribute, or allow anyone else to access, view, or distribute any record, file, or report, whether in hard copy or electronic file format, or any other confidential, protected, or sensitive information except in accordance with the Records Maintenance and Release and Protected Information policies and the Records Section procedure manual.

Records Maintenance and Release

802.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of department records. Protected information is separately covered in the Protected Information Policy.

802.1.1 DEFINITIONS

Definitions related to this policy include:

Confidential Data on Individuals - Data classified as confidential by state or federal law and that identifies individuals and cannot be disclosed to the public or even to the individual who is the subject of the data (Minn. Stat. § 13.02, Subd. 3).

Corrections and Detention Data - Data on individuals created, collected, used or maintained because of their lawful confinement or detainment in state reformatories, prisons and correctional facilities, municipal or county jails, lockups, work houses, work farms and all other correctional and detention facilities (Minn. Stat. § 13.85, Subd. 1).

Data on Individuals - All government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual (Minn. Stat. § 13.02, Subd. 5).

Government Data - Data collected, created, received, maintained or disseminated by this department regardless of its physical form, storage media or conditions of use (Minn. Stat. § 13.02, Subd. 7).

Private Data - Data classified as private by state or federal law and that identifies individuals that are only available to the individual who is the subject of the data or with the individual's consent (Minn. Stat. § 13.02, Subd. 12).

802.2 POLICY

The South Saint Paul Police Department is committed to providing public access to records and data in a manner that is consistent with the Minnesota Government Data Practices Act (MGDPA) and Official Records Act (Minn. Stat. § 13.03; Minn. Stat. § 15.17).

The South Saint Paul Police Department is committed to maintaining a high degree of information security for its protected CJIS environment. In order to accomplish this, the South Saint Paul Police Department has adopted all of the core security controls outlined in the FBI's CJIS Security Policy Version 5.7 (and future versions).

The CJIS 5.7 Security Policy manual is located in H:/CJIS Training Info.

All South Saint Paul Police Department staff, as well as any non-criminal justice contractors and personnel, shall follow the security controls as outlined in the CJIS Security Policy Version 5.7 (and future versions).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Maintenance and Release

802.3 CUSTODIAN OF RECORDS RESPONSIBILITIES

The Chief of Police shall designate a Custodian of Records. The responsibilities of the Custodian of Records include, but are not limited to:

- (a) Managing the records management system for the Department, including the retention, archiving, release, and destruction of department data (Minn. Stat. § 15.17; Minn. Stat. § 138.17, Subd. 7).
- (b) Maintaining and updating the department records retention schedule, including:
 - 1. Identifying the minimum length of time the Department must keep data.
 - 2. Identifying the department division responsible for the original data.
- (c) Establishing rules regarding the inspection and copying of department data as reasonably necessary for the protection of such data.
- (d) Identifying data or portions of data that are confidential under state or federal law and not open for inspection or copying.
- (e) Establishing rules regarding the processing of subpoenas for the production of data.
- (f) Ensuring a current schedule of fees for public data as allowed by law is available.
- (g) Ensuring the posting or availability to the public a document that contains the basic rights of a person who requests government data, the responsibilities of the Department, and any associated fees (Minn. Stat. § 13.025).
- (h) Ensuring data created by the Department is inventoried and subject to inspection and release pursuant to lawful requests consistent with the MGDPA requirements (Minn. Stat. § 13.03, Subd. 1).
- (i) Ensuring that the current version of each department policy identified in Minn. R. 6700.1615 is posted on the department's website or otherwise posted in the public area of the Department in accordance with Minn. R. 6700.1615 (Minn. R. 6700.1615, Subd. 2).

802.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any department member who receives a request for data shall route the request to the Custodian of Records or the authorized designee.

802.4.1 REQUESTS FOR RECORDS

The processing of requests for data is subject to the following:

- (a) A person shall be permitted to inspect and copy public government data upon request at reasonable times and places and shall be informed of the data's meaning if requested (Minn. Stat. § 13.03, Subd. 3).
 - 1. The Department may not charge or require the requesting person to pay a fee to inspect data. Inspection includes, but is not limited to, the visual inspection of paper and similar types of government data. Inspection does not include printing copies, unless printing a copy is the only method to provide for inspection of the data (Minn. Stat. § 13.03, Subd. 3(b)).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Maintenance and Release

2. For data stored and made available in electronic form via remote access, public inspection includes allowing remote access by the public to the data and the ability to print copies or download the data. A fee may be charged for remote access to data where either the data or the access is enhanced at the request of the person seeking access (Minn. Stat. § 13.03, Subd. 3(b)).
- (b) Government data maintained by this department using a computer storage medium shall be provided in that medium in electronic form, if a copy can be reasonably made. The Department is not required to provide the data in an electronic format or program that is different from the format or program in which the data is maintained (Minn. Stat. § 13.03, Subd. 3 (e)).
- (c) The Department is not required to create records that do not exist.
- (d) The Custodian of Records or designee processing the request shall determine if the requested data is available and, if so, whether the data is restricted from release or denied. The Custodian of Records or designee shall inform the requesting person of the determination either orally at the time of the request or in writing as soon after that time as reasonably possible. The Custodian of Records or designee shall cite the specific statutory section, temporary classification or specific provision of state or federal law on which the determination is based. Upon the request of any person denied access to data, the denial shall be certified in writing (Minn. Stat. § 13.03, Subd. 3 (f)).
- (e) When a record contains data with release restrictions and data that is not subject to release restrictions, the restricted data shall be redacted and the unrestricted data released.
 1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the department-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

802.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

- (a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address, and telephone number; and medical or disability information that is contained in any driver's license record, motor vehicle record, or any department record, including traffic collision reports, is restricted except as authorized by the Department, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).
- (b) Private data on the following individuals (Minn. Stat. § 13.82, Subd. 17):
 1. An undercover law enforcement officer
 2. A victim or alleged victim of criminal sexual conduct, or sex trafficking, or of a violation of Minn. Stat. § 617.246, Subd. 2

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Maintenance and Release

3. A paid or unpaid informant if the Department reasonably believes revealing the identity would threaten the personal safety of the informant
 4. A victim of or witness to a crime if the victim or witness specifically requests not to be identified publicly, unless the Department reasonably determines that revealing the identity of the victim or witness would not threaten the personal safety or property of the individual
 5. A person who placed a call to a 9-1-1 system or the identity of the person whose phone was used to place a call to the 9-1-1 system when revealing the identity may threaten the personal safety or property of any person or the purpose of the call was to receive help in a mental health emergency. A voice recording of a call placed to the 9-1-1 system is deemed to reveal the identity of the caller
 6. A juvenile witness when the subject matter of the investigation justifies protecting the identity of the witness
 7. A mandated reporter
 8. A judicial official as described in Minn. Stat. § 480.40 (Minn. Stat. § 13.991)
- (c) Audio recordings of calls placed to the 9-1-1 system requesting law enforcement, fire, or medical agency response, except that a written transcript of the call is public unless it reveals the identity of protected individuals (Minn. Stat. § 13.82, Subd. 4).
- (d) Criminal investigative data involving active cases and inactive investigative data (Minn. Stat. § 13.82, Subd. 7):
1. If the release of the data would jeopardize another ongoing investigation or would reveal the identity of protected individuals or is otherwise restricted.
 2. Images and recordings, including photographs, video, and audio records that are clearly offensive to common sensibilities. However, the existence of any such image or recording shall be disclosed.
 3. As otherwise restricted by law.
- (e) Juvenile records and data (Minn. Stat. § 260B.171).
- (f) State criminal history data held in the Bureau of Criminal Apprehension (BCA) database, including but not limited to fingerprints, photographs, identification data, arrest data, prosecution data, criminal court data, and custody and supervision data (Minn. Stat. § 13.87).
- (g) Traffic collision reports and related supplemental information (Minn. Stat. § 169.09, Subd. 13).
- (h) Corrections and detention data (Minn. Stat. § 13.85).
- (i) Personnel data except, unless otherwise restricted (Minn. Stat. § 13.43, Subd. 2):
1. Name, employee identification number, and some aspects of compensation
 2. Job title, bargaining unit, job description, education and training background, and previous work experience
 3. Date of first and last employment

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Maintenance and Release

4. Existence and status of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action
 5. Final disposition of any disciplinary action together with the specific reasons for the action, and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of this department
 6. Terms of any agreement settling any dispute arising out of an employment relationship
 7. Work location, work telephone number, badge number, and honors and awards received
 8. Time sheets or other comparable data only used to account for an employee's work time for payroll purposes, excluding the use of sick or other medical leave or other nonpublic data
 9. All other personnel data regarding employees of this department are private data and may only be released as authorized by that classification
- (j) Any data that was created under the direction or authority of the City Attorney exclusively in anticipation of potential litigation involving this department shall be classified as protected nonpublic or confidential data while such action is pending (Minn. Stat. § 13.39).
- (k) All data collected by an Automated License Plate Reader (ALPR) on individuals or nonpublic data absent an exception (Minn. Stat. § 13.82; Minn. Stat. § 13.824).
- (l) Response or incident data, so long as the Custodian of Records determines that public access would likely endanger the physical safety of an individual or cause a perpetrator to flee, evade detection, or destroy evidence (Minn. Stat. § 13.82, Subd. 14).
- (m) Any data on individuals receiving peer counseling or critical incident stress management services (Minn. Stat. § 13.02, Subd. 12; Minn. Stat. § 181.9731; Minn. Stat. § 181.9732).

Any other record not addressed in this policy shall not be subject to release where such record is classified as other than public data. All public data shall be released as required by the MGDPA (Minn. Stat. § 13.03, Subd. 1).

802.6 SUBPOENAS AND DISCOVERY REQUESTS

Any member who receives a subpoena duces tecum or discovery request for data should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested data.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the County and City Attorney Offices, City Attorney or the courts.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Maintenance and Release

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Department so that a timely response can be prepared.

802.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the department name and to whom the record was released.

Each audio/video recording released shall include the department name and to whom the record was released.

802.8 EXPUNGEMENT

A petition for expungement and expungement orders received by the Department shall be reviewed for appropriate action by the Custodian of Records.

802.8.1 PETITION FOR EXPUNGEMENT

When responding to a petition for expungement, the Custodian of Records shall inform the court and the individual seeking expungement that the response contains private or confidential data (Minn. Stat. § 609A.03, Subd. 3).

802.8.2 ORDERS OF EXPUNGEMENT

The Custodian of Records shall expunge such records as ordered by the court. Records may include, but are not limited to, a record of arrest, investigation, detention or conviction. Once a record is expunged, members shall respond to any inquiry as though the record did not exist.

Upon request by the individual whose records are to be expunged, the Custodian of Records must send a letter at an address provided by the individual confirming the receipt of the expungement order and that the record has been expunged (Minn. Stat. § 609A.03, Subd. 8).

Expunged records may be opened only by court order (Minn. Stat. § 609A.03, Subd. 7).

Expunged records of conviction may be opened for purposes of evaluating a prospective employee of the Department without a court order.

The Custodian of Records shall inform any law enforcement, prosecution or corrections authority, upon request, of the existence of a sealed record and of the right to obtain access to it.

802.8.3 BCA NOTIFICATION OF GRANT OF EXPUNGEMENT

If the Department receives notice from the BCA that its records may be affected by an automatic grant of expungement, the Custodian of Records shall determine if any records requested thereafter were expunged and, if so, treat the records as private data except as provided by law (Minn. Stat. § 609A.015, Subd. 5).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Records Maintenance and Release

802.9 MAINTENANCE OF CLOSED RECORDS

Records such as offense reports, arrest reports, juvenile records or other sensitive records shall be secured in such a manner as to reasonably protect them from unauthorized disclosure. Closed records shall be kept separate from public records and shall remain confidential.

Protected Information

803.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the South Saint Paul Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the government data information covered in the Records Maintenance and Release Policy.

803.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the South Saint Paul Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

803.2 POLICY

Members of the South Saint Paul Police Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

803.3 RESPONSIBILITIES

The Chief of Police shall select a member of the Department to coordinate the use of protected information (Minn. Stat. § 13.05, Subd. 13).

The responsibilities of this position include but are not limited to:

- (a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, the National Law Enforcement Telecommunications System (NLETS), Minnesota Division of Driver and Vehicle Services (DVS) records, Minnesota Bureau of Criminal Apprehension (BCA), and the Minnesota Comprehensive Incident-Based Reporting System (CIBRS).
- (b) Developing, disseminating, and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy. See the South Saint Paul Police Department CJIS Access, Maintenance, and Security Policy for additional guidance.
- (c) Developing, disseminating, and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release, and security of protected information.
- (d) Developing procedures to ensure training and certification requirements are met.
- (e) Resolving specific questions that arise regarding authorized recipients of protected information.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Protected Information

- (f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.
- (g) Ensuring a comprehensive security assessment of any personal information maintained by the South Saint Paul Police Department is conducted at least annually (Minn. Stat. § 13.055, Subd. 6).
- (h) Ensuring CIBRS is notified within 10 days that an investigation in CIBRS has become inactive (Minn. Stat. § 299C.40).

803.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, South Saint Paul Police Department policy, or training (Minn. Stat. § 13.09). Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access (Minn. Stat. § 13.05; Minn. Stat. § 299C.40).

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution. See the CJIS Access, Maintenance, and Security Policy for additional guidance.

803.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Section to ensure proper documentation of the release (see the Records Release and Security Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other department members or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

803.5.1 REVIEW OF CHRI

Members of this department shall refer individuals seeking access to CHRI to the Minnesota BCA (Minn. Stat. § 13.87, Subd. 1(b)).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Protected Information

803.5.2 REVIEW OF CIBRS DATA

An individual who is the subject of private data held by CIBRS may request access to the data by making a request to the Records Supervisor. If the request is to release the data to a third party, the individual who is the subject of private data must appear in person at the Department to give informed consent to the access or release.

Private data provided to the individual must also include the name of the law enforcement agency that submitted the data to CIBRS and the name, telephone number and address of the agency responsible for the data.

A person who is the subject of private data may challenge the data. The Records Supervisor shall review the challenge and determine whether the data should be completed, corrected or destroyed. The corrected data must be submitted to CIBRS and any future dissemination must be of the corrected data.

The Records Supervisor must notify BCA as soon as reasonably practicable whenever data held by CIBRS is challenged. The notification must identify the data that was challenged and the subject of the data.

803.6 SECURITY OF PROTECTED INFORMATION

The Chief of Police will select a member of the Department to oversee the security of protected information.

The responsibilities of this position include but are not limited to (see the CJIS Access, Maintenance, and Security Policy for additional guidance):

- (a) Developing and maintaining security practices, procedures, and training.
- (b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.
- (c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents, including computer attacks.
- (d) Tracking, documenting, and reporting all breach of security incidents to the Chief of Police and appropriate authorities.

803.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

803.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Protected Information

authorized access and use of protected information, as well as its proper handling and dissemination.

803.8 SECURITY BREACHES

In the event of an actual or potential breach of the security or other unauthorized acquisition of private or confidential information, the Chief of Police or designee shall ensure an investigation into the breach is made. Upon completion of the investigation and final disposition of any disciplinary action, a report containing the facts and result of the investigation shall be prepared. If the breach was conducted by an employee, contractor or agent of South Saint Paul, the report must include a description of the type of data that was breached, the number of individuals whose information was breached, the disposition of any related disciplinary action, and the identity of the employee determined to be responsible for the breach (Minn. Stat. § 13.055).

Written notice shall be given to any individual whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person as soon as reasonably practicable. The notice shall include the following (Minn. Stat. § 13.055):

- (a) Notification that an investigation will be conducted.
- (b) Notification that a report containing the facts and results will be prepared.
- (c) Information on how the person may obtain access to the report, including that he/she may request delivery of the report by mail or e-mail.

The notice may be delayed only so long as necessary to determine the scope of the breach and restore the reasonable security of the data or so long as it will impede an active criminal investigation. Notice shall be made by first class mail, electronic notice or substitute notice as provided in Minn. Stat. § 13.055, Subd. 4., If notification is required to be made to more than 1,000 individuals, notice to all consumer reporting agencies of the timing distribution and content of the notices must also be made (Minn. Stat. § 13.055, Subd. 5).

CJIS Policy

804.1 CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY POLICY

The South St. Paul Police Department Police Department is committed to maintaining a high degree of Information Security for its protected CJIS Environment. In order to accomplish this, the South St. Paul Police Department Police Department has adopted all of the core security controls outlined in the FBI's CJIS Security Policy Version 5.7 (and future versions).

The CJIS 5.7 Security Policy manual is located in this Lexipol Policy.

All South St. Paul Police Department Police Department staff, as well as any non-criminal justice contractor(s) and personnel, shall follow the security controls as outline in the CJIS Security Policy Version 5.7 (and future versions).

Specific CJIS Policy mandated Procedures that accompany this memo, can be found in this Lexipol Policy.

804.2 MANAGEMENT CONTROL AGREEMENT

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the South St Paul IT for the interstate exchange of criminal history/criminal justice information, the South St. Paul Police Department shall have the authority, via managed control, to set, maintain, and enforce:

1. Priorities
2. Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI);
3. Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community
4. Restriction of unauthorized personnel from access or use of equipment accessing the State network; and
5. Compliance with all rules and regulations of the South St. Paul Police Department's Policies and CJIS Security Policy in the operation of all information received.

This agreement ensures that management control of the criminal justice function remains solely with the Criminal Justice Agency. Section 5.1.1.4

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Policy

This agreement covers the overall supervision of all South St. Paul Police Department's systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any South St. Paul Police Department system to include NCIC Programs that may be subsequently designed and/or implemented within the South St. Paul Police Department.

804.3 PHYSICAL PROTECTION PROCEDURE FOR SOUTH ST. PAUL POLICE DEPARTMENT

The Purpose of these procedures is to ensure that access to CJIS Data and Systems that contain CJIS Data are protected with the required Physical Controls, so that only authorized users are able to gain access.

Any CJIS Data that the South St. Paul Police Department is responsible for can be found in the following:

- CAD
- ProPhoenix RMS
- Tracker Evidence System
- BCA Portals
- CJN eForms Reporting System
- Laserfiche
- LiveScan Fingerprint System
- Local Police File Server

Physically Secure Location is Define by CJIS Policy as:

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

The South St. Paul Police Department shall implement the following physical Security Controls to protect the Physically Secure Locations:

- (a) Perimeter of the Secure Locations are marked with signs that say, "Authorized Personnel Only;"
- (b) Ensure that authorized personnel are on boarded and then access is removed within one week or less of termination;
- (c) Access Control Badges shall be issued to all authorized personnel in order to control access to controlled locations;

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Policy

- (d) Access Control System shall be programmed, using role based assignments, in order to control access to only the CJIS Systems they are authorized to access;
- (e) The South St. Paul Building Management shall be responsible for monitoring the Access Control system;
- (f) Visitors shall be required to sign in at the Front Counter prior to being escorted into any Secure Location by an authorized staff member;

804.4 MEDIA PROTECTION PROCEDURE FOR SOUTH ST. PAUL POLICE DEPARTMENT

The purpose of this procedure is to comply with CJIS Policy 5.7 as it relates to CJIS Data that may be found on computer and server hard drives, removable storage devices (i.e USB drives or flash drives, mobile tablets or laptops and smartphones). For the same reason that if you delete a file by accident, you can often recover it using data recovery software, also makes it difficult to truly destroy CJIS data when disposing of these devices. Therefore this procedure is designed to ensure that the South St. Paul Police Department and the South St. Paul IT working on behalf of the agency handle media containing CJIS data properly and in accordance to CJIS Policy.

Definition of Devices:

Devices include computers, servers, SAN or NAS's, tablets, smartphones, laptops, MDC's, and other devices that would store CJIS Data.

Definition of Media:

Media includes computer hard drives, SAN or NAS media, removable storage USB drives, backup tapes, CD's, and floppy disks.

Protection of Devices and Paper Media that contain CJIS Data:

- (a) All staff that handles paper media that contains CJIS Data shall ensure that these documents are store in Secured Locations so that people that are not authorized to handle the Agency's CJIS Data cannot access it;
- (b) Mobile Devices shall be handled with care in order to ensure they do not get lost or stolen;
- (c) Any loss or theft of Paper Media and/or Mobile Devices shall be immediately reported to Police Command Staff

Encryption for Devices in Unsecure Locations:

Any device that contains CJIS Data must be encrypted if it is located in an unsecure location. The South St. Paul Police Department shall accomplish this in the following manners:

- Squad Car MDC's shall use BitLocker or similar.
- SmartPhone or Mobile Tablets shall use an MDA, such as AirWatch or similar.

Electronic Media Disposal Procedure:

- (a) Whenever a device is about to be disposed of, that device shall be collected by South St. Paul IT Department;

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Policy

- (b) South St. Paul IT Department shall store the old devices in the IT Storage Room, which is a locked room;
- (c) South St. Paul IT Department shall remove the media or hard drives from the devices and store them in the in IT Storage Room
- (d) As needed, the South St. Paul IT shall get all stored hard drives ready for destruction, by inventorying their serial numbers in a spreadsheet which shall be dated and document the person(s) doing the inventory;
- (e) These hard drives shall then be destroyed using method, degaussing, FIPS-102, or professional destruction/shred service (i.e Shred-IT).
- (f) Upon Destruction, a Certificate of destruction shall be obtained from the destruction company;
- (g) The Certificate of Destruction and the Inventory spreadsheet shall be attached to each other and turned into the South St. Paul Police Department for documentation and retained for a period as defined in the City's retention policy.

Paper Media Disposal:

- (a) Paper Media Disposal refers to paper which is longer needed and contains CJIS Data;
- (b) Paper Media shall be temporarily disposed of in locked Paper Destruction Boxes;
- (c) As needed, these bins will be collected by professional destruction company and professionally destroyed;
- (d) Upon Destruction, a Certificate of destruction shall be obtained from the destruction company;
- (e) The Certificate of Destruction turned into the South St. Paul Police Department for documentation and retained for a period as defined in the City's retention policy.
- (f) Any other Paper Media shall be destroyed by a cross-cut quality shredder or better;

804.5 IDENTITY AND AUTHORIZATION PROCEDURES FOR SOUTH ST. POLICE DEPARTMENT

The purpose of this procedure is to ensure that the South St. Paul Police Department is able to identify each unique user who is authorized to access CJIS Data through any of the CJIS Data Systems that the South St. Paul Police Department uses. The second purpose of this procedure is to prove that the unique person accessing CJIS Data is really them, by using authentication methods such as passwords, PINs, and other Advance Authentication methods.

CJIS Data Systems:

The following systems contain or may contain some CJIS Data and should follow the procedures outlined in this document:

- CAD
- ProPhoenix RMS
- Tracker Evidence System

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Policy

- BCA Portals
- CJN eForms Reporting System
- Laserfiche
- LiveScan Fingerprint System
- Local Police File Server

The CJIS Account Administrator for each application shall be responsible for adding new users and disabling/deleting users once their access has been revoked.

Name Account Administrator for each:

- CAD – Police Command Staff
- ProPhoenix RMS – Police Command Staff
- Tracker Evidence System– Police Command Staff
- BCA Portals – TAC
- CJN eForms Reporting System – Police Command Staff
- Laserfiche South St. Paul IT Director or Designee
- LiveScan Fingerprint System – Police Command Staff
- Local Police File Server – South St. Paul IT Director or Designee

Unique Identification:

User Names must be unique. They can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier.

When accessing CJIS Data through a shared hosted system, such as a county dispatch CAD system, access/queries shall be logged with the Agency's originating agency identifier (ORI). The ORI shall be provided to the application owner during setup, when applicable.

The Agency must ensure that the application provider maintains an audit trail justifying each query of a subject.

Authentication Setup:

- CAD workstations– CAD Administrator shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;
- ProPhoenix RMS - RMS Administrator shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;
- Tracker Evidence System – The Evidence System Administrator shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;
- BCA Portals - TAC shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Policy

- Booking System – System Administrator shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;
- Fingerprint System – The LiveScan System Administrator shall issue a unique password for each user access this system
- CJN eForms Reporting System - System Administrator shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;
- Laserfiche - System Administrator shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;
- Local Police File Server - System Administrator shall issue a Temporary Password for setup, then the user shall change it to a unique password of their own;

Authenticator Criteria:

When creating authenticators, the following criteria shall be flowed in detail from the CJIS Policies:

- (a) Passwords – Follow CJIS Policy 5.6.2.1.1 for Passwords
- (b) Personal Identification Number (PIN) - Follow CJIS Policy 5.6.2.1.2 for PIN's
- (c) One-Time Passwords (OTP) - Follow CJIS Policy 5.6.2.1.3 for OTP's

Advance Authentication:

When accessing CJIS data from an unsecure location, users must also use 2-Factor-Authentication:

- (a) Access the CJIS systems via a VPN tunnel using the Cisco AnyConnect VPN/solution;
- (b) Police Command Staff authorizes the setup of the VPN token and then it is setup by the VPN System Administrator;
- (c) Each user will get a unique VPN username;
- (d) Each user will be assigned a unique hard or soft Entrust Token;
- (e) Each user will also get a unique PIN assigned to them for authentication;
- (f) Each device will be assigned a static IP upon authenticating;
- (g) Police Command Staff authorizes the Revocation of the VPN token and then it is terminated by the VPN System Administrator and the physical token is taken away from them;
- (h) If the token is lost Police Command Staff authorizes the reissue of a new VPN token and then it is setup by the VPN System Administrator;

804.6 ACCESS CONTROL PROCEDURE FOR SOUTH ST. PAUL POLICE DEPARTMENT

The purpose of this procedure is to limit the access to CJIS Data to only those that are authorized and need it to complete their job duties. In order to accomplish this, the following procedures shall be followed:

- (a) Users shall be granted access to CJIS Data according to the Identity and Authorization Procedure;

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Policy

- (b) Access and Permissions to CJIS Data shall be maintained by system administrators, information system security officers, maintainers, and system programmers, as determined by the South St. Paul Chief of Police;
- (c) Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system;
- (d) The South St. Paul Police Department shall limit access to CJIS Data to only authorized personnel with the need and the right to know;
- (e) Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is;

Access Control can be achieved by one or more of the following Criteria and Mechanisms:

- (a) Job assignment or function (i.e., the role) of the user seeking access;
- (b) Physical location;
- (c) Logical location;
- (d) Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside);
- (e) Time-of-day and day-of-week/month restrictions;
- (f) Access Control Lists (ACL's); and/or
- (g) Application user rights/roles;

When a user logs into a CJIS related system, the South St. Paul Police Department shall display a System Use Notification Banner that shall contain the following information:

- (a) The user is accessing a restricted information system;
- (b) System usage may be monitored, recorded, and subject to audit;
- (c) Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties;
- (d) Use of the system indicates consent to monitoring and recording; and
- (e) The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system;

Session Lockout:

- (a) All Devices shall have an automatic lockout after a minimum of 30 minutes of inactivity (except CAD Monitor Computer due to Dispatch necessities);

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Policy

- (b) Devices that are located in a Secure area (ie Squad Car MDC's) shall be exempt from this criteria for the purposes of officer safety;

Account Lockouts:

- (a) Systems shall enforce an automatic lockout after 5 unsuccessful login attempts, which shall last for a minimum of 10 minutes;
- (b) An account administrator may unlock the account with just cause;

Remote Access and Virtual Escorting:

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

- (a) The session shall be monitored at all times by an authorized escort;
- (b) The escort shall be familiar with the system/area in which the work is being performed;
- (c) The escort shall have the ability to end the session at any time;
- (d) The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path; and
- (e) The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

Concurrent Active Sessions:

- (a) For the purposes of officer safety, MDC's that are already logged into inside the Squad Cars (which is a Secure Location), shall not have a forced screen lockout; however
- (b) When an officer is logged into a device in a common Secured Location CJIS environment, when an officer is already logged into an MDC in a secure locked Squad Car, shall have a compensating control of an automatic screen lock after 30 minutes;

804.7 U.S. DEPARTMENT OF JUSTICE CRIMINAL JUSTICE INFORMATION SERVICES SECURITY POLICY

See attachment: [CJIS Security Policy_v5-7_20180816.pdf](#)

[Animal Control]

806.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for interacting with animals and responding to calls for service that involve animals.

806.2 [ANIMAL CONTROL] RESPONSIBILITIES

Animal control services are generally the primary responsibility of [Animal Control] and include the following:

- (a) Animal-related matters during periods when [Animal Control] is available.
- (b) Ongoing or persistent animal nuisance complaints. Such complaints may be scheduled, if reasonable, for handling during periods that [Animal Control] is available for investigation and resolution.
- (c) Follow-up on animal-related calls, such as locating owners of injured animals.

806.3 MEMBER RESPONSIBILITIES

Members who respond to or assist with animal-related calls for service should evaluate the situation and determine appropriate actions to control the situation.

Due to the hazards of handling animals without proper training and equipment, responding members generally should not attempt to capture and pick up any animal, but should keep the animal under observation until the arrival of appropriate assistance.

Members may consider acting before the arrival of such assistance when:

- (a) There is a threat to public safety.
- (b) An animal has bitten someone; members should take measures to confine the animal and prevent further injury.
- (c) An animal is creating a traffic hazard.
- (d) An animal is seriously injured.
- (e) The owner/handler has been arrested or is incapacitated. In such circumstances, the member should find appropriate placement for the animal.
 - 1. This is only necessary when the arrestee is expected to be in custody for a time period longer than would reasonably allow him/her to properly care for the animal.
 - 2. With the owner's consent, locating appropriate placement may require contacting relatives or neighbors to care for the animal.
 - 3. If no person can be found or the owner does not or cannot give consent, the animal should be taken to a designated animal care facility.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

[Animal Control]

806.4 DECEASED ANIMALS

When a member becomes aware of a deceased animal all reasonably attempts should be made to preliminarily determine if the death of the animal is related to criminal activity.

- (a) Deceased animals on public property should be removed, sealed in a plastic bag and properly disposed of by the responding member.
- (b) Members should not climb onto or under any privately owned structure for the purpose of removing a deceased animal.

806.5 INJURED ANIMALS

When a member becomes aware of an injured domesticated animal, all reasonable attempts shall be made to contact the owner or responsible handler.

If an owner or responsible handler cannot be located, the animal should be taken to a designated animal care facility.

806.6 DESTRUCTION OF ANIMALS

When it is necessary to use a firearm to euthanize a badly injured animal or stop an animal that poses an imminent threat to human safety, the Firearms Policy shall be followed. A badly injured animal shall only be euthanized with the approval of a supervisor.

806.7 POLICY

It is the policy of the South Saint Paul Police Department to be responsive to the needs of the community regarding animal-related issues. This includes enforcing local, state and federal laws relating to animals and appropriately resolving or referring animal-related problems, as outlined in this policy.

806.8 ANIMAL CRUELTY COMPLAINTS

Laws relating to the cruelty to animals should be enforced, including but not limited to (Minn. Stat. § 343.21 et seq.):

- (a) An investigation should be conducted on all reports of animal cruelty.
- (b) Legal steps should be taken to protect an animal that is in need of immediate care or protection from acts of cruelty (Minn. Stat. § 343.29).
 - 1. An officer may remove, shelter and care for any animal that is not properly sheltered from cold, heat or inclement weather, or any animal not properly fed and watered or provided with suitable food and drink, in circumstances that threaten the life of the animal.
 - 2. An animal taken into care during an animal cruelty investigation may be euthanized following a determination by a doctor of veterinary medicine that the animal is suffering and is beyond cure through reasonable care and treatment.

806.9 ANIMAL BITE REPORTS

Members investigating an animal bite should obtain as much information as possible for follow-up with the appropriate health or animal authorities. Efforts should be made to capture or otherwise

South Saint Paul Police Department

S Saint Paul PD Policy Manual

[Animal Control]

have the animal placed under control. Members should attempt to identify and notify the owner of the final disposition of the animal.

806.9.1 ANIMAL BITES TO HUMANS

Members should coordinate with appropriate animal authorities to ensure that animals who have bitten a human are quarantined for rabies observation as required by Minn. R. 1721.0580.

806.10 STRAY DOGS

If the dog has a license or can otherwise be identified, the owner should be contacted (Minn. Stat. § 343.29), if possible. If the owner is contacted, the dog should be released to the owner and a citation may be issued, if appropriate. If a dog is taken into custody, it shall be transported to the appropriate shelter/holding pen.

Members shall provide reasonable treatment to animals in their care (e.g., food, water, shelter).

806.11 DANGEROUS ANIMALS

In the event responding members cannot fulfill a request for service because an animal is difficult or dangerous to handle, the Sergeant will be contacted to determine available resources, including requesting the assistance of animal control services from an allied agency.

806.12 PUBLIC NUISANCE CALLS RELATING TO ANIMALS

Members should diligently address calls related to nuisance animals (e.g., barking dogs), as such calls may involve significant quality of life issues.

CJIS Access, Maintenance, and Security

807.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use, maintenance, and security of department systems that access Criminal Justice Information.

807.1.1 DEFINITIONS

Definitions related to this policy include:

Criminal Justice Information (CJI) - Data provided by FBI Criminal Justice Information Services (CJIS) that is necessary for law enforcement agencies to perform their mission and enforce the laws (e.g., biometric, identity history, person, organization, case/incident history data).

Security incident - Any incident that compromises the security of CJI or systems that access CJI. Examples include but are not limited to unauthorized use of legitimate code or credentials within department systems, email communications that contain malicious code, data breaches, signaling to external systems, and unauthorized exporting of information.

807.2 POLICY

It is the policy of the South Saint Paul Police Department to maintain the security, confidentiality, and integrity of its information systems that access CJI by collaborating with appropriate state and federal agencies to implement the applicable established protocols.

807.3 CJIS COORDINATOR

The Chief of Police shall appoint a CJIS coordinator, who shall be responsible for the South Saint Paul Police Department's adherence to FBI CJIS Security Policy requirements.

The CJIS coordinator shall establish procedures necessary to govern the department's use, maintenance, and security of systems that access CJI as described in this policy.

807.3.1 CJIS COORDINATOR RESPONSIBILITIES

The responsibilities of the CJIS coordinator include but are not limited to:

- (a) Coordinating with others, such as the information technology or legal departments, as appropriate, to maintain department compliance with FBI CJIS Security Policy requirements and the Minnesota Bureau of Criminal Apprehension (BCA).
- (b) Managing member accounts with access to CJI, including:
 - 1. Creating, enabling, modifying, disabling, and removing member accounts in accordance with this policy and the FBI CJIS Security Policy.
 - 2. Configuring member accounts in accordance with federal and state requirements (e.g., limiting unsuccessful login attempts).
 - 3. Reviewing member accounts for compliance with legal and policy requirements at least annually.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Access, Maintenance, and Security

- (c) Overseeing the maintenance, repair, and replacement of CJI systems and system components in accordance with manufacturer or vendor specifications and/or department requirements, including:
 - 1. Maintaining a list of organizations and personnel approved by the Chief of Police to perform maintenance on CJI systems.
 - 2. Approving, scheduling, documenting, and monitoring all maintenance and diagnostic activities, whether performed on-site, remotely, or off-site, and maintaining records.
 - 3. Verifying that non-escorted personnel performing maintenance on any CJI system or terminal possess the required access authorizations, and designating members who have the required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
 - 4. Maintaining records for all system maintenance and diagnostic activities.
- (d) Monitoring department systems that have access to CJI to ensure compliance with applicable laws and this policy; developing processes to detect, identify, and correct flaws in software and firmware; and conducting security updates as necessary.
- (e) Providing for the security of hardware that includes provisions for the following:
 - 1. How hardware is to be brought into and taken out of department facilities
 - 2. Physical security of hardware within department facilities
 - 3. Physical security of areas containing network connections and transmission lines, including monitored access
- (f) Implementing and carrying out the department Incident Response Plan, including:
 - 1. Tracking and documenting all suspected or actual security incidents related to CJI in an appropriate manner.
 - 2. Directing annual testing of the department's information security incident response capabilities using tabletop or walk-through exercises, simulations, or other types of testing.
 - 3. Making the appropriate notifications outside of the Department (see the Records Maintenance and Release Policy for additional guidance).
 - 4. Providing information on security incidents to any third-party software developers or vendors as appropriate.
- (g) Protecting digital and non-digital media that contain CJI, including physical security, transportation, destruction/sanitization, and documentation requirements.
- (h) Developing and updating department information security and privacy literacy training and incident response training as required by policy.
- (i) Maintaining audit records in accordance with the established records retention schedule, but in no event for less than one year.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Access, Maintenance, and Security

- (j) Managing the development, documentation, and dissemination of procedures for the following:
 - 1. Awareness and training
 - 2. Incident response
 - 3. Audit and accountability
 - 4. Access control
 - 5. Identification and authentication
 - 6. Configuration management
 - 7. Media protection
 - 8. Physical and environmental protection
 - 9. System and communications protection
 - 10. System and information integrity
 - 11. Maintenance
 - 12. Security and privacy planning
 - 13. Contingency planning
 - 14. Risk assessment
- (k) Reviewing this policy and related procedures as required by the FBI CJIS Security Policy and proposing updates as needed to the Chief of Police.

807.4 MEMBER RESPONSIBILITIES

All members of the Department shall be committed to detecting information security incidents and making the appropriate notifications.

Any member who suspects that there may have been unauthorized access, disclosure, or other compromise of CJI shall report their suspicions in accordance with the Incident Response Plan within one hour of the discovery.

Personally owned devices or systems and publicly accessible systems shall not be used to access, process, store, or transmit CJI.

807.5 SUPERVISOR RESPONSIBILITIES

Supervisors shall notify the CJIS coordinator when the account access of a member they supervise needs to be modified, disabled, or removed for any reason, such as resignation, termination, or change of duties.

807.6 MEMBER ACCOUNTS

Department accounts used to access CJI shall only be created upon approval of the Chief of Police or the authorized designee.

Member accounts shall be disabled within one week of any of the following:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Access, Maintenance, and Security

- (a) The account has expired.
- (b) The account is no longer associated with a member.
- (c) The account is found to be in violation of this policy.
- (d) The account has been inactive for 90 calendar days.

If any threat to the confidentiality, integrity, or availability of CJI related to a specific member account is detected, the CJIS coordinator or designated member shall disable the account within 30 minutes of the discovery.

807.6.1 ACCESS AUTHORIZATION

Access authorization for systems transmitting, receiving, using, or storing CJI shall be based on the principle of least privilege as follows:

- (a) Members shall only be granted access authorizations that are necessary to accomplish assigned department tasks.
- (b) Accounts with security privileges shall only be authorized for members with an operational need for the privileges. Privileged functions shall be logged as they are executed.
- (c) Non-privileged members shall not be allowed to execute privileged functions.

807.6.2 ACCOUNT REVIEW ACTIVITIES

At least annually, the CJIS coordinator shall review member accounts for compliance with policy and applicable laws. The CJIS coordinator shall validate account privileges and remove or reassign them as necessary to accurately reflect the department mission and law enforcement needs.

807.7 MEDIA PROTECTION

Access to media containing CJI shall be restricted to authorized members and stored within physically secured locations or controlled areas, in accordance with the FBI CJIS Security Policy.

Digital media (e.g., flash drives, external or removable hard disk drives, compact discs) containing CJI shall be encrypted. Personally owned digital media devices or digital media devices with no identifiable owner shall not be used on department systems that store, process, or transmit CJI.

Non-digital media (e.g., paper files, printed pages, microfilm) containing CJI should be enclosed in an opaque folder or container if they are to be transported outside of physically secure locations or controlled areas. Media containing CJI shall not be left unattended outside of a physically secure location.

Transportation and transfers of media containing CJI shall be documented.

807.7.1 MEDIA DISPOSAL AND RELEASE

Digital media containing CJI shall be overwritten at least three times or degaussed (i.e., erased) prior to being disposed of, released from department control, or released for reuse. Inoperable digital media devices, such as hard drives or solid-state drives that cannot be accessed to

South Saint Paul Police Department

S Saint Paul PD Policy Manual

CJIS Access, Maintenance, and Security

overwrite the data, shall be physically destroyed. When non-digital media is no longer needed for investigative or security purposes, it shall be destroyed by crosscut shredding or incineration.

807.8 SYSTEM AND INFORMATION INTEGRITY

The integrity of department CJI systems shall be protected through the implementation of appropriate controls such as:

- (a) Flaw remediation.
- (b) System monitoring.
- (c) Security alerts, advisories, and directives.
- (d) Software, firmware, and information integrity controls.
- (e) Spam protection.

807.9 INCIDENT RESPONSE PLAN

[Insert your agency's Incident Response Plan consistent with CJIS 5.3 IR-4, IR-7, and IR-8 – see the Guide Sheet for additional guidance.]

807.10 SECURITY AWARENESS TRAINING

Members with physical or electronic access to CJI or CJI systems shall complete security awareness training appropriate to their assigned roles and responsibilities and shall certify their understanding by signing a formal Security Awareness Training Acknowledgement. Training shall include information security and privacy literacy training, security incident response training, and a review of this policy and related procedures.

Security awareness training shall be completed prior to accessing any CJI data or system and at least annually thereafter. Additional training shall be completed as required following any changes to CJI systems and for any member involved in a security incident within 30 days of the event.

Individual training records shall be maintained in accordance with the established records retention schedule, but in no event for less than three years.

The department's CJIS training shall be reviewed for any necessary updates or changes annually and following any security incident or change in a CJI system or the FBI CJIS Security Policy.

807.11 SANCTIONS

Failure to adhere to policies and procedures pertaining to CJI shall result in disciplinary action, up to and including termination. Misuse of or failure to secure CJI may also result in temporary or permanent restrictions in the use of CJI. Intentional misuse of CJI may also be prosecutable under applicable laws.

Chapter 9 - Custody

Temporary Custody of Adults

900.1 PURPOSE AND SCOPE

This policy provides guidelines to address the health and safety of adults taken into temporary custody by members of the South Saint Paul Police Department for processing prior to being released or transferred to a housing or other type of facility.

Temporary custody of juveniles is addressed in the Temporary Custody of Juveniles Policy. Juveniles will not be permitted where adults who are in custody are being held.

Custodial searches are addressed in the Custodial Searches Policy.

Additional guidance for transferring persons in custody to another facility or court is provided in the Transporting Persons in Custody Policy.

900.1.1 DEFINITIONS

Definitions related to this policy include:

Holding cell/cell - Any locked enclosure for the custody of an adult or any other enclosure that prevents the occupants from being directly visually monitored at all times by a member of the Department.

Safety checks - Direct, visual observation by a member of this department performed at random intervals, within time frames prescribed in this policy, to provide for the health and welfare of adults in temporary custody.

Temporary custody - The time period an adult is in custody at the South Saint Paul Police Department prior to being released or transported to a housing or other type of facility.

900.1.2 DETAINABLE PRISONERS

Arrestees who fall within the following classifications may be detained in the South Saint Paul Police Department Temporary Holding Facility:

- (a) Posting of bail.
- (b) Release on Own Recognizance (O.R.).
- (c) Release on citation in accordance with the Cite and Release Policy in this manual.
- (d) Transportation to the county jail.
- (e) In-custody interview or other investigation.

900.2 POLICY

The South Saint Paul Police Department is committed to releasing adults from temporary custody as soon as reasonably practicable and to keeping adults safe while in temporary custody at the Department. Adults should be in temporary custody only for as long as reasonably necessary for investigation, processing, transfer or release.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

900.3 GENERAL CRITERIA AND SUPERVISION

No adult should be in temporary custody for longer than four hours (Minn. R. 2945.0100; Minn. R. 2945.0120).

900.3.1 INDIVIDUALS WHO SHOULD NOT BE IN TEMPORARY CUSTODY

Individuals who exhibit certain behaviors or conditions should not be in temporary custody at the South Saint Paul Police Department, but should be transported to a jail facility, a medical facility or other type of facility as appropriate. These include:

- (a) Any individual who is unconscious or has been unconscious while being taken into custody or while being transported.
- (b) Any individual who has a medical condition, including pregnancy, or who may require medical attention, supervision or medication while in temporary custody.
- (c) Any individual who is seriously injured.
- (d) Individuals who are a suspected suicide risk (see the Civil Commitments Policy).
 - 1. If the officer taking custody of an individual believes that he/she may be a suicide risk, the officer shall ensure continuous direct supervision until evaluation, release or a transfer to an appropriate facility is completed.
- (e) Individuals who are obviously in crisis, as defined in the Crisis Intervention Incidents Policy.
- (f) Individuals who are under the influence of alcohol, a controlled substance or any substance to the degree that may require medical attention, or who have ingested any substance that poses a significant risk to their health, whether or not they appear intoxicated.
- (g) Any individual who has exhibited extremely violent or continuously violent behavior.
- (h) Any individual who has claimed, is known to be afflicted with, or displays symptoms of any communicable disease that poses an unreasonable exposure risk.
- (i) Any individual with a prosthetic or orthopedic device where removal of the device would be injurious to his/her health or safety.

Officers taking custody of a person who exhibits any of the above conditions should notify a supervisor of the situation. These individuals should not be in temporary custody at the Department unless they have been evaluated by a qualified medical or mental health professional, as appropriate for the circumstances.

900.3.2 SUPERVISION IN TEMPORARY CUSTODY

An authorized department member capable of supervising shall be present at all times when an individual is held in temporary custody. The member responsible for supervising should not have other duties that could unreasonably conflict with his/her supervision. Any individual in custody must be able to summon the supervising member if needed. If the person in custody is deaf or hard of hearing or cannot speak, accommodations shall be made to provide this ability.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

At least one female department member should be present when a female adult is in temporary custody. In the event that none is readily available, the female in custody should be transported to another facility or released pursuant to another lawful process.

Absent exigent circumstances, such as a medical emergency or a violent subject, members should not enter the cell of a person of the opposite sex unless a member of the same sex as the person in custody is present.

No individual in custody shall be permitted to supervise, control or exert any authority over other individuals in custody.

900.3.3 ENTRY RESTRICTIONS

Entry into any location where a person is held in custody should be restricted to:

- (a) Authorized members entering for official business purposes.
- (b) Emergency medical personnel when necessary.
- (c) Any other person authorized by the Sergeant.

When practicable, more than one authorized member should be present for entry into a location where a person is held in custody for security purposes and to witness interactions.

900.4 INITIATING TEMPORARY CUSTODY

The officer responsible for an individual in temporary custody should evaluate the person for any apparent chronic illness, disability, vermin infestation, possible communicable disease or any other potential risk to the health or safety of the individual or others. The officer should specifically ask if the individual is contemplating suicide and evaluate him/her for obvious signs or indications of suicidal intent.

The receiving officer should ask the arresting officer if there is any statement, indication or evidence surrounding the individual's arrest and transportation that would reasonably indicate the individual is at risk for suicide or critical medical care. If there is any suspicion the individual may be suicidal, he/she shall be transported to the City jail or the appropriate mental health facility.

The officer should promptly notify the Sergeant of any conditions that may warrant immediate medical attention or other appropriate action. The Sergeant shall determine whether the individual will be placed in a cell, immediately released or transported to jail or other facility.

900.4.1 SCREENING AND PLACEMENT

The officer responsible for an individual in custody shall:

- (a) Advise the Sergeant of any significant risks presented by the individual (e.g., suicide risk, health risk, violence).
- (b) Evaluate the following issues against the stated risks in (a) to determine the need for placing the individual in a single cell:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

1. Consider whether the individual may be at a high risk of being sexually abused based on all available known information (28 CFR 115.141) or whether the person is facing any other identified risk.
 2. Provide any individual identified as being at a high risk for sexual or other victimization with heightened protection. This may include (28 CFR 115.113; 28 CFR 115.141):
 - (a) Continuous, direct sight and sound supervision.
 - (b) Single-cell placement in a cell that is actively monitored on video by a member who is available to immediately intervene.
 3. Ensure individuals are separated according to severity of the crime (e.g., felony or misdemeanor).
 4. Ensure males and females are separated by sight and sound when in cells.
 5. Ensure restrained individuals are not placed in cells with unrestrained individuals.
- (c) Ensure that those confined under civil process or for civil causes are kept separate from those who are in temporary custody pending criminal charges.
- (d) Ensure separation, as appropriate, based on other factors, such as age, criminal sophistication, assaultive/non-assaultive behavior, mental state, disabilities and sexual orientation.

900.4.2 CONSULAR NOTIFICATION

Consular notification may be mandatory when certain foreign nationals are arrested. The Patrol Division Commander will ensure that the U.S. Department of State's list of countries and jurisdictions that require mandatory notification is readily available to department members. There should also be a published list of foreign embassy and consulate telephone and fax numbers, as well as standardized notification forms that can be transmitted and then retained for documentation. Prominently displayed signs informing foreign nationals of their rights related to consular notification should also be posted in areas used for the temporary custody of adults.

Department members assigned to process a foreign national shall:

- (a) Inform the individual without delay he/she may have his/her consular officers notified of the arrest or detention and may communicate with them.
 1. This notification should be documented.
- (b) Determine whether the foreign national's country is on the U.S. Department of State's mandatory notification list.
 1. If the country is on the mandatory notification list, then:
 - (a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.
 - (b) Tell the individual this notification has been made and inform him/her without delay he/she may communicate with consular officers.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

- (c) Forward any communication from the individual to his/her consular officers without delay.
 - (d) Document all notifications to the embassy or consulate and retain the faxed notification and any fax confirmation for the individual's file.
- 2. If the country is not on the mandatory notification list and the individual requests his/her consular officers be notified, then:
 - (a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.
 - (b) Forward any communication from the individual to his/her consular officers without delay.

900.5 SAFETY, HEALTH AND OTHER PROVISIONS

900.5.1 TEMPORARY CUSTODY LOGS

Any time an individual is in temporary custody at the South Saint Paul Police Department, the custody shall be promptly and properly documented in a custody log, including:

- (a) Identifying information about the individual, including his/her name.
- (b) Date and time of arrival at the Department.
- (c) Any charges for which the individual is in temporary custody and any case number.
- (d) Time of all safety checks.
- (e) Any medical and other screening requested and completed.
- (f) Any emergency situations or unusual incidents.
- (g) Any other information that may be required by other authorities, such as compliance inspectors.
- (h) Date and time of release from the South Saint Paul Police Department.

The Sergeant should initial the log to approve the temporary custody and should also initial the log when the individual is released from custody or transferred to another facility.

The Sergeant should make periodic checks to ensure all log entries and safety and security checks are made on time.

900.5.2 TEMPORARY CUSTODY REQUIREMENTS

Members monitoring or processing anyone in temporary custody shall ensure:

- (a) Safety checks and significant incidents/activities are noted on the log.
- (b) Individuals in custody are informed they will be monitored at all times, except when using the toilet.
 - 1. There shall be no viewing devices, such as peep holes or mirrors, of which the individual is not aware.
 - 2. This does not apply to surreptitious and legally obtained recorded interrogations.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

- (c) There is reasonable access to toilets and wash basins.
- (d) There is reasonable access to a drinking fountain or water.
- (e) There are reasonable opportunities to stand and stretch, particularly if handcuffed or otherwise restrained.
- (f) There is privacy during attorney visits.
- (g) Those in temporary custody are generally permitted to remain in their personal clothing unless it is taken as evidence or is otherwise unsuitable or inadequate for continued wear while in custody.
- (h) Clean blankets are provided as reasonably necessary to ensure the comfort of an individual.
 - 1. The supervisor should ensure that there is an adequate supply of clean blankets.
- (i) Adequate shelter, heat, light and ventilation are provided without compromising security or enabling escape.
- (j) Adequate furnishings are available, including suitable chairs or benches.

900.5.3 MEDICAL CARE

First-aid equipment and basic medical supplies should be available to department members. At least one member who has current certification in basic first aid and CPR should be on-duty at all times.

Should a person in custody be injured or become ill, appropriate medical assistance should be sought. A supervisor should meet with those providing medical aid at the facility to allow access to the person. Members shall comply with the opinion of medical personnel as to whether an individual in temporary custody should be transported to the hospital. If the person is transported while still in custody, he/she will be accompanied by an officer.

Those who require medication while in temporary custody should not be at the South Saint Paul Police Department. They should be released or transferred to another facility as appropriate.

900.5.4 ORTHOPEDIC OR PROSTHETIC APPLIANCE

Subject to safety and security concerns, individuals shall be permitted to retain an orthopedic or prosthetic appliance. However, if the appliance presents a risk of bodily harm to any person or is a risk to the security of the facility, the appliance may be removed from the individual unless its removal would be injurious to his/her health or safety.

Whenever a prosthetic or orthopedic appliance is removed, the Sergeant shall be promptly apprised of the reason. It shall be promptly returned when it reasonably appears any risk no longer exists.

900.5.5 TELEPHONE CALLS

Every individual in temporary custody should be allowed to make a reasonable number of completed telephone calls as soon as possible after arrival.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

- (a) Telephone calls may be limited to local calls, except that long-distance calls may be made by the individual at his/her own expense.
 - 1. The Department should pay the cost of any long-distance calls related to arranging for the care of a child or dependent adult (see the Child and Dependent Adult Safety Policy).
- (b) The individual should be given sufficient time to contact whomever he/she desires and to make any necessary arrangements, including child or dependent adult care, or transportation upon release.
 - 1. Telephone calls are not intended to be lengthy conversations. The member assigned to monitor or process the individual may use his/her judgment in determining the duration of the calls.
- (c) Calls between an individual in temporary custody and his/her attorney shall be deemed confidential and shall not be monitored, eavesdropped upon or recorded.

900.5.6 RELIGIOUS ACCOMMODATION

Subject to available resources, safety and security, the religious beliefs and needs of all individuals in custody should be reasonably accommodated. Requests for religious accommodation should generally be granted unless there is a compelling security or safety reason and denying the request is the least restrictive means available to ensure security or safety. The responsible supervisor should be advised any time a request for religious accommodation is denied.

Those who request to wear headscarves or simple head coverings for religious reasons should generally be accommodated absent unusual circumstances. Head coverings shall be searched before being worn.

Individuals wearing headscarves or other approved coverings shall not be required to remove them while in the presence of or while visible to the opposite sex if they so desire. Religious garments that substantially cover the individual's head and face may be temporarily removed during the taking of any photographs.

900.5.7 FIREARMS AND OTHER SECURITY MEASURES

Firearms and other weapons and control devices shall not be permitted in secure areas where individuals are in custody or are processed. They should be properly secured outside of the secure area. An exception may occur only during emergencies, and upon approval of a supervisor.

All perimeter doors to secure areas shall be kept locked at all times except during routine cleaning when no individuals in custody are present or in the event of an emergency, such as an evacuation.

900.5.8 FINGERPRINTING

Once the person has been taken into temporary custody the arresting officer should ensure the following are taken:

- (a) Finger and thumb prints
- (b) Photographs

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

- (c) Distinctive physical mark identification data
- (d) Information on any known aliases or street names
- (e) Any other identification data requested or required by the Bureau of Criminal Apprehension

The Sergeant should ensure fingerprints and other identifying information is entered into the searchable database managed by the Bureau of Criminal Apprehension (Minn. Stat. § 299C.10, Subd. 1).

900.6 USE OF RESTRAINT DEVICES

Individuals in custody may be handcuffed in accordance with the Handcuffing and Restraints Policy. Unless an individual presents a heightened risk handcuffs should generally be removed when the person is in a cell.

The use of restraints other than handcuffs or leg irons generally should not be used for individuals in temporary custody at the South Saint Paul Police Department unless the person presents a heightened risk and then only in compliance with the Handcuffing and Restraints Policy.

Individuals in restraints shall be kept away from other unrestrained individuals in custody and monitored to protect them from abuse.

900.6.1 PREGNANT ADULTS

Women who are known to be pregnant should be restrained in accordance with the Handcuffing and Restraints Policy.

900.7 PERSONAL PROPERTY

The personal property of an individual in temporary custody should be removed, inventoried and processed as provided in the Custodial Searches Policy unless the individual requests a different disposition. For example an individual may request property (i.e., cash, car or house keys, medications) be released to another person. A request for the release of property to another person must be made in writing. Release of the property requires the recipient's signature on the appropriate form.

Upon release of an individual from temporary custody his/her items of personal property shall be compared with the inventory, and he/she shall sign a receipt for the property's return. If the individual is transferred to another facility or court, the member transporting the individual is required to obtain the receiving person's signature as notice of receipt. The Department shall maintain a copy of the property receipt.

The Sergeant shall be notified whenever an individual alleges there is a shortage or discrepancy regarding his/her property. The Sergeant shall attempt to prove or disprove the claim.

All intangible personal property that is unclaimed for more than three years is presumed abandoned (Minn. Stat. § 345.38).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

900.8 HOLDING CELLS

A thorough inspection of a cell shall be conducted before placing an individual into the cell to ensure there are no weapons or contraband and that the cell is clean and sanitary. An inspection also should be conducted when he/she is released. Any damage noted to the cell should be photographed and documented. The following requirements shall apply:

- (a) The individual shall be searched (see the Custodial Searches Policy), and anything that could create a security or suicide risk such as contraband, hazardous items, belts, shoes or shoelaces and jackets, shall be removed.
- (b) The individual shall constantly be monitored by an audio/video system during the entire custody.
- (c) The individual shall have constant auditory access to department members.
- (d) The individual's initial placement into and removal from a locked enclosure shall be logged.
- (e) Safety checks by department members shall occur no less than every 15 minutes.
 - (a) Safety checks should be at varying times.
 - (b) All safety checks shall be logged.
 - (c) The safety check should involve questioning the individual as to his/her well-being.
 - (d) Individuals who are sleeping or apparently sleeping should be awakened.
 - (e) Requests or concerns of the individual should be logged.

900.9 SUICIDE ATTEMPT, DEATH, OR SERIOUS INJURY

The Patrol Division Commander will ensure procedures are in place to address any suicide attempt, death, or serious injury of any individual in temporary custody at the South Saint Paul Police Department. The procedures should include (Minn. Stat. § 390.11, Subd. 1(6)):

- (a) Immediate request for emergency medical assistance if appropriate.
- (b) Immediate notification of the Sergeant, Chief of Police, and Investigation Division Commander.
- (c) Notification of the spouse, next of kin, or other appropriate person.
- (d) Notification of the appropriate prosecutor.
- (e) Notification of the City Attorney.
- (f) Notification of the Medical Examiner.
- (g) Evidence preservation.

900.10 RELEASE AND/OR TRANSFER

When an individual is released or transferred from custody, the member releasing the individual should ensure the following:

- (a) All proper reports, forms, and logs have been completed prior to release.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Custody of Adults

- (b) A check has been made to ensure the individual is not reported as missing and does not have outstanding warrants.
- (c) It has been confirmed the correct individual is being released or transported.
- (d) All property, except evidence, contraband, or dangerous weapons, has been returned to, or sent with, the individual.
- (e) All pertinent documentation accompanies the individual being transported to another facility (e.g., copies of booking forms, medical records, an itemized list of property, warrant copies).
- (f) The individual is not permitted in any nonpublic areas of the South Saint Paul Police Department unless escorted by a member of the Department.
- (g) Any known threat or danger the individual may pose (e.g., escape risk, suicide potential, medical condition) is documented, and the documentation transported with the individual if the individual is being sent to another facility.
- (h) Transfers between facilities or other entities, such as a hospital, should be accomplished with a custodial escort of the same sex as the person being transferred to assist with the person's personal needs as reasonable.
- (i) Transfers that exceed 100 miles shall be accomplished with a custodial escort of the same sex as the individual being transferred unless video and audio recording equipment is installed in the vehicle that is capable of recording the transferee for the entire duration of the transfer (Minn. Stat. § 631.412).
 - (a) Recordings of such transfer shall be maintained by the Department for at least 12 months after the date of the transfer.

900.11 ASSIGNED ADMINISTRATOR

The Patrol Division Commander will ensure any reasonably necessary supplemental procedures are in place to address the following issues:

- (a) General security
- (b) Key control
- (c) Sanitation and maintenance
- (d) Emergency medical treatment
- (e) Escapes
- (f) Evacuation plans
- (g) Fire- and life-safety
- (h) Disaster plans
- (i) Building and safety code compliance

900.12 TRAINING

Department members should be trained and familiar with this policy and any supplemental procedures.

Custodial Searches

901.1 PURPOSE AND SCOPE

This policy provides guidance regarding searches of individuals in custody. Such searches are necessary to eliminate the introduction of contraband, intoxicants or weapons into the South Saint Paul Police Department facility. Such items can pose a serious risk to the safety and security of department members, individuals in custody, contractors and the public.

Nothing in this policy is intended to prohibit the otherwise lawful collection of evidence from an individual in custody.

901.1.1 DEFINITIONS

Definitions related to this policy include:

Custody search - An in-custody search of an individual and of his/her property, shoes and clothing, including pockets, cuffs and folds on the clothing, to remove all weapons, dangerous items and contraband.

Physical body cavity search - A search that includes a visual inspection and may include a physical intrusion into a body cavity. Body cavity means the stomach or rectal cavity of an individual, and the vagina of a female person.

Strip search - A search that requires an individual to remove or rearrange some or all of his/her clothing to permit a visual inspection of the underclothing, breasts, buttocks, anus or outer genitalia. This includes monitoring an individual who is changing clothes, where his/her underclothing, buttocks, genitalia or female breasts are visible.

901.2 POLICY

All searches shall be conducted with concern for safety, dignity, courtesy, respect for privacy and hygiene, and in compliance with policy and law to protect the rights of those who are subject to any search.

Searches shall not be used for intimidation, harassment, punishment or retaliation.

901.3 FIELD AND TRANSPORTATION SEARCHES

An officer should conduct a custody search of an individual immediately after his/her arrest, when receiving an individual from the custody of another, and before transporting a person who is in custody in any department vehicle.

Whenever practicable, a custody search should be conducted by an officer of the same sex as the person being searched. If an officer of the same sex is not reasonably available, a witnessing officer should be present during the search.

901.4 SEARCHES AT POLICE FACILITIES

Custody searches shall be conducted on all individuals in custody, upon entry to the South Saint Paul Police Department facilities. Except in exigent circumstances, the search should be

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Custodial Searches

conducted by a member of the same sex as the individual being searched. If a member of the same sex is not available, a witnessing member must be present during the search.

Custody searches should also be conducted any time an individual in custody enters or re-enters a secure area, or any time it is reasonably believed that a search is necessary to maintain the safety and security of the facility.

901.4.1 PROPERTY

Members shall take reasonable care in handling the property of an individual in custody to avoid discrepancies or losses. Property retained for safekeeping shall be kept in a secure location until the individual is released or transferred.

Some property may not be accepted by a facility or agency that is taking custody of an individual from this department, such as weapons or large items. These items should be retained for safekeeping in accordance with the Property and Evidence Policy.

All property shall be inventoried by objective description (this does not include an estimated value). The individual from whom it was taken shall be required to sign the completed inventory. If the individual's signature cannot be obtained, the inventory shall be witnessed by another department member. The inventory should include the case number, date, time, member's South Saint Paul Police Department identification number and information regarding how and when the property may be released.

901.4.2 VERIFICATION OF MONEY

All money shall be counted in front of the individual from whom it was received. When possible, the individual shall initial the dollar amount on the inventory. Additionally, all money should be placed in a separate envelope and sealed. Negotiable checks or other instruments and foreign currency should also be sealed in an envelope with the amount indicated but not added to the cash total. All envelopes should clearly indicate the contents on the front. The department member sealing it should place his/her initials across the sealed flap. Should any money be withdrawn or added, the member making such change shall enter the amount below the original entry and initial it. The amount of money in the envelope should always be totaled and written on the outside of the envelope.

901.5 STRIP SEARCHES

No individual in temporary custody at any South Saint Paul Police Department facility shall be subjected to a strip search unless there is reasonable suspicion based upon specific and articulable facts to believe the individual has a health condition requiring immediate medical attention or is concealing a weapon or contraband. Factors to be considered in determining reasonable suspicion include, but are not limited to:

- (a) The detection of an object during a custody search that may be a weapon or contraband and cannot be safely retrieved without a strip search.
- (b) Circumstances of a current arrest that specifically indicate the individual may be concealing a weapon or contraband.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Custodial Searches

1. A felony arrest charge or being under the influence of a controlled substance should not suffice as reasonable suspicion absent other facts.
- (c) Custody history (e.g., past possession of contraband while in custody, assaults on department members, escape attempts).
- (d) The individual's actions or demeanor.
- (e) Criminal history (i.e., level of experience in a custody setting).

No transgender or intersex individual shall be searched or examined for the sole purpose of determining the individual's genital status. If the individual's genital status is unknown, it may be determined during conversations with the person, by reviewing medical records, or as a result of a broader medical examination conducted in private by a medical practitioner (28 CFR 115.115).

901.5.1 STRIP SEARCH PROCEDURES

Strip searches at South Saint Paul Police Department facilities shall be conducted as follows (28 CFR 115.115):

- (a) Written authorization from the Sergeant shall be obtained prior to the strip search.
- (b) All members involved with the strip search shall be of the same sex as the individual being searched, unless the search is conducted by a medical practitioner.
- (c) All strip searches shall be conducted in a professional manner under sanitary conditions and in a secure area of privacy so that it cannot be observed by those not participating in the search. The search shall not be reproduced through a visual or sound recording.
- (d) Whenever possible, a second member of the same sex should also be present during the search, for security and as a witness to the finding of evidence.
- (e) Members conducting a strip search shall not touch the breasts, buttocks, or genitalia of the individual being searched.
- (f) The primary member conducting the search shall prepare a written report to include:
 1. The facts that led to the decision to perform a strip search.
 2. The reasons less intrusive methods of searching were not used or were insufficient.
 3. The written authorization for the search, obtained from the Sergeant.
 4. The name of the individual who was searched.
 5. The name and sex of the members who conducted the search.
 6. The name, sex, and role of any person present during the search.
 7. The time and date of the search.
 8. The place at which the search was conducted.
 9. A list of the items, if any, that were recovered.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Custodial Searches

10. The facts upon which the member based their belief that the individual was concealing a weapon or contraband.
- (g) No member should view an individual's private underclothing, buttocks, genitalia, or female breasts while that individual is showering, performing bodily functions, or changing clothes, unless the individual otherwise qualifies for a strip search. However, if serious hygiene or health issues make it reasonably necessary to assist the individual with a shower or a change of clothes, a supervisor should be contacted to ensure reasonable steps are taken to obtain the individual's consent and/or otherwise protect the individual's privacy and dignity.

901.5.2 SPECIAL CIRCUMSTANCE FIELD STRIP SEARCHES

A strip search may be conducted in the field only with Sergeant authorization and only in exceptional circumstances, such as when:

- (a) There is probable cause to believe that the individual is concealing a weapon or other dangerous item that cannot be recovered by a more limited search.
- (b) There is probable cause to believe that the individual is concealing controlled substances or evidence that cannot be recovered by a more limited search, and there is no reasonable alternative to ensure the individual cannot destroy or ingest the substance during transportation.

These special-circumstance field strip searches shall only be authorized and conducted under the same restrictions as the strip search procedures in this policy, except that the Sergeant authorization does not need to be in writing.

901.6 PHYSICAL BODY CAVITY SEARCH

Physical body cavity searches shall be subject to the following:

- (a) No individual shall be subjected to a physical body cavity search without written approval of the Sergeant and only upon a search warrant or approval of legal counsel. A copy of any search warrant and the results of the physical body cavity search shall be included with the related reports and made available, upon request, to the individual or authorized representative (except for those portions of the warrant ordered sealed by a court).
- (b) Only a physician may conduct a physical body cavity search.
- (c) Except for the physician conducting the search, persons present must be of the same sex as the individual being searched. Only the necessary department members needed to maintain the safety and security of the medical personnel shall be present.
- (d) Privacy requirements, including restricted touching of body parts and sanitary condition requirements, are the same as required for a strip search.
- (e) All such searches shall be documented, including:
 1. The facts that led to the decision to perform a physical body cavity search of the individual.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Custodial Searches

2. The reasons less intrusive methods of searching were not used or were insufficient.
 3. The Sergeant's approval.
 4. A copy of the search warrant.
 5. The time, date, and location of the search.
 6. The medical personnel present.
 7. The names, sex, and roles of any department members present.
 8. Any contraband or weapons discovered by the search.
- (f) A copy of the written authorization shall be retained and shall be provided to the individual who was searched or other authorized representative upon request.

901.7 TRAINING

The Support Services Commander shall ensure members have training that includes (28 CFR 115.115):

- (a) Conducting searches of cross-gender individuals.
- (b) Conducting searches of transgender and intersex individuals.
- (c) Conducting searches in a professional and respectful manner, and in the least intrusive manner possible, consistent with security needs.

901.8 JUVENILES

No juvenile should be subjected to a strip search or a physical body cavity search at the Department.

The Chief of Police or the authorized designee should establish procedures for the following:

- (a) Safely transporting a juvenile who is suspected of concealing a weapon or contraband, or who may be experiencing a medical issue related to such concealment, to a medical facility or juvenile detention facility as appropriate in the given circumstances.
 1. Procedures should include keeping a juvenile suspected of concealing a weapon under constant and direct supervision until custody is transferred to the receiving facility.
- (b) Providing officers with information identifying appropriate medical and juvenile detention facilities to which a juvenile should be transported for a strip or body cavity search.

Nothing in this section is intended to prevent an officer from rendering medical aid to a juvenile in emergency circumstances (see the Medical Aid and Response Policy for additional guidance).

Prison Rape Elimination

902.1 PURPOSE AND SCOPE

This policy provides guidance for complying with the Prison Rape Elimination Act of 2003 (PREA) and the implementing regulation that establishes standards (PREA Rule) to prevent, detect and respond to sexual abuse, harassment and retaliation against prisoners in the South Saint Paul Police Department Temporary Holding Facilities (28 CFR 115.111).

902.1.1 DEFINITIONS

Definitions related to this policy include:

Intersex - A person whose sexual or reproductive anatomy or chromosomal pattern does not seem to fit typical definitions of male or female. Intersex medical conditions are sometimes referred to as disorders of sex development (28 CFR 115.5).

Sexual abuse - Any of the following acts, if the prisoner does not consent, is coerced into such act by overt or implied threats of violence or is unable to consent or refuse:

- Contact between the penis and the vulva or the penis and the anus, including penetration, however slight
- Contact between the mouth and the penis, vulva or anus
- Penetration of the anal or genital opening of another person, however slight, by a hand, finger, object or other instrument
- Any other intentional touching, either directly or through the clothing, of the genitalia, anus, groin, breast, inner thigh or the buttocks of another person, excluding contact incidental to a physical altercation (28 CFR 115.6)

Sexual abuse also includes abuse by a staff member, contractor or volunteer as follows, with or without consent of the prisoner or resident:

- Contact between the penis and the vulva or the penis and the anus, including penetration, however slight
- Contact between the mouth and the penis, vulva or anus
- Contact between the mouth and any body part where the staff member, contractor or volunteer has the intent to abuse, arouse or gratify sexual desire
- Penetration of the anal or genital opening, however slight, by a hand, finger, object or other instrument, that is unrelated to official duties, or where the staff member, contractor or volunteer has the intent to abuse, arouse or gratify sexual desire
- Any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh or the buttocks, that is unrelated to official duties, or where the staff member, contractor or volunteer has the intent to abuse, arouse or gratify sexual desire

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

- Any attempt, threat or request by a staff member, contractor or volunteer to engage in the activities described above
- Any display by a staff member, contractor or volunteer of his/her uncovered genitalia, buttocks or breast in the presence of a prisoner or resident
- Voyeurism by a staff member, contractor or volunteer (28 CFR 115.6)

Sexual harassment - Repeated and unwelcome sexual advances; requests for sexual favors; verbal comments, gestures or actions of a derogatory or offensive sexual nature by one prisoner or resident that are directed toward another; repeated verbal comments or gestures of a sexual nature to a prisoner or resident by a staff member, contractor or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures (28 CFR 115.6).

Transgender - A person whose gender identity (i.e., internal sense of feeling male or female) is different from the person's assigned sex at birth (28 CFR 115.5).

902.2 POLICY

The South Saint Paul Police Department has zero tolerance toward all forms of sexual abuse and sexual harassment (28 CFR 115.111). The Department will not tolerate retaliation against any person who reports sexual abuse or sexual harassment or who cooperates with a sexual abuse or sexual harassment investigation.

The South Saint Paul Police Department will take immediate action to protect prisoners who are reasonably believed to be subject to a substantial risk of imminent sexual abuse (28 CFR 115.162).

902.3 PREA COORDINATOR

The Chief of Police shall appoint an upper-level manager with sufficient time and authority to develop, implement and oversee department efforts to comply with PREA standards in the South Saint Paul Police Department Temporary Holding Facilities (28 CFR 115.111). The PREA Coordinator's responsibilities shall include:

- (a) Developing and maintaining procedures to comply with the PREA Rule.
- (b) Ensuring that any contract for the confinement of South Saint Paul Police Department prisoners includes the requirement to adopt and comply with applicable PREA standards and the PREA Rule, including the obligation to provide incident-based and aggregated data, as required in 28 CFR 115.187 (28 CFR 115.112).
- (c) Developing a staffing plan to provide adequate levels of staffing and video monitoring, where applicable, in order to protect prisoners from sexual abuse (28 CFR 115.113). This includes documenting deviations and the reasons for deviations from the staffing plan, as well as reviewing the staffing plan a minimum of once per year.
- (d) Developing methods for staff to privately report sexual abuse and sexual harassment of prisoners (28 CFR 115.151).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

- (e) Developing a written plan to coordinate response among staff first responders, medical and mental health practitioners, investigators and department leadership to an incident of sexual abuse (28 CFR 115.165).
- (f) Ensuring a protocol is developed for investigating allegations of sexual abuse in the Temporary Holding Facility. The protocol shall include (28 CFR 115.121; 28 CFR 115.122):
 - 1. Evidence collection practices that maximize the potential for obtaining usable physical evidence based on the most recent edition of the U.S. Department of Justice's (DOJ) Office on Violence Against Women publication, "A National Protocol for Sexual Assault Medical Forensic Examinations, Adults/Adolescents" or a similarly comprehensive and authoritative protocol.
 - 2. A process to ensure a criminal or administrative investigation is completed on all allegations of sexual abuse or sexual harassment.
 - 3. A process to document all referrals to other law enforcement agencies.
 - 4. Access to forensic medical examinations, without financial cost, for all victims of sexual abuse where appropriate. Such examinations shall be performed by Sexual Assault Forensic Examiners (SAFEs) or Sexual Assault Nurse Examiners (SANEs) where possible. If SAFEs or SANEs cannot be made available, the examination can be performed by other qualified medical practitioners. The efforts to provide SAFEs or SANEs shall be documented.
 - 5. In accordance with security needs, provisions to permit, to the extent available, prisoner access to victim advocacy services if the prisoner is transported for a forensic examination to an outside hospital that offers such services.
- (g) Ensuring that prisoners with limited English proficiency and disabilities have an equal opportunity to understand and benefit from efforts to prevent, detect and respond to sexual abuse and sexual harassment. This includes, as appropriate, access to interpreters and written materials in formats or through methods that provide effective communication to those with disabilities (e.g., limited reading skills, intellectual, hearing or vision disabilities) (28 CFR 115.116).
 - 1. The agency shall not rely on other prisoners for assistance except in limited circumstances where an extended delay in obtaining an interpreter could compromise the prisoner's safety, the performance of first-response duties under this policy, or the investigation of a prisoner's allegations of sexual abuse, harassment or retaliation.
- (h) Publishing on the department's website:
 - 1. Information on how to report sexual abuse and sexual harassment on behalf of a prisoner (28 CFR 115.154).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

2. A protocol describing the responsibilities of the Department and any other investigating agency that will be responsible for conducting sexual abuse or sexual harassment investigations (28 CFR 115.122).
- (i) Establishing a process that includes the use of a standardized form and set of definitions to ensure accurate, uniform data is collected for every allegation of sexual abuse at facilities under this agency's direct control (28 CFR 115.187).
 1. The data collected shall include, at a minimum, the data necessary to answer all questions from the most recent version of the Survey of Sexual Violence, conducted by DOJ, or any subsequent form developed by DOJ and designated for lockups.
 2. The data shall be aggregated at least annually.
- (j) Ensuring audits are conducted pursuant to 28 CFR 115.401 through 28 CFR 115.405 for all Temporary Holding Facilities used to house prisoners overnight (28 CFR 115.193).
- (k) Ensuring contractors or others who work in the Temporary Holding Facility are informed of the agency's zero-tolerance policy regarding sexual abuse and sexual harassment (28 CFR 115.132).

902.4 REPORTING SEXUAL ABUSE AND HARASSMENT

Prisoners may make reports verbally, in writing, privately or anonymously of any of the following (28 CFR 115.151):

- Sexual abuse
- Sexual harassment
- Retaliation by other prisoners or staff for reporting sexual abuse or sexual harassment
- Staff neglect or violation of responsibilities that may have contributed to sexual abuse or sexual harassment

During intake the Department shall notify all prisoners of the zero-tolerance policy regarding sexual abuse and sexual harassment, and of at least one way to report abuse or harassment to a public or private entity that is not part of the Department and that is able to receive and immediately forward prisoner reports of sexual abuse and sexual harassment to agency officials. This allows the prisoner to remain anonymous (28 CFR 115.132; 28 CFR 115.151).

902.4.1 MEMBER RESPONSIBILITIES

Department members shall accept reports from prisoners and third parties and shall promptly document all reports (28 CFR 115.151).

All members shall report immediately to the supervisor any knowledge, suspicion or information regarding:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

- (a) An incident of sexual abuse or sexual harassment that occurs in the Temporary Holding Facility.
- (b) Retaliation against prisoners or the member who reports any such incident.
- (c) Any neglect or violation of responsibilities on the part of any department member that may have contributed to an incident or retaliation (28 CFR 115.161).

No member shall reveal any information related to a sexual abuse report to anyone other than to the extent necessary to make treatment and investigation decisions.

902.4.2 SUPERVISOR RESPONSIBILITIES

The supervisor shall report to the department's designated investigators all allegations of sexual abuse, harassment, retaliation, neglect or violations leading to sexual abuse, harassment or retaliation. This includes third-party and anonymous reports (28 CFR 115.161).

If the alleged victim is under the age of 18 or considered a vulnerable adult, the supervisor shall also report the allegation as required under mandatory reporting laws and department policy.

Upon receiving an allegation that a prisoner was sexually abused while confined at another facility, the supervisor shall notify the head of the facility or the appropriate office of the agency where the alleged abuse occurred. The notification shall be made as soon as possible but no later than 72 hours after receiving the allegation. The supervisor shall document such notification (28 CFR 115.163).

If an alleged prisoner victim is transferred from the Temporary Holding Facility to a jail, prison or medical facility, the Department shall, as permitted by law, inform the receiving facility of the incident and the prisoner's potential need for medical or social services, unless the prisoner requests otherwise (28 CFR 115.165).

902.5 INVESTIGATIONS

The Department shall promptly, thoroughly and objectively investigate all allegations, including third-party and anonymous reports, of sexual abuse or sexual harassment. Only investigators who have received department-approved special training shall conduct sexual abuse investigations (28 CFR 115.171).

902.5.1 FIRST RESPONDERS

The first officer to respond to a report of sexual abuse or sexual assault shall (28 CFR 115.164):

- (a) Separate the parties.
- (b) Establish a crime scene to preserve and protect any evidence. Identify and secure witnesses until steps can be taken to collect any evidence.
- (c) If the abuse occurred within a time period that still allows for the collection of physical evidence, request that the alleged victim not take any actions that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking or eating.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

- (d) If the abuse occurred within a time period that still allows for the collection of physical evidence, ensure that the alleged abuser does not take any actions that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking or eating.

If the first responder is not an officer the responder shall request that the alleged victim not take any actions that could destroy physical evidence and should then notify a law enforcement staff member (28 CFR 115.164).

902.5.2 INVESTIGATOR RESPONSIBILITIES

Investigators shall (28 CFR 115.171):

- (a) Gather and preserve direct and circumstantial evidence, including any available physical and biological evidence and any available electronic monitoring data.
- (b) Interview alleged victims, suspects and witnesses.
- (c) Review any prior complaints and reports of sexual abuse involving the suspect.
- (d) Conduct compelled interviews only after consulting with prosecutors as to whether compelled interviews may be an obstacle for subsequent criminal prosecution.
- (e) Assess the credibility of the alleged victim, suspect or witness on an individual basis and not by the person's status as a prisoner or a member of the South Saint Paul Police Department.
- (f) Document in written reports a description of physical, testimonial, documentary and other evidence, the reasoning behind any credibility assessments, and investigative facts and findings.
- (g) Refer allegations of conduct that may be criminal to the County and City Attorney Offices for possible prosecution, including any time there is probable cause to believe a prisoner sexually abused another prisoner in the Temporary Holding Facility (28 CFR 115.178).
- (h) Cooperate with outside investigators and remain informed about the progress of any outside investigation.

902.5.3 ADMINISTRATIVE INVESTIGATIONS

Administrative investigations shall include an effort to determine whether staff actions or failures to act contributed to the abuse. The departure of the alleged abuser or victim from the employment or control of this department shall not be used as a basis for terminating an investigation (28 CFR 115.171).

902.5.4 SEXUAL ASSAULT AND SEXUAL ABUSE VICTIMS

No prisoner who alleges sexual abuse shall be required to submit to a polygraph examination or other truth-telling device as a condition for proceeding with the investigation of such an allegation (28 CFR 115.171(e)).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

Prisoner victims of sexual abuse shall receive timely, unimpeded access to emergency medical treatment. Treatment services shall be provided to the victim without financial cost and regardless of whether the victim names the abuser or cooperates with any investigation arising out of the incident (28 CFR 115.182).

902.5.5 CONCLUSIONS AND FINDINGS

All completed investigations shall be forwarded to the Chief of Police, or if the allegations may reasonably involve the Chief of Police, to the City Administrator. The Chief of Police or City Administrator shall review the investigation and determine whether any allegations of sexual abuse or sexual harassment have been substantiated by a preponderance of the evidence (28 CFR 115.172).

All personnel shall be subject to disciplinary sanctions up to and including termination for violating this policy. Termination shall be the presumptive disciplinary sanction for department members who have engaged in sexual abuse. All discipline shall be commensurate with the nature and circumstances of the acts committed, the member's disciplinary history and the sanctions imposed for comparable offenses by other members with similar histories (28 CFR 115.176).

All terminations for violations of this policy, or resignations by members who would have been terminated if not for their resignation, shall be criminally investigated unless the activity was clearly not criminal and reported to any relevant licensing body (28 CFR 115.176).

Any contractor or volunteer who engages in sexual abuse shall be prohibited from contact with prisoners and reported to any relevant licensing bodies (28 CFR 115.177). The Chief of Police shall take appropriate remedial measures and consider whether to prohibit further contact with prisoners by a contractor or volunteer.

902.6 RETALIATION PROHIBITED

All prisoners and members who report sexual abuse or sexual harassment or who cooperate with sexual abuse or sexual harassment investigations shall be protected from retaliation (28 CFR 115.167). If any other individual who cooperates with an investigation expresses a fear of retaliation, appropriate measures shall be taken to protect that individual.

The supervisor or the authorized designee shall employ multiple protection measures, such as housing changes or transfers for prisoner victims or abusers, removal of alleged abusers from contact with victims, and emotional support services for prisoners or members who fear retaliation for reporting sexual abuse or sexual harassment or for cooperating with investigations.

The supervisor or the authorized designee shall identify a staff member to monitor the conduct and treatment of prisoners or members who have reported sexual abuse and of prisoners who were reported to have suffered sexual abuse. The staff member shall act promptly to remedy any such retaliation. In the case of prisoners, such monitoring shall also include periodic status checks.

902.7 REVIEWS AND AUDITS

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

902.7.1 INCIDENT REVIEWS

An incident review shall be conducted at the conclusion of every sexual abuse investigation, unless the allegation has been determined to be unfounded. The review should occur within 30 days of the conclusion of the investigation. The review team shall include upper-level management officials and seek input from line supervisors and investigators (28 CFR 115.186).

The review shall (28 CFR 115.186):

- (a) Consider whether the allegation or investigation indicates a need to change policy or practice to better prevent, detect or respond to sexual abuse.
- (b) Consider whether the incident or allegation was motivated by race; ethnicity; gender identity; lesbian, gay, bisexual, transgender or intersex identification, status or perceived status; gang affiliation; or was motivated or otherwise caused by other group dynamics at the facility.
- (c) Examine the area in the facility where the incident allegedly occurred to assess whether physical barriers in the area may enable abuse.
- (d) Assess the adequacy of staffing levels in that area during different shifts.
- (e) Assess whether monitoring technology should be deployed or augmented to supplement supervision by staff.

The review team shall prepare a report of its findings, including any determinations made pursuant to this section and any recommendations for improvement. The report shall be submitted to the Chief of Police and the PREA Coordinator. The Chief of Police or the authorized designee shall implement the recommendations for improvement or shall document the reasons for not doing so (28 CFR 115.186).

902.7.2 DATA REVIEWS

The facility shall conduct an annual review of collected and aggregated incident-based sexual abuse data. The review should include, as needed, data from incident-based documents, including reports, investigation files and sexual abuse incident reviews (28 CFR 115.187).

The purpose of these reviews is to assess and improve the effectiveness of sexual abuse prevention, detection and response policies, practices and training. An annual report shall be prepared that includes (28 CFR 115.188):

- (a) Identification of any potential problem areas.
- (b) Identification of any corrective actions taken.
- (c) Recommendations for any additional corrective actions.
- (d) A comparison of the current year's data and corrective actions with those from prior years.
- (e) An assessment of the department's progress in addressing sexual abuse.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

The report shall be approved by the Chief of Police and made readily available to the public through the department website or, if it does not have one, through other means. Material may be redacted from the reports when publication would present a clear and specific threat to the safety and security of the Temporary Holding Facility. However, the nature of the redacted material shall be indicated.

All aggregated sexual abuse data from South Saint Paul Police Department facilities and private facilities with which it contracts shall be made readily available to the public at least annually through the department website or, if it does not have one, through other means. Before making aggregated sexual abuse data publicly available, all personal identifiers shall be removed (28 CFR 115.189).

902.8 RECORDS

The Department shall retain all written reports from administrative and criminal investigations pursuant to this policy for as long as the alleged abuser is held or employed by the Department, plus five years (28 CFR 115.171).

All other data collected pursuant to this policy shall be securely retained for at least 10 years after the date of the initial collection unless federal, state or local law requires otherwise (28 CFR 115.189).

902.9 TRAINING

All employees, volunteers and contractors who may have contact with prisoners shall receive department-approved training on the prevention and detection of sexual abuse and sexual harassment within this facility. The Support Services Commander shall be responsible for developing and administering this training as appropriate, covering at a minimum (28 CFR 115.131):

- The Department's zero-tolerance policy and prisoners' right to be free from sexual abuse and sexual harassment, and from retaliation for reporting sexual abuse or harassment.
- The dynamics of sexual abuse and harassment in confinement settings, including which prisoners are most vulnerable.
- The right of prisoners and staff members to be free from sexual abuse and sexual harassment, and from retaliation for reporting sexual abuse or harassment.
- Detecting and responding to signs of threatened and actual abuse.
- Communicating effectively and professionally with all prisoners.
- Compliance with relevant laws related to mandatory reporting of sexual abuse to outside authorities.

Investigators assigned to sexual abuse investigations shall also receive training in conducting such investigations in confinement settings. Training should include (28 CFR 115.134):

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Prison Rape Elimination

- Techniques for interviewing sexual abuse victims.
- Proper use of *Miranda* and *Garrity* warnings.
- Sexual abuse evidence collection in confinement settings.
- Criteria and evidence required to substantiate a case for administrative action or prosecution referral.

The Support Services Commander shall maintain documentation that employees, volunteers, contractors and investigators have completed required training and that they understand the training. This understanding shall be documented through individual signature or electronic verification.

All current employees and volunteers who may have contact with prisoners shall be trained within one year of the effective date of the PREA standards. The agency shall provide annual refresher information to all such employees and volunteers to ensure that they understand the current sexual abuse and sexual harassment policies and procedures.

Transporting Persons in Custody

903.1 PURPOSE AND SCOPE

This policy provides guidelines for transporting persons who are in the custody of the South Saint Paul Police Department.

See the Handcuffing and Restraints Policy for additional guidance.

903.2 POLICY

It is the policy of the South Saint Paul Police Department to provide safe, secure, and humane transportation for all persons in custody.

903.3 PATROL DIVISION COMMANDER RESPONSIBILITIES

The Patrol Division Commander should establish related procedures for:

- Safely transporting persons who have their legs restrained.
- Seating placement of persons being transported in vehicles with and without safety barriers.

903.4 OFFICER RESPONSIBILITIES

Persons in custody should be transported in a vehicle properly equipped to transport passengers. They should be appropriately restrained and positioned during transport.

Officers transporting a person in custody should:

- (a) Search all areas of the vehicle accessible to a person in custody before and after each transport.
- (b) Immediately search persons in custody after arrest, when receiving the person from the custody of another officer, and before transferring the person. Refer to the Custodial Searches Policy before conducting any search other than a field search.
 1. Whenever practicable, a search should be conducted by an officer of the same gender as the person being searched. If an officer of the same gender is not reasonably available, a witnessing officer should be present during the search.
- (c) Provide Dispatch with any required notifications (e.g., start time, mileage, end time).
- (d) Properly secure all property.
- (e) Use audio/video equipment (when properly equipped) to observe and record any person in custody during transport (see the Mobile Video Recorders and Body-Worn Cameras policies for additional guidance).
- (f) Make a reasonable effort to prevent inappropriate conversations between persons being transported (e.g., demeaning or insulting language) or conversations between a person being transported and someone outside the vehicle.
- (g) Plan travel times and routes to avoid situations that might impede transportation (e.g., heavy traffic, unfavorable road conditions, extreme weather) when reasonably practicable.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Transporting Persons in Custody

- (h) Make a verbal welfare check with a person in custody at least every 10 minutes. Provide sufficient visual observation and audio communication during the transport of:
 - 1. Individuals in auxiliary restraints.
 - 2. Individuals in leg restraints.
 - 3. Individuals wearing a spit hood.
 - 4. Individuals who are a suspected suicide risk.
- (i) Verify that the vehicle's security devices (e.g., window and rear-door child-safety locks) are activated.
- (j) Assess uncooperative persons who cannot or will not sit upright for a medical condition (see the Medical Aid and Response Policy for additional guidance):
 - 1. If no medical condition exists, alternative transportation should be arranged (e.g., a special transport van).

903.5 TRANSPORT RESTRICTIONS

When transporting multiple persons, officers:

- (a) Should not transport persons in custody together. Persons in custody should be transported individually when practicable, or within their own compartment of a multiple-compartment vehicle, unless supervisor approval is received based on unusual circumstances.
 - 1. Juveniles and adults shall not be transported together.
 - 2. Persons with known hostilities toward each other, such as mutual combatants or rival gang members, shall not be transported together.
 - 3. Persons of different genders should not be transported together.
- (b) If segregating individuals is not possible, transporting officers should be alert to inappropriate physical or verbal contact and take appropriate action.

903.6 TRANSPORT VANS

An officer trained on the safety and restraint systems of a transport van should be present during the transport van's use for transporting a person in custody.

An officer should assist persons getting into and out of the transport van to avoid falls.

903.7 TRANSPORTING PERSONS IN CUSTODY WHO HAVE A DISABILITY

When transporting a person in custody who has a disability, a transporting officer should request assistance as necessary to transport the person in a reasonable and safe manner. The transporting officer should ensure that any special equipment (e.g., canes, wheelchairs, prosthetics) is transported to the person's destination in a way that does not threaten the safety or security of the person in custody or the officer.

Officers transporting a person who has a disability should consult with the person in custody and use good judgment in determining what, if any, restraining devices may be appropriate based on the person's disability to ensure the security, safety, and dignity of all persons.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Transporting Persons in Custody

903.8 TRANSPORTING ILL OR INJURED PERSONS IN CUSTODY

Except in exceptional cases where alternatives are not reasonably available, officers should not transport persons in custody who are unconscious, have serious injuries, or who may be seriously ill. EMS personnel should be called to handle such transportation.

Officers shall notify a supervisor as soon as practicable when transporting a person in custody to a hospital.

An officer should accompany any person in custody during transport in an ambulance when requested by EMS personnel, when it reasonably appears necessary to provide security, when it is necessary for investigative purposes, or when so directed by a Sergeant.

Any person in custody suspected of having a communicable disease should be transported in compliance with the exposure control plan in the Communicable Diseases Policy.

See the Medical Aid and Response Policy for additional guidance on ill or injured persons in custody.

903.9 TRANSPORTING PREGNANT PERSONS IN CUSTODY

Persons in custody who are known to be pregnant should be restrained during transport in the least restrictive manner that is effective for officer safety. Leg restraints, waist chains, or handcuffs behind the body should not be used unless the officer has a reasonable suspicion that the person may resist, attempt escape, injure themselves or others, or damage property.

Absent exceptional circumstances, persons in labor or delivery should not be transported by officers. EMS personnel should be called to handle transportation.

903.10 CIVIL COMMITMENT TRANSPORTS

When transporting any individual for a civil commitment, the transporting officer should request that Dispatch notify the receiving facility of the estimated time of arrival, the level of cooperation of the individual, and whether any special medical care is needed.

Should the person require transport in a medical transport vehicle, and the safety of any person, including the person in custody, requires the presence of an officer during the transport, Sergeant approval is required before transport commences.

See the Civil Commitments Policy for additional guidance.

903.10.1 TYPE OF TRANSPORTATION

When transporting any individual on a Minn. Stat. § 253B.051 admission, and if reasonably practicable, officers should not be in uniform and should not use a vehicle visibly marked as a law enforcement vehicle (Minn. Stat. § 253B.051, Subd. 1(e)).

903.11 INTERRUPTION OF TRANSPORT

Absent extraordinary circumstances, officers should not interrupt a transport to provide emergency assistance without supervisory approval. Officers encountering an emergency should notify Dispatch and request an appropriate response.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Transporting Persons in Custody

903.12 EXTENDED TRANSPORTS

During transports for extended durations, transporting officers may be required to make necessary stops. With supervisory approval and due consideration for security risks and the in-custody person's health and well-being, these stops should be limited to fuel, meals, bathroom breaks, and other purposes reasonably necessary for the continuation of the transport.

903.13 PROHIBITIONS

When transporting a person in custody, officers should not:

- (a) Use transport as a form of punishment or retaliation (e.g., intentionally rough rides, excessive heat or cold, obnoxiously loud music).
- (b) Handcuff a person to any part of a vehicle.
- (c) Leave the vehicle unattended with the person in custody in the vehicle.
- (d) Allow any person who is not in custody (e.g., friend, family member) to have contact with or be in close proximity to the person in custody.
- (e) Allow any food, drink, or other consumables to be given to the person in custody by anyone other than department personnel or receiving agency personnel.
- (f) Stop to conduct any personal activities.
- (g) Engage in a pursuit.

903.14 ESCAPES

In the event that a person in custody escapes while being transported, the transporting officer should immediately advise Dispatch and other units of the escape, provide a description of the escapee, notify the Sergeant, and submit a written report as soon as practicable describing the circumstances of the escape and any recapture.

The Sergeant should notify the Chief of Police or the authorized designee upon learning of an escape.

If the escape occurs outside the jurisdiction of the South Saint Paul Police Department, the Sergeant should notify the appropriate agency or agencies within the jurisdiction where the escape occurred.

903.15 DOCUMENTATION

If a person is injured during transportation, officers should document the injury in the appropriate report. Documentation should include the condition of the person prior to transportation and the known or suspected causes of the injury during transportation (e.g., hitting head, struggling with restraints, fighting with other persons in custody). Any visible or reported injuries should be photographed and included with the report.

903.16 NOTIFICATIONS

Officers should notify a supervisor and any receiving facility of information regarding any circumstances the officer reasonably believes would be potential safety concerns or medical

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Transporting Persons in Custody

risks to the person (e.g., uncooperative or violent, prolonged struggle, extreme agitation, medical conditions) that may have occurred prior to, or during, transportation.

903.17 TRAINING

The Support Services Commander should provide periodic training on this policy and procedures related to transporting persons in custody, restraint systems, and restraint devices.

Chapter 10 - Personnel

Anti-Retaliation

1000.1 PURPOSE AND SCOPE

This policy prohibits retaliation against members who identify workplace issues, such as fraud, waste, abuse of authority, gross mismanagement or any inappropriate conduct or practices, including violations that may pose a threat to the health, safety or well-being of members.

This policy does not prohibit actions taken for nondiscriminatory or non-retaliatory reasons, such as discipline for cause.

These guidelines are intended to supplement and not limit members' access to other applicable remedies. Nothing in this policy shall diminish the rights or remedies of a member pursuant to any applicable federal law, provision of the U.S. Constitution, law, ordinance or collective bargaining agreement.

1000.2 POLICY

The South Saint Paul Police Department has a zero tolerance for retaliation and is committed to taking reasonable steps to protect from retaliation members who, in good faith, engage in permitted behavior or who report or participate in the reporting or investigation of workplace issues. All complaints of retaliation will be taken seriously and will be promptly and appropriately investigated.

1000.3 RETALIATION PROHIBITED

No member may retaliate against any person for engaging in lawful or otherwise permitted behavior; for opposing a practice believed to be unlawful, unethical, discriminatory or retaliatory; for reporting or making a complaint under this policy; or for participating in any investigation related to a complaint under this or any other policy.

Retaliation includes any adverse action or conduct, including but not limited to:

- Refusing to hire or denying a promotion.
- Extending the probationary period.
- Unjustified reassignment of duties or change of work schedule.
- Real or implied threats or other forms of intimidation to dissuade the reporting of wrongdoing or filing of a complaint, or as a consequence of having reported or participated in protected activity.
- Taking unwarranted disciplinary action.
- Spreading rumors about the person filing the complaint or about the alleged wrongdoing.
- Shunning or unreasonably avoiding a person because he/she has engaged in protected activity.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Anti-Retaliation

1000.3.1 RETALIATION PROHIBITED FOR INTERVENING OR REPORTING

An officer shall not be retaliated against for intervening or reporting that another law enforcement officer or a member used excessive force (Minn. Stat. § 626.8452).

1000.4 COMPLAINTS OF RETALIATION

Any member who feels he/she has been retaliated against in violation of this policy should promptly report the matter to any supervisor, command staff member, Chief of Police or the City Director of Human Services.

Members shall act in good faith, not engage in unwarranted reporting of trivial or minor deviations or transgressions, and make reasonable efforts to verify facts before making any complaint in order to avoid baseless allegations. Members shall not report or state an intention to report information or an allegation knowing it to be false, with willful or reckless disregard for the truth or falsity of the information or otherwise act in bad faith.

Investigations are generally more effective when the identity of the reporting member is known, thereby allowing investigators to obtain additional information from the reporting member. However, complaints may be made anonymously. All reasonable efforts shall be made to protect the reporting member's identity. However, confidential information may be disclosed to the extent required by law or to the degree necessary to conduct an adequate investigation and make a determination regarding a complaint. In some situations, the investigative process may not be complete unless the source of the information and a statement by the member is part of the investigative process.

1000.5 SUPERVISOR RESPONSIBILITIES

Supervisors are expected to remain familiar with this policy and ensure that members under their command are aware of its provisions.

The responsibilities of supervisors include, but are not limited to:

- (a) Ensuring complaints of retaliation are investigated as provided in the Personnel Complaints Policy.
- (b) Receiving all complaints in a fair and impartial manner.
- (c) Documenting the complaint and any steps taken to resolve the problem.
- (d) Acknowledging receipt of the complaint, notifying the Chief of Police via the chain of command and explaining to the member how the complaint will be handled.
- (e) Taking appropriate and reasonable steps to mitigate any further violations of this policy.
- (f) Monitoring the work environment to ensure that any member making a complaint is not subjected to further retaliation.
- (g) Periodic follow-up with the complainant to ensure that retaliation is not continuing.
- (h) Not interfering with or denying the right of a member to make any complaint.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Anti-Retaliation

- (i) Taking reasonable steps to accommodate requests for assignment or schedule change made by a member who may be the target of retaliation if it would likely mitigate the potential for further violations of this policy.

1000.6 COMMAND STAFF RESPONSIBILITIES

The Chief of Police should communicate to all supervisors the prohibition against retaliation.

Command staff shall treat all complaints as serious matters and shall ensure that prompt actions take place, including but not limited to:

- (a) Communicating to all members the prohibition against retaliation.
- (b) The timely review of complaint investigations.
- (c) Remediation of any inappropriate conduct or condition and instituting measures to eliminate or minimize the likelihood of recurrence.
- (d) The timely communication of the outcome to the complainant.

1000.7 WHISTLE-BLOWING

The Minnesota Whistleblower Act protects an employee who, in good faith (Minn. Stat. § 181.932):

- (a) Communicates a violation of any law or rule to the Department or to any government body or law enforcement official.
- (b) Participates in an investigation, hearing, or inquiry at the request of a public body or office.
- (c) Refuses an order to perform an act that the employee objectively believes violates a law, rule, or regulation, and informs the employer of the reason.
- (d) Reports a situation where the quality of health care services provided by a health care facility or provider violates a state or federal standard and potentially places the public at risk of harm.
- (e) Communicates the findings of a technical or scientific study that the employee believes, in good faith, to be truthful and accurate.

Members who believe they have been the subject of retaliation for engaging in such protected behaviors should promptly report it to a supervisor. Supervisors should refer the complaint to the Support Services Commander for investigation pursuant to the Personnel Complaints Policy.

1000.8 RECORDS RETENTION AND RELEASE

The Records Supervisor shall ensure that documentation of investigations is maintained in accordance with the established records retention schedules.

1000.9 TRAINING

The policy should be reviewed with each new member.

All members should receive periodic refresher training on the requirements of this policy.

Reporting of Employee Convictions and Court Orders

1001.1 PURPOSE AND SCOPE

Convictions of certain offenses may restrict or prohibit an employee's ability to properly perform official duties. Therefore, all employees shall be required to promptly notify the Department of any past and current criminal convictions.

1001.2 DOMESTIC VIOLENCE CONVICTIONS AND RESTRAINING ORDERS

Minnesota and federal law prohibit individuals convicted of certain offenses and individuals subject to certain court orders from lawfully possessing a firearm. Such convictions and court orders often involve allegations of the use or attempted use of force or threatened use of a weapon on any individual in a domestic relationship (e.g., spouse, cohabitant, parent, child) (18 USC § 922; Minn. Stat. § 518B.01).

All members are responsible for ensuring that they have not been disqualified from possessing a firearm by any such conviction or court order and shall promptly report any such conviction or court order to a supervisor, as provided in this policy.

1001.3 CRIMINAL CONVICTIONS

Any person convicted of a felony is prohibited from being a peace officer in the State of Minnesota. Any license of a peace officer convicted of a felony is automatically revoked (Minn. Stat. § 626.8431).

Even when legal restrictions are not imposed by statute or by the courts upon conviction of any criminal offense, criminal conduct by a member of this department may prohibit him/her from carrying out law enforcement duties.

Minn. Stat. § 624.713 prohibits ineligible persons from possessing a handgun or semi-automatic assault weapon.

1001.3.1 COURT ORDERS

All employees shall promptly notify the department if they are a party to, or have been served with, any court order from any jurisdiction.

1001.4 REPORTING PROCEDURE

All members of this department and all retired officers with an identification card issued by the Department shall promptly notify their immediate supervisor (or the Chief of Police in the case of retired officers) in writing of any past or current criminal arrest or conviction regardless of whether the matter is currently on appeal and regardless of the penalty or sentence, if any.

All members and all retired officers with an identification card issued by the Department shall further promptly notify their immediate supervisor (or the Chief of Police in the case of retired

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Reporting of Employee Convictions and Court Orders

officers) in writing if the member or retiree becomes the subject of a domestic violence restraining court order or similar court order.

Any member whose criminal conviction unduly restricts or prohibits that member from fully and properly performing his/her duties may be disciplined including, but not limited to, being placed on administrative leave, reassignment and/or termination.

Any member failing to provide prompt written notice pursuant to this policy shall be subject to discipline.

1001.5 CHEMICAL DEPENDENCY TREATMENT

If an officer is informally admitted to a treatment facility or program pursuant to Minn. Stat. § 253B.04 for chemical dependency he/she is not eligible to possess a pistol, unless the officer possesses a certificate from the head of the treatment facility discharging or provisionally discharging the officer from the treatment facility (Minn. Stat. § 624.713 Subd. 1(6)).

Officers in this situation shall promptly notify the department.

Communicable Diseases

1002.1 PURPOSE AND SCOPE

This policy provides general guidelines to assist in minimizing the risk of department members contracting and/or spreading communicable diseases.

1002.1.1 DEFINITIONS

Definitions related to this policy include:

Communicable disease - A human disease caused by microorganisms that are present in and transmissible through human blood, bodily fluid, tissue, or by breathing or coughing. These diseases commonly include, but are not limited to, hepatitis B virus (HBV), HIV and tuberculosis.

Exposure - When an eye, mouth, mucous membrane or non-intact skin comes into contact with blood or other potentially infectious materials, or when these substances are injected or infused under the skin; when an individual is exposed to a person who has a disease that can be passed through the air by talking, sneezing or coughing (e.g., tuberculosis), or the individual is in an area that was occupied by such a person. Exposure only includes those instances that occur due to a member's position at the South Saint Paul Police Department. (See the exposure control plan for further details to assist in identifying whether an exposure has occurred.)

1002.2 POLICY

The South Saint Paul Police Department is committed to providing a safe work environment for its members. Members should be aware that they are ultimately responsible for their own health and safety.

1002.3 EXPOSURE CONTROL OFFICER

The Chief of Police will assign a person as the Exposure Control Officer (ECO). The ECO shall develop an exposure control plan that includes:

- (a) Exposure-prevention and decontamination procedures.
- (b) Procedures for when and how to obtain medical attention in the event of an exposure or suspected exposure.
- (c) The provision that department members will have no-cost access to the appropriate personal protective equipment (PPE) (e.g., gloves, face masks, eye protection, pocket masks) for each member's position and risk of exposure.
- (d) Evaluation of persons in custody for any exposure risk and measures to separate them.
- (e) Compliance with all relevant laws or regulations related to communicable diseases, including:
 - 1. Responding to requests and notifications regarding exposures covered under the Ryan White law (42 USC § 300ff-133; 42 USC § 300ff-136).
 - 2. Exposure control mandates in 29 CFR 1910.1030 (Minn. R. 5206.0600).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Communicable Diseases

3. Reporting cases and suspected cases of communicable diseases to the Department of Public Health (Minn. R. 4605.7070; Minn. Stat. § 144.4804).
4. Notifying appropriate medical facilities regarding member exposures and providing assistance locating source individuals, as applicable (Minn. Stat. § 144.7414)

The ECO should also act as the liaison with the Minnesota Occupational Safety and Health Administration (MNOSHA) and may request voluntary compliance inspections. The ECO should annually review and update the exposure control plan and review implementation of the plan.

1002.4 EXPOSURE PREVENTION AND MITIGATION

1002.4.1 GENERAL PRECAUTIONS

All members are expected to use good judgment and follow training and procedures related to mitigating the risks associated with communicable disease. This includes, but is not limited to (29 CFR 1910.1030; Minn. R. 5206.0600):

- (a) Stocking disposable gloves, antiseptic hand cleanser, CPR masks or other specialized equipment in the work area or department vehicles, as applicable.
- (b) Wearing department-approved disposable gloves when contact with blood, other potentially infectious materials, mucous membranes and non-intact skin can be reasonably anticipated.
- (c) Washing hands immediately or as soon as feasible after removal of gloves or other PPE.
- (d) Treating all human blood and bodily fluids/tissue as if it is known to be infectious for a communicable disease.
- (e) Using an appropriate barrier device when providing CPR.
- (f) Using a face mask or shield if it is reasonable to anticipate an exposure to an airborne transmissible disease.
- (g) Decontaminating non-disposable equipment (e.g., flashlight, control devices, clothing and portable radio) as soon as possible if the equipment is a potential source of exposure.
 1. Clothing that has been contaminated by blood or other potentially infectious materials shall be removed immediately or as soon as feasible and stored/decontaminated appropriately.
- (h) Handling all sharps and items that cut or puncture (e.g., needles, broken glass, razors, knives) cautiously and using puncture-resistant containers for their storage and/or transportation.
- (i) Avoiding eating, drinking, smoking, applying cosmetics or lip balm, or handling contact lenses where there is a reasonable likelihood of exposure.
- (j) Disposing of biohazardous waste appropriately or labeling biohazardous material properly when it is stored.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Communicable Diseases

1002.4.2 IMMUNIZATIONS

Members who could be exposed to HBV due to their positions may receive the HBV vaccine and any routine booster at no cost (29 CFR 1910.1030; Minn. R. 5206.0600).

1002.5 POST EXPOSURE

1002.5.1 INITIAL POST-EXPOSURE STEPS

Members who experience an exposure or suspected exposure shall:

- (a) Begin decontamination procedures immediately (e.g., wash hands and any other skin with soap and water, flush mucous membranes with water).
- (b) Obtain medical attention as appropriate.
- (c) Notify a supervisor as soon as practicable.

1002.5.2 REPORTING REQUIREMENTS

The supervisor on-duty shall investigate every exposure or suspected exposure that occurs as soon as possible following the incident. The supervisor shall ensure the following information is documented (29 CFR 1910.1030; Minn. R. 5206.0600):

- (a) Name of the member exposed
- (b) Date and time of the incident
- (c) Location of the incident
- (d) Potentially infectious materials involved and the source of exposure (e.g., identification of the person who may have been the source)
- (e) Work being done during exposure
- (f) How the incident occurred or was caused
- (g) PPE in use at the time of the incident
- (h) Actions taken post-event (e.g., clean-up, notifications)

The supervisor shall advise the member that disclosing the identity and/or infectious status of a source to the public or to anyone who is not involved in the follow-up process is prohibited. The supervisor should complete the incident documentation in conjunction with other reporting requirements that may apply (see the Occupational Disease, Personal Injury and Death Reporting Policy).

1002.5.3 MEDICAL CONSULTATION, EVALUATION AND TREATMENT

Department members shall have the opportunity to have a confidential medical evaluation immediately after an exposure and follow-up evaluations as necessary.

The ECO should request a written opinion/evaluation from the treating medical professional that contains only the following information (29 CFR 1910.1030; Minn. R. 5206.0600):

- (a) Whether the member has been informed of the results of the evaluation.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Communicable Diseases

- (b) Whether the member has been notified of any medical conditions resulting from exposure to blood or other potentially infectious materials which require further evaluation or treatment.

No other information should be requested or accepted by the ECO.

1002.5.4 COUNSELING

The Department shall provide the member, and his/her family if necessary, the opportunity for counseling and consultation regarding the exposure (29 CFR 1910.1030; Minn. R. 5206.0600).

1002.5.5 SOURCE TESTING

Testing a person for communicable diseases when that person was the source of an exposure should be done when it is desired by the exposed member or when it is otherwise appropriate. Source testing is the responsibility of the ECO. If the ECO is unavailable to seek timely testing of the source, it is the responsibility of the exposed member's supervisor to ensure testing is sought.

Source testing may be achieved by:

- (a) Obtaining consent from the individual.
- (b) Seeking testing through the procedures of Minn. Stat. § 144.7401 to Minn. Stat. § 144.7415 through a licensed hospital or other emergency medical care facility.

Since there is the potential for overlap between the different manners in which source testing may occur, the ECO is responsible for coordinating the testing to prevent unnecessary or duplicate testing.

The ECO should seek the consent of the individual for testing and consult the City Attorney to discuss other options when no statute exists for compelling the source of an exposure to undergo testing if he/she refuses.

1002.6 CONFIDENTIALITY OF REPORTS

Medical information shall remain in confidential files and shall not be disclosed to anyone without the member's written consent (except as required by law). Test results from persons who may have been the source of an exposure are to be kept confidential as well (Minn. Stat. § 144.7411).

1002.7 TRAINING

All members shall participate in training regarding communicable diseases commensurate with the requirements of their position. The training (29 CFR 1910.1030; Minn. R. 5206.0700):

- (a) Shall be provided at the time of initial assignment to tasks where an occupational exposure may take place and at least annually after the initial training.
- (b) Shall be provided whenever the member is assigned new tasks or procedures affecting his/her potential exposure to communicable disease.
- (c) Should provide guidance on what constitutes an exposure, what steps can be taken to avoid an exposure and what steps should be taken if a suspected exposure occurs.

Personnel Complaints

1003.1 PURPOSE AND SCOPE

This policy provides guidelines for the reporting, investigation and disposition of complaints regarding the conduct of members of the South Saint Paul Police Department (Minn. R. 6700.2200). This policy shall not apply to any questioning, counseling, instruction, informal verbal admonishment or other routine or unplanned contact of a member in the normal course of duty, by a supervisor or any other member, nor shall this policy apply to a criminal investigation.

Nothing in this policy is intended to supersede disciplinary procedures as identified in the rules of the South St Paul Police Civil Service Commission.

1003.2 POLICY

The South Saint Paul Police Department takes seriously all complaints regarding the service provided by the Department and the conduct of its members.

The Department will accept and address all complaints of misconduct in accordance with this policy and applicable federal, state and local law, municipal and county rules and the requirements of any memorandum of understanding.

It is also the policy of this department to ensure that the community can report misconduct without concern for reprisal or retaliation.

1003.3 PERSONNEL COMPLAINTS

Personnel complaints include any allegation of misconduct or improper job performance that, if true, would constitute a violation of department policy or of federal, state or local law, policy or rule. Personnel complaints may be generated internally or by the public.

Inquiries about conduct or performance that, if true, would not violate department policy or federal, state or local law, policy or rule may be handled informally by a supervisor and shall not be considered a personnel complaint. Such inquiries generally include clarification regarding policy, procedures or the response to specific incidents by the Department.

1003.3.1 COMPLAINT CLASSIFICATIONS

Personnel complaints shall be classified in one of the following categories:

Informal - A matter in which the Sergeant is satisfied that appropriate action has been taken by a supervisor of rank greater than the accused member.

Formal - A matter in which a supervisor determines that further action is warranted. Such complaints may be investigated by a supervisor of rank greater than the accused member or referred to the the Chief depending on the seriousness and complexity of the investigation.

Incomplete - A matter in which the complaining party either refuses to cooperate or becomes unavailable after diligent follow-up investigation. At the discretion of the assigned supervisor or the

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

Chief, such matters may be further investigated depending on the seriousness of the complaint and the availability of sufficient information.

1003.3.2 SOURCES OF COMPLAINTS

The following applies to the source of complaints:

- (a) Individuals from the public may make complaints in any form, including in writing, by email, in person or by telephone.
- (b) Any department member becoming aware of alleged misconduct shall immediately notify a supervisor.
- (c) Supervisors shall initiate a complaint based upon observed misconduct or receipt from any source alleging misconduct that, if true, could result in disciplinary action.
- (d) Anonymous and third-party complaints should be accepted and investigated to the extent that sufficient information is provided.
- (e) Tort claims and lawsuits may generate a personnel complaint.
- (f) The Minnesota Board of Peace Officer Standards and Training (POST) may refer complaints alleging a violation of a statute or rule that the board is empowered to enforce (Minn. Stat. § 214.10, Subd. 10).
- (g) Any person making a complaint may be accompanied by an attorney or other representative, including at the time the complaint is made.
- (h) Any person wishing to file a complaint against the Chief of Police should be referred to the City Administrator for investigation by an outside agency.

1003.4 AVAILABILITY AND ACCEPTANCE OF COMPLAINTS

1003.4.1 COMPLAINT FORMS

Personnel complaint forms will be maintained in a clearly visible location in the public area of the police facility and be accessible through the department website. Forms may also be available at other City facilities.

Personnel complaint forms in languages other than English may also be provided, as determined necessary or practicable.

1003.4.2 ACCEPTANCE

All complaints will be courteously accepted by any department member and promptly given to the appropriate supervisor. Although written complaints are preferred, a complaint may also be filed orally, either in person or by telephone. Such complaints will be directed to a supervisor. If a supervisor is not immediately available to take an oral complaint, the receiving member shall obtain contact information sufficient for the supervisor to contact the complainant. The supervisor, upon contact with the complainant, shall complete and submit a complaint form as appropriate.

Although not required, complainants should be encouraged to file complaints in person so that proper identification, signatures, photographs or physical evidence may be obtained as necessary.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

1003.4.3 COMPLAINT COPIES

After a complaint is filed, the accepting member should sign the document, keep a copy for the department and provide a copy to the complainant.

1003.5 DOCUMENTATION

Supervisors shall ensure that all formal and informal complaints are documented on a complaint form. The supervisor shall ensure that the nature of the complaint is defined as clearly as possible.

All complaints and inquiries should also be documented in a log that records and tracks complaints. The log shall include the nature of the complaint and the actions taken to address the complaint. On an annual basis, the Department should audit the log and send an audit report to the Chief of Police or the authorized designee.

1003.6 ADMINISTRATIVE INVESTIGATIONS

Allegations of misconduct will be administratively investigated as follows (Minn. R. 6700.2200).

1003.6.1 SUPERVISOR RESPONSIBILITIES

In general, the primary responsibility for the investigation of a personnel complaint shall rest with the member's immediate supervisor, unless the supervisor is the complainant, or the supervisor is the ultimate decision-maker regarding disciplinary action or has any personal involvement regarding the alleged misconduct. The Chief of Police or the authorized designee may direct that another supervisor investigate any complaint.

A supervisor who becomes aware of alleged misconduct shall take reasonable steps to prevent aggravation of the situation.

The responsibilities of supervisors include, but are not limited to:

- (a) Ensuring that upon receiving or initiating any formal complaint, a complaint form is completed.
 - 1. The original complaint form will be directed to the Sergeant of the accused member, via the chain of command, who will take appropriate action and/or determine who will have responsibility for the investigation.
 - 2. In circumstances where the integrity of the investigation could be jeopardized by reducing the complaint to writing or where the confidentiality of a complainant is at issue, a supervisor shall orally report the matter to the member's Division Commander or the Chief of Police, who will initiate appropriate action.
- (b) Responding to all complaints in a courteous and professional manner.
- (c) Resolving those personnel complaints that can be resolved immediately.
 - 1. Follow-up contact with the complainant should be made within 24 hours of the Department receiving the complaint.
 - 2. If the matter is resolved and no further action is required, the supervisor will note the resolution on a complaint form and forward the form to the Sergeant.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

- (d) Ensuring that upon receipt of a complaint involving allegations of a potentially serious nature, the Sergeant and Chief of Police are notified via the chain of command as soon as practicable.
- (e) Promptly contacting the Department of Human Resources and the Sergeant for direction regarding their roles in addressing a complaint that relates to sexual, racial, ethnic or other forms of prohibited harassment or discrimination.
- (f) Forwarding unresolved personnel complaints to the Sergeant, who will determine whether to contact the complainant or assign the complaint for investigation.
- (g) Informing the complainant of the investigator's name and the complaint number within three days after assignment.
- (h) Investigating a complaint as follows:
 - 1. Making reasonable efforts to obtain names, addresses and telephone numbers of witnesses.
 - 2. When appropriate, ensuring immediate medical attention is provided and photographs of alleged injuries and accessible uninjured areas are taken.
- (i) Ensuring that the procedural rights of the accused member are followed.
- (j) Ensuring interviews of the complainant are generally conducted during reasonable hours.

1003.6.2 ADMINISTRATIVE INVESTIGATION PROCEDURES

Whether conducted by a supervisor or an assigned member of the Support Services Commander, the following shall apply to members covered by the Peace Officer Discipline Procedures Act (Minn. Stat. § 626.89):

- (a) Interviews of an accused member shall be conducted during reasonable hours and preferably when the member is on-duty (Minn. Stat. § 626.89, Subd. 7). If the member is off-duty, he/she shall be compensated.
- (b) Unless waived by the member, interviews of an accused member shall be at the South Saint Paul Police Department or at a place agreed upon by the accused member (Minn. Stat. § 626.89, Subd. 4).
- (c) No more than two interviewers should ask questions of an accused member.
- (d) Prior to any interview, a member should be informed of the nature of the investigation.
 - 1. The member shall be given a copy of any written complaint signed by the complainant (Minn. Stat. § 626.89, Subd. 5).
- (e) All interviews should be for a reasonable period and the member's personal needs should be accommodated (Minn. Stat. § 626.89, Subd. 7).
- (f) No member should be subjected to offensive or threatening language, nor shall any promises, rewards or other inducements be used to obtain answers.
- (g) Any member refusing to answer questions directly related to the investigation may be ordered to answer questions administratively and may be subject to discipline for failing to do so.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

1. A member should be given an order to answer questions in an administrative investigation that might incriminate the member in a criminal matter only after the member has been given a *Garrity* advisement. Administrative investigators should consider the impact that compelling a statement from the member may have on any related criminal investigation and should take reasonable steps to avoid creating any foreseeable conflicts between the two related investigations. This may include conferring with the person in charge of the criminal investigation (e.g., discussion of processes, timing, implications).
 2. No information or evidence administratively coerced from a member may be provided to anyone involved in conducting the criminal investigation or to any prosecutor.
- (h) The interviewer shall record all interviews of members and witnesses. The member may also record the interview. A complete copy or transcript of the interview must be made available to the member upon written request without charge or undue delay. If the member has been previously interviewed, a copy of that recorded interview shall be provided to the member prior to any subsequent interview (Minn. Stat. § 626.89, Subd. 8).
- (i) All members subjected to interviews that could result in discipline have the right to have an uninvolved representative or attorney present before or during the interview (Minn. Stat. § 626.89, Subd. 9). When a member requests a representative or attorney, no interview may be taken until a reasonable opportunity is provided for the member to obtain that person's presence. However, in order to maintain the integrity of each individual's statement, involved members shall not consult or meet with a representative or attorney collectively or in groups prior to being interviewed.
- (j) All members shall provide complete and truthful responses to questions posed during interviews.
- (k) No member may be compelled to submit to a polygraph examination, nor shall any refusal to submit to such examination be mentioned in any investigation.
- (l) Before a formal statement is taken, the member shall be advised in writing or on the record that admissions made may be used as evidence of misconduct or a basis for discipline (Minn. Stat. § 626.89, Subd. 10).
- (m) A member may not be required to produce financial records (Minn. Stat. § 626.89, Subd. 11).
- (n) A member's photograph will not be released unless allowed by law (Minn. Stat. § 626.89, Subd. 12).

1003.6.3 ADMINISTRATIVE INVESTIGATION FORMAT

Formal investigations of personnel complaints shall be thorough, complete and essentially follow this format:

Introduction - Include the identity of the members, the identity of the assigned investigators, the initial date and source of the complaint.

Synopsis - Provide a brief summary of the facts giving rise to the investigation.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

Summary - List the allegations separately, including applicable policy sections, with a brief summary of the evidence relevant to each allegation. A separate recommended finding should be provided for each allegation.

Evidence - Each allegation should be set forth with the details of the evidence applicable to each allegation provided, including comprehensive summaries of member and witness statements. Other evidence related to each allegation should also be detailed in this section.

Conclusion - A recommendation regarding further action or disposition should be provided.

Exhibits - A separate list of exhibits (e.g., recordings, photos, documents) should be attached to the report.

1003.6.4 DISPOSITIONS

Each personnel complaint shall be classified with one of the following dispositions:

Unfounded - When the investigation discloses that the alleged acts did not occur or did not involve department members. Complaints that are determined to be frivolous will fall within the classification of unfounded.

Exonerated - When the investigation discloses that the alleged act occurred but that the act was justified, lawful and/or proper.

Not sustained - When the investigation discloses that there is insufficient evidence to sustain the complaint or fully exonerate the member.

Sustained - When the investigation discloses sufficient evidence to establish that the act occurred and that it constituted misconduct.

If an investigation discloses misconduct or improper job performance that was not alleged in the original complaint, the investigator shall take appropriate action with regard to any additional allegations.

The Chief of Police may authorize that any investigation be re-opened any time substantial new evidence is discovered concerning the complaint.

1003.6.5 COMPLETION OF INVESTIGATIONS

Every investigator or supervisor assigned to investigate a personnel complaint or other alleged misconduct shall proceed with due diligence in an effort to complete the investigation within one year from the date of discovery by an individual authorized to initiate an investigation.

1003.6.6 EXTERNAL INVESTIGATIONS

The Chief of Police may request that an outside agency conduct an investigation anytime the Chief of Police determines an external investigation is appropriate.

This department should not conduct an investigation when the Chief of Police is the subject of the complaint. An external investigation should be requested through the City Administrator.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

1003.6.7 NOTICE TO COMPLAINANT OF INVESTIGATION STATUS

The member conducting the investigation shall provide the complainant with periodic updates on the status of the investigation, as appropriate and consistent with the provisions of the Minnesota Government Data Practices Act (MGDP) (Minn. Stat. § 13.43, Subd. 2; Minn. R. 6700.2200).

1003.7 ADMINISTRATIVE SEARCHES

Assigned lockers, storage spaces and other areas, including desks, offices and vehicles, may be searched as part of an administrative investigation upon a reasonable suspicion of misconduct.

Such areas may also be searched any time by a supervisor for non-investigative purposes, such as obtaining a needed report, radio or other document or equipment.

1003.8 ADMINISTRATIVE LEAVE

When a complaint of misconduct is of a serious nature, or when circumstances indicate that allowing the accused to continue to work would adversely affect the mission of the Department, the Chief of Police or the authorized designee may temporarily assign an accused employee to administrative leave. Any employee placed on administrative leave:

- (a) May be required to relinquish any department badge, identification, assigned weapons and any other department equipment.
- (b) Shall be required to continue to comply with all policies and lawful orders of a supervisor.
- (c) May be temporarily reassigned to a different shift, generally a normal business-hours shift, during the investigation. The employee may be required to remain available for contact at all times during such shift, and will report as ordered.

1003.9 CRIMINAL INVESTIGATION

Where a member is accused of potential criminal conduct, a separate supervisor or investigator shall be assigned to investigate the criminal allegations apart from any administrative investigation. Any separate administrative investigation may parallel a criminal investigation.

The Chief of Police shall be notified as soon as practicable when a member is accused of criminal conduct. The Chief of Police may request a criminal investigation by an outside law enforcement agency.

A member accused of criminal conduct shall be provided with all rights afforded to a civilian. The member should not be administratively ordered to provide any information in the criminal investigation.

No information or evidence administratively coerced from a member may be provided to anyone involved in conducting the criminal investigation or to any prosecutor.

The South Saint Paul Police Department may release information concerning the arrest or detention of any member, including an officer, that has not led to a conviction. No disciplinary action should be taken until an independent administrative investigation is conducted.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

The Chief of Police may postpone making a decision on an administrative investigation until any related criminal charges are resolved. The complainant and involved member should be informed of this decision.

1003.10 POST-ADMINISTRATIVE INVESTIGATION PROCEDURES

Upon completion of a formal investigation, an investigation report should be forwarded to the Chief of Police through the chain of command. Each level of command should review and include their comments in writing before forwarding the report. The Chief of Police may accept or modify any classification or recommendation for disciplinary action.

1003.10.1 DIVISION COMMANDER RESPONSIBILITIES

Upon receipt of any completed personnel investigation, the Division Commander of the involved member shall review the entire investigative file, the member's personnel file and any other relevant materials.

The Division Commander may make recommendations regarding the disposition of any allegations and the amount of discipline, if any, to be imposed.

Prior to forwarding recommendations to the Chief of Police, the Division Commander may return the entire investigation to the assigned investigator or supervisor for further investigation or action.

When forwarding any written recommendation to the Chief of Police, the Division Commander shall include all relevant materials supporting the recommendation. Actual copies of a member's existing personnel file need not be provided and may be incorporated by reference.

1003.10.2 CHIEF OF POLICE RESPONSIBILITIES

Upon receipt of any written recommendation for disciplinary action, the Chief of Police shall review the recommendation and all accompanying materials. The Chief of Police may modify any recommendation and/or may return the file to the Division Commander for further investigation or action.

Once the Chief of Police is satisfied that no further investigation or action is required by staff, the Chief of Police shall determine the amount of discipline, if any, that should be imposed. In the event disciplinary action is proposed, the Chief of Police shall provide the member with a written notice and the following:

- (a) Access to all of the materials considered by the Chief of Police in recommending the proposed discipline.
- (b) An opportunity to respond orally or in writing to the Chief of Police within five days of receiving the notice.
 - 1. Upon a showing of good cause by the member, the Chief of Police may grant a reasonable extension of time for the member to respond.
 - 2. If the member elects to respond orally, the presentation shall be recorded by the Department. Upon request, the member shall be provided with a copy of the recording.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

Once the member has completed his/her response or if the member has elected to waive any such response, the Chief of Police shall consider all information received in regard to the recommended discipline. The Chief of Police shall render a timely written decision to the member and specify the grounds and reasons for discipline and the effective date of the discipline. Once the Chief of Police has issued a written decision, the discipline shall become effective.

1003.10.3 MINNESOTA POST INVESTIGATIONS

The Minnesota POST Board may require an administrative investigation based upon a complaint alleging a violation of a statute or rule that the board is empowered to enforce.

Any such misconduct allegation or complaint assigned to this department shall be completed and a written summary submitted to the POST executive director within 30 days of the order for inquiry (Minn. Stat. § 214.10, Subd. 10).

The Department shall cooperate with POST's investigation and provide requested information unless (Minn. Stat. § 626.8457):

- (a) There is an active criminal investigation or active criminal proceeding regarding the same incident or misconduct that is being investigated by POST.
- (b) An active internal investigation exists regarding the same incident or misconduct that is being investigated by POST during 45 days from the time the request was made by POST. The Chief of Police or the authorized designee shall comply with the request upon completion of the internal investigation or once 45 days has passed, whichever occurs first.

1003.10.4 DISCIPLINE

Disciplinary action may include, but is not limited to (Minn. R. 6700.2200):

- (a) Oral reprimand.
- (b) Written reprimand.
- (c) Suspension.
- (d) Demotion.
- (e) Discharge.

1003.10.5 NOTICE OF FINAL DISPOSITION TO THE COMPLAINANT

The Chief of Police or the authorized designee shall ensure that the complainant is notified of the disposition (i.e., sustained, not sustained, exonerated, unfounded) of the complaint. Notice must be consistent with the provisions of the MGD (Minn. Stat. § 13.43, Subd. 2; Minn. R. 6700.2200).

1003.10.6 CIVILIAN OVERSIGHT COUNCIL

When applicable, the Chief of Police or the authorized designee shall cooperate with the designated civilian oversight council, as appropriate (Minn. Stat. § 626.89, Subd. 17).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Complaints

1003.11 RESIGNATIONS/RETIREMENTS PRIOR TO DISCIPLINE

In the event that a member tenders a written resignation or notice of retirement prior to the imposition of discipline, it shall be noted in the file. The tender of a resignation or retirement by itself shall not serve as grounds for the termination of any pending investigation or discipline.

1003.12 PROBATIONARY EMPLOYEES AND OTHER MEMBERS

At-will and probationary employees and members other than non-probationary employees may be disciplined and/or released from employment without adherence to any of the procedures set out in this policy, and without notice or cause at any time. These individuals are not entitled to any rights under this policy except for employees covered by the Veterans Preference Act (Minn. Stat. § 197.46). However, any of these individuals released for misconduct should be afforded an opportunity solely to clear their names through a liberty interest hearing, which shall be limited to a single appearance before the Chief of Police or the authorized designee (Minn. R. 6700.2200).

Any probationary period may be extended at the discretion of the Chief of Police in cases where the individual has been absent for more than a week or when additional time to review the individual is considered to be appropriate.

1003.13 RETENTION OF PERSONNEL INVESTIGATION FILES

All personnel complaints shall be maintained in accordance with the established records retention schedule and as described in the Personnel Records Policy.

1003.13.1 CONFIDENTIALITY OF PERSONNEL FILES

All active investigations of alleged misconduct and personnel complaints shall be considered confidential and maintained separately from peace officer personnel files. The contents of such files shall not be revealed to other than the involved member or authorized personnel, except pursuant to lawful process, such as Minn. R. 6700.2500. Data in closed files shall be treated as private or public data depending on whether discipline was imposed upon the member.

1003.13.2 LETTERS OF DISCIPLINE AND REPRIMANDS

Letters of discipline and reprimands may only be placed in a member's personnel file after they are received by the member (see generally Minn. Stat. § 626.89, Subd. 13).

1003.14 REQUIRED REPORTING TO POST

The Chief of Police or the authorized designee shall notify POST of certain officer personnel events, including but not limited to:

- (a) A termination or resignation of an officer who is the subject of an internal or criminal investigation due to alleged misconduct regardless of whether the investigation has been initiated or completed, or whether the officer was criminally charged (Minn. Stat. § 626.8457, Subd. 4).
- (b) The violation of a required POST model policy identified in Minn. R. 6700.1615 (Minn. R. 6700.1615, Subd. 2).

Seat Belts

1004.1 PURPOSE AND SCOPE

This policy establishes guidelines for the use of seat belts and child restraints. This policy will apply to all members operating or riding in department vehicles (Minn. Stat. § 169.686).

Guidance for transporting persons in custody may be found in the Transporting Persons in Custody and Handcuffing and Restraints policies.

1004.1.1 DEFINITIONS

Child Passenger Safety Seat System - An infant or child passenger restraint system that meets Federal Motor Vehicle Safety Standards set forth in 49 CFR Part 571 (Minn. Stat. § 169.685 Subd. 5 (e)).

1004.2 WEARING OF SAFETY RESTRAINTS

All members shall wear properly adjusted safety restraints when operating or riding in a seat equipped with restraints, in any vehicle owned, leased or rented by this department while on- or off-duty, or in any privately owned vehicle while on-duty. The member driving such a vehicle shall ensure that all other occupants, including those who are not members of the Department, are properly restrained (Minn. Stat. § 169.686).

Exceptions to the requirement to wear safety restraints may be made only in exceptional situations where, due to unusual circumstances, wearing a seat belt would endanger the department member or the public. Members must be prepared to justify any deviation from this requirement.

1004.2.1 TRANSPORTING CHILDREN

An approved child passenger safety seat system should be used for all children younger than 8 years of age and shorter than 4 feet 9 inches tall (Minn. Stat. § 169.685 Subd. 5 (b)).

However, if a child passenger restraint is not available, an officer may transport the child using the standard seat belt (Minn. Stat. § 169.685 Subd. 6 (a) (2)).

Rear seat passengers in a cage-equipped vehicle may have reduced clearance which requires careful seating and positioning of seat belts. Due to this reduced clearance, children and the child passenger safety seat system or booster seat should be secured properly in the front seat of these vehicles, provided this positioning meets the vehicle and the child passenger safety seat system manufacturer's design and use recommendations. In the event that a child is transported in the front seat of a vehicle, the passenger side air bag should be deactivated. If this is not possible, officers should consider arranging alternative transportation.

1004.3 INOPERABLE SEAT BELTS

Department vehicles shall not be operated when the seat belt in the driver's position is inoperable. Persons shall not be transported in a seat in which the seat belt is inoperable.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Seat Belts

Department vehicle seat belts shall not be modified, removed, deactivated or altered in any way, except by the vehicle maintenance and repair staff, who shall do so only with the express authorization of the Chief of Police.

Members who discover an inoperable restraint system shall report the defect to the appropriate supervisor. Prompt action will be taken to replace or repair the system.

1004.4 VEHICLES MANUFACTURED WITHOUT SEAT BELTS

Vehicles manufactured and certified for use without seat belts or other restraint systems are subject to the manufacturer's operator requirements for safe use.

1004.5 VEHICLE AIRBAGS

In all vehicles equipped with airbag restraint systems, the system will not be tampered with or deactivated, except when transporting children as written elsewhere in this policy. All equipment installed in vehicles equipped with airbags will be installed as per the vehicle manufacturer specifications to avoid the danger of interfering with the effective deployment of the airbag device.

Body Armor

1005.1 PURPOSE AND SCOPE

The purpose of this policy is to provide law enforcement officers with guidelines for the proper use of body armor.

1005.2 POLICY

It is the policy of the South Saint Paul Police Department to maximize officer safety through the use of body armor in combination with prescribed safety procedures. While body armor provides a significant level of protection, it is not a substitute for the observance of officer safety procedures.

1005.3 ISSUANCE OF BODY ARMOR

The Operations Lieutenant shall ensure that body armor is issued to all officers when the officer begins service at the South Saint Paul Police Department and that, when issued, the body armor meets or exceeds the standards of the National Institute of Justice.

The Operations Lieutenant shall establish a body armor replacement schedule and ensure that replacement body armor is issued pursuant to the schedule or whenever the body armor becomes worn or damaged to the point that its effectiveness or functionality has been compromised.

1005.3.1 USE OF SOFT BODY ARMOR

Generally, the use of body armor is required subject to the following:

- (a) Officers shall only wear agency-approved body armor.
- (b) Officers shall wear body armor anytime they are in a situation where they could reasonably be expected to take enforcement action.
- (c) Officers may be excused from wearing body armor when they are functioning primarily in an administrative or support capacity and could not reasonably be expected to take enforcement action.
- (d) Body armor shall be worn when an officer is working in uniform.
- (e) An officer may be excused from wearing body armor when he/she is involved in undercover or plainclothes work that his/her supervisor determines could be compromised by wearing body armor, or when a supervisor determines that other circumstances make it inappropriate to mandate wearing body armor.

1005.3.2 INSPECTIONS OF BODY ARMOR

Supervisors should ensure that body armor is worn and maintained in accordance with this policy through routine observation and periodic documented inspections. Annual inspections of body armor should be conducted by an authorized designee for fit, cleanliness and signs of damage, abuse and wear.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Body Armor

1005.3.3 CARE AND MAINTENANCE OF SOFT BODY ARMOR

Soft body armor should be cared for and cleaned pursuant to the manufacturer's care instructions provided with the soft body armor. The instructions can be found on labels located on the external surface of each ballistic panel. The carrier should also have a label that contains care instructions. Failure to follow these instructions may damage the ballistic performance capabilities of the armor. If care instructions for the soft body armor cannot be located, contact the manufacturer to request care instructions.

Soft body armor should not be exposed to any cleaning agents or methods not specifically recommended by the manufacturer, as noted on the armor panel label.

1005.4 OPERATIONS LIEUTENANT RESPONSIBILITIES

The Operations Commander should:

- (a) Monitor technological advances in the body armor industry for any appropriate changes to Department approved body armor.
- (b) Assess weapons and ammunition currently in use and the suitability of approved body armor to protect against those threats.

Personnel Records

1006.1 PURPOSE AND SCOPE

This policy governs maintenance and access to personnel data. Personnel data includes any file maintained under an individual member's name.

Without regard to where and how stored, all data about a current or former employee or applicant for employment shall be defined and classified as personnel data consistent with Minn. Stat. § 13.43. All data relating to a criminal investigation of a current or former employee or applicant shall be defined and classified as criminal data consistent with Minn. Stat. § 13.82.

1006.2 DEPARTMENT FILE

The department file shall be maintained as a record of a person's employment/appointment with this department. The department file should contain, at a minimum:

- (a) Personal data, including photographs, marital status, names of family members, educational and employment history or similar information. A photograph of the member should be permanently retained.
- (b) Election of employee benefits.
- (c) Personnel action reports reflecting assignments, promotions and other changes in employment/appointment status. These should be permanently retained.
- (d) Original performance evaluations. These should be permanently maintained.
- (e) Discipline records, including copies of sustained personnel complaints.
- (f) Adverse comments such as supervisor notes or memos may be retained in the department file after the member has had the opportunity to read and initial the comment.
 - 1. Once a member has had an opportunity to read and initial any adverse comment, the member shall be given the opportunity to respond in writing to the adverse comment.
 - 2. Any member response shall be attached to and retained with the original adverse comment.
 - 3. If a member refuses to initial or sign an adverse comment, at least one supervisor should note the date and time of such refusal on the original comment. Such a refusal, however, shall not be deemed insubordination, nor shall it prohibit the entry of the adverse comment into the member's file.
- (g) Commendations and awards.
- (h) Any other information, the disclosure of which would constitute an unwarranted invasion of personal privacy.

1006.3 DIVISION FILE

Division files may be separately maintained internally by a member's supervisor for the purpose of completing timely performance evaluations. The Division file may contain supervisor comments,

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Records

notes, notices to correct and other materials that are intended to serve as a foundation for the completion of timely performance evaluations.

1006.4 TRAINING FILE

An individual training file shall be maintained by the Support Services Commander for each member. Training files will contain records of all training; original or photocopies of available certificates, transcripts, diplomas and other documentation; and education and firearms qualifications. Training records may also be created and stored remotely, either manually or automatically (e.g., Daily Training Bulletin (DTB) records).

- (a) The involved member is responsible for providing the Support Services Commander or immediate supervisor with evidence of completed training/education in a timely manner.
- (b) The Support Services Commander or supervisor shall ensure that copies of such training records are placed in the member's training file.

1006.5 INTERNAL AFFAIRS FILE

Internal affairs files shall be maintained under the exclusive control of the Support Services Commander in conjunction with the office of the Chief of Police. Access to these files may only be approved by the Chief of Police or the Support Services Commander supervisor.

These files shall contain the complete investigation of all formal complaints of member misconduct, regardless of disposition. Investigations of complaints that result in the following findings shall not be placed in the member's department file but will be maintained in the internal affairs file:

- (a) Not sustained
- (b) Unfounded
- (c) Exonerated

1006.6 MEDICAL FILE

A private medical file shall be maintained separately from all other personnel data and shall contain all documents relating to the member's medical condition and history, including but not limited to:

- (a) Materials relating to a medical leave of absence, including leave under the Family and Medical Leave Act (FMLA).
- (b) Documents relating to workers' compensation claims or the receipt of short- or long-term disability benefits.
- (c) Fitness-for-duty examinations, psychological and physical examinations, follow-up inquiries and related documents.
- (d) Medical release forms, doctor's slips and attendance records that reveal a member's medical condition.
- (e) Any other documents or materials that reveal the member's medical history or medical condition, including past, present or future anticipated mental, psychological or physical limitations.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Records

1006.7 EMPLOYEE ASSISTANCE PROGRAMS

Employee assistance records must be kept separate from personnel records and shall not become part of an employee's personnel file (Minn. Stat. § 181.980, Subd. 3).

1006.8 SECURITY

Personnel data should be maintained in a secured location and locked either in a cabinet or access-controlled room. Personnel data maintained in an electronic format should have adequate password protection.

Any personnel data not deemed public data is private and shall not be subject to disclosure except as provided in this policy, the Records Maintenance and Release Policy, according to applicable discovery procedures or with the member's written consent (Minn. Stat. § 13.43; Minn. Stat. § 181.967, Subd. 4).

Nothing in this policy is intended to preclude review of personnel data by the City Administrator, City Attorney or other attorneys or representatives of the City in connection with official business.

1006.8.1 REQUESTS FOR DISCLOSURE

Any member receiving a request for personnel data shall promptly notify the Custodian of Records or other person charged with the maintenance of such data.

Upon receipt of any such request, the responsible person shall notify the affected member as soon as practicable that such a request has been made.

The responsible person shall further ensure that an appropriate response to the request is made in a timely manner, consistent with applicable law. In many cases, this may require assistance of available legal counsel.

All requests for disclosure that result in access to a member's personnel data shall be logged in the corresponding file.

1006.8.2 RELEASE OF PRIVATE DATA

Except as provided by this policy, pursuant to lawful process, pursuant to state law or court order, no private data shall be disclosed without the written consent of the employee or written authorization of the Chief of Police designee (Minn. Stat. § 13.43; Minn. Stat. § 181.967, Subd. 4).

1006.9 MEMBER ACCESS TO HIS/HER OWN PERSONNEL RECORDS

Upon request, any member may request access to his/her own personnel file as set forth in Minn. Stat. § 181.961.

Any member seeking the removal of any item from his/her personnel files shall file a written request to the Chief of Police through the chain of command. The Department shall remove any such item if appropriate, or within 30 days provide the member with a written explanation of why the contested item will not be removed. If the contested item is not removed from the file, the member's request and the written response from the Department shall be retained with the contested item in the member's corresponding personnel file. If the contested item is ultimately removed, the written

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personnel Records

responses shall also be removed (Minn. Stat. § 181.962, Subd. 1). An employee not satisfied with this resolution may seek such other remedies as are authorized by the MGDPA.

Members may be restricted from accessing files containing any of the following information:

- (a) An ongoing internal affairs investigation to the extent that it could jeopardize or compromise the investigation pending final disposition or notice to the member of the intent to discipline.
- (b) Confidential portions of internal affairs files that have not been sustained against the member.
- (c) Letters of reference concerning employment/appointment, licensing or issuance of permits regarding the member.
- (d) Any portion of a test document, except the cumulative total test score for either a section of the test document or for the entire test document.
- (e) Materials used by the Department for staff management planning, including judgments or recommendations concerning future salary increases and other wage treatments, management bonus plans, promotions and job assignments or other comments or ratings used for department planning purposes.
- (f) Information of a personal nature about a person other than the member if disclosure of the information would constitute a clearly unwarranted invasion of the other person's privacy.
- (g) Records relevant to any other pending claim between the Department and the member that may be discovered in a judicial proceeding.

1006.10 RETENTION AND PURGING

Unless provided otherwise in this policy, personnel data shall be maintained in accordance with the established records retention schedule.

- (a) During the preparation of each member's performance evaluation, all personnel complaints and disciplinary actions should be reviewed to determine the relevancy, if any, to progressive discipline, training and career development. Each supervisor responsible for completing the member's performance evaluation should determine whether any prior sustained disciplinary file should be retained beyond the required period for reasons other than pending litigation or other ongoing legal proceedings.
- (b) If a supervisor determines that records of prior discipline should be retained beyond the required period, approval for such retention should be obtained through the chain of command from the Chief of Police.
- (c) If, in the opinion of the Chief of Police, a personnel complaint or disciplinary action maintained beyond the required retention period is no longer relevant, all records of such matter may be destroyed in accordance with the established records retention schedule.

Commendations and Awards

1007.1 PURPOSE AND SCOPE

Special recognition may be in order whenever an employee performs his/her duties in an exemplary manner. Citizens may at times perform a meritorious act that deserves recognition. This procedure provides general guidelines for the commending of exceptional employee performance or meritorious acts by citizens.

1007.2 WHO MAY MAKE COMMENDATIONS

Any member of this department may request that another member be recognized for their extraordinary conduct or work product. The requesting officer will write a letter describing the exceptional work or conduct and submit it to the chief of police or his designee. The chief or designee will then approve or deny the request and determine what level of recognition the recipient should receive. Citizen requests for officer recognition or officer requests for citizen recognition will be handled in the same manner.

A written commendation may also be made by a member of the public regarding any Department employee.

Written recommendations for a citizen's meritorious acts may be made by any member of this department or any member of the public.

1007.3 LEVELS OF RECOGNITION

Letter of Appreciation: A letter issued to a sworn officer, or civilian employee, acknowledging an event that reflects the recipient's faithful service and ongoing dedication to their position.

Certificates of Commendation: A certificate issued to a sworn officer, civilian employee, or civilian, acknowledging the recipient's creativity, hard work and resolve during a particular case, project or assignment.

Chief's Achievement Award: An award issued to a sworn officer, group of officers, or civilian, acknowledging their resourcefulness and willingness to go above and beyond the call of duty on a daily basis to achieve a particular goal or result.

Meritorious Service Award: The award shall recognize incident(s) wherein the officer's or civilian's courage, diligence and perseverance goes beyond that which is normally encountered in the protection of life, property and/or the apprehension of a dangerous criminal.

Life Saving Award: An award issued to an officer or civilian for their intervention in a life and death situation where their actions were directly responsible for the preservation of human life.

Valor Award: The highest award issued to a sworn officer, where the actions of said officer, clearly went above and beyond the call of duty and involved significant self-sacrifice or great personal risk to the officer.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Commendations and Awards

1007.3.1 CITIZEN RECOGNITION

Letters of Appreciation: Civilians may be awarded letters of appreciation for their general participation in police department projects or their support of the department's overall mission.

Certificate of Achievement: Certificates of Achievement may be issued to a civilian or citizen for achieving a department goal involving dedication, resourcefulness and some measure of self-sacrifice.

1007.3.2 ADDITIONAL COMMENDATIONS

Recognition of seniority: Sworn personnel will be issued the blue and gold seniority pin. A solid blue bar will be issued after one year of continued service. Blue bars with gold stars will be issued later. Each star will represent five years of the employee's continued service.

Recognition of military service: Sworn personnel who have served in the United States Armed Forces, and have been honorably discharged, will be issued the military pin corresponding with their branch of service.

Recognition of specialized service: Sworn officers who have served in any of the following categories, for the designated time period, will be recognized for their specialized areas of service with a service pin. The single pin will have a number displayed, signifying the number of specialized units the officer has served with.

- Investigations One year
- SWAT / Negotiator One Year
- School Resource Officer One (school) year
- Drug Task Force One Year
- DARE One complete DARE cycle
- Firearms Instructor Three years
- Use of Force Instructor Three years
- Armorer Three years
- Property Officer Three Years
- Mobile Field Force Three Years
- Community Engagement Officer/Mental Health Officer One Year
- Primary Explorer Advisor One Year
- Peer Support Officer Three Years
- Social Media Coordinator Three Years

Recognition of Field Training Officer: Recognizing that the training officer is a crucial element of the police recruit's development, each field training officer will be awarded an approved FTO pin.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Commendations and Awards

Recognition of Canine Officer: Recognizing that a canine officer is a full time responsibility, each canine officer will be awarded an approved K9 pin.

Authority: All recognition will be awarded and distributed by the authority of the Chief of Police or his designee. With the exception of the seniority pin, all awards will be accompanied by a certificate, signed by the Chief of Police, or his designee, outlining the reason for the award.

Uniform display of awards and pins: Service and seniority pins will be worn on the right hand pocket of the uniform shirt, directly below the flag. Awards will be worn on the left hand pocket of the uniform shirt, directly below the badge. The highest award will be worn on top with the rest of the awards being worn in descending order.

1007.3.3 RECOMMENDATION FOR CITATION FORM

The Recommendation for Citation Form shall be used to document the commendation of the employee and shall contain the following: Employee name, bureau and assignment at the date and time of the commendation. A brief account of the commendable action with report numbers, as appropriate. Signature of the commending supervisor. Completed reports should be forwarded to the appropriate Division Commander for review. The Division Commander shall sign and forward the report to the Chief of Police for review. The Chief of Police will return the commendation to the employee for signature. The report will then be returned to the administrative secretary for entry into the employee's personnel file.

Fitness for Duty

1008.1 PURPOSE AND SCOPE

All officers are required to be free from any physical, emotional or mental condition that might adversely affect the exercise of peace officer duties. The purpose of this policy is to ensure that all officers of this department remain fit for duty and able to perform their job functions.

1008.2 EMPLOYEE RESPONSIBILITIES

- (a) It shall be the responsibility of each member of this department to maintain good physical condition sufficient to safely and properly perform essential duties of the position.
- (b) Each member of this department shall perform his/her respective duties without physical, emotional and/or mental constraints.
- (c) During working hours, all employees are required to be alert, attentive and capable of performing assigned responsibilities.
- (d) Any employee who feels unable to perform his/her duties shall promptly notify a supervisor. In the event that an employee believes that another employee is unable to perform his/her duties, such observations and/or belief shall be promptly reported to a supervisor.

1008.3 SUPERVISOR RESPONSIBILITIES

- (a) A supervisor observing an employee, or receiving a report of an employee, who is perceived to be unable to safely perform his/her duties due to a physical, medical or mental condition shall take prompt and appropriate action in an effort to resolve the situation.
- (b) Whenever feasible, the supervisor should attempt to ascertain the reason or source of the problem and in all cases a preliminary evaluation should be made to determine the level of inability of the employee to perform his/her duties.
- (c) In the event the employee appears to be in need of immediate medical or psychiatric treatment, all reasonable efforts should be made to provide such care.
- (d) In conjunction with the supervisor or the employee's available Division Commander, a determination should be made whether the employee should be temporarily relieved from his/her duties.
- (e) The Chief of Police shall be promptly notified in the event that any employee is relieved from duty.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Fitness for Duty

1008.4 NON-WORK RELATED CONDITIONS

Any employee suffering from a non-work related condition that warrants a temporary relief from duty may be required to use sick leave or other paid time off in order to obtain medical treatment or other reasonable rest period.

1008.5 WORK RELATED CONDITIONS

Any employee suffering from a work-related condition that warrants a temporary relief from duty shall be required to comply with personnel rules and guidelines for processing such claims.

Upon the recommendation of the supervisor and concurrence of a Division Commander, any employee whose actions or use of force in an official capacity result in death or serious injury to another may be temporarily removed from regularly assigned duties and/or placed on paid administrative leave for the well-being of the employee and until such time as the following may be completed:

- (a) A preliminary determination that the employee's conduct appears to be in compliance with policy and law.
- (b) If appropriate, the employee has had the opportunity to receive necessary counseling and/or psychological clearance to return to full duty.

1008.6 PHYSICAL AND PSYCHOLOGICAL EXAMINATIONS

- (a) Whenever circumstances reasonably indicate that an employee is unfit for duty, the Chief of Police may serve that employee with a written order to undergo a physical and/or psychological examination in cooperation with the Department of Human Resources to determine the level of the employee's fitness for duty. The order shall indicate the date, time and place for the examination.
- (b) The examining physician or therapist will provide the Department with a report indicating that the employee is either fit for duty or, if not, list any functional limitations that limit the employee's ability to perform job duties. If the employee places his/her condition at issue in any subsequent or related administrative action or grievance, the examining physician or therapist may be required to disclose any and all information that is relevant to such proceeding.
- (c) To facilitate the examination of any employee, the Department will provide all appropriate documents and available information to assist in the evaluation and/or treatment.
- (d) All reports and evaluations submitted by the treating physician or therapist shall be part of the employee's private medical file.
- (e) Any employee ordered to receive a fitness for duty examination shall comply with the terms of the order and cooperate fully with the examining physician or therapist regarding any clinical interview, tests administered or other procedures as directed. Any failure to comply with such an order and any failure to cooperate with the

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Fitness for Duty

examining physician or therapist may be deemed insubordination and may subject the employee to discipline up to and including termination.

- (f) Once an employee has been deemed fit for duty by the examining physician or therapist, the employee will be notified to resume his/her duties.
- (g) If an employee is deemed unfit for duty by the Department, the employee may submit a report from the employee's personal physician, psychiatrist, psychologist or other health care provider that will be taken into consideration.

1008.7 LIMITATION ON HOURS WORKED

Absent emergency operations, members should not work more than:

- 16 hours in one day (24 hour) period or
- 30 hours in any two day (48 hour) period or
- 84 hours in any seven day (168 hour) period

Except in very limited circumstances members should have a minimum of eight hours off between shifts. Supervisors should give consideration to reasonable rest periods and are authorized to deny overtime or relieve to off-duty status any member who has exceeded the above guidelines.

Limitations on the number of hours worked apply to shift changes, shift trades, rotation, holdover, training, special events, contract work, general overtime and any other work assignments.

1008.8 APPEALS

An employee who is separated from paid employment or receives a reduction in salary resulting from a fitness for duty examination shall be entitled to an administrative appeal as outlined in the Conduct Policy.

Lactation Breaks

1009.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance regarding reasonable accommodations for lactating members.

1009.2 POLICY

It is the policy of the South Saint Paul Police Department to provide, in compliance with federal and state law, reasonable accommodations for lactating members. This includes break time and appropriate facilities to accommodate any member desiring to express breast milk (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Minn. Stat. § 181.939).

1009.3 LACTATION BREAK TIME

A rest period should be permitted each time the member requires a lactation break (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3). In general, lactation breaks that cumulatively total 30 minutes or less during any four-hour work period or major portion of a four-hour work period would be considered reasonable. However, individual circumstances may require more or less time.

Lactation breaks may be taken at the same time as the member's regularly scheduled rest or meal periods (Minn. Stat. § 181.939).

Members desiring to take a lactation break shall notify the dispatcher or supervisor prior to taking such a break.

Once a lactation break has been approved, the break should not be interrupted except for emergency or exigent circumstances.

1009.4 PRIVATE LOCATION

The Department will make reasonable efforts to accommodate members with the use of an appropriate room or other location to express milk in private. Such room or place should be in proximity to the member's work area and shall be other than a bathroom or toilet stall. The location must be shielded from view, free from intrusion from coworkers and the public, and otherwise satisfy the requirements of federal and state law (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Minn. Stat. § 181.939).

Members occupying such private areas shall either secure the door or otherwise make it clear to others that the area is occupied with a need for privacy. All other members should avoid interrupting a member during an authorized break, except to announce an emergency or other urgent circumstance.

Authorized lactation breaks for members assigned to the field may be taken at the nearest appropriate private area.

1009.5 STORAGE OF EXPRESSED MILK

Any member storing expressed milk in any authorized refrigerated area within the Department shall clearly label it as such and shall remove it when the member's shift ends.

Call Back Procedure; Voluntary and Mandatory

1010.1 PURPOSE AND SCOPE

Purpose: To establish guidelines allowing for, as far as is practicable and without reducing efficiency, a system to distribute overtime call back opportunities among all eligible officers in a fair and equitable manner.

Scope: Applies to all sworn officers of the South St. Paul Police Department below the rank of Commander certified for solo patrol.

Discussion: Generally, the voluntary and mandatory call back procedures will be used for the purpose of staffing shortages resulting from sick leave usage, training, special assignment, or other causes. Two separate call back lists will be maintained, one to be used for voluntary call backs and the other for mandatory call backs. Nothing in this policy precludes the on-duty supervisor from deviating from this policy should time constraints or other good reasons dictate.

1010.2 PROCEDURES

1010.2.1 GENERAL PROVISIONS

1. The shift supervisor or officer in charge is responsible for conducting call backs. The call back may be made by the supervisor's designee when circumstances dictate.
2. The departmental mass communication system is the default method for conducting a call back, although circumstances will exist where manually calling utilizing the call back list will happen. A callback may be completed in advance of an known shortage by department email or mass communication system.
3. The initial voluntary and mandatory call back list will be created using department seniority. The most senior officer will have his or her name appear first on the voluntary call back list followed, in order, by officers with less department seniority. The least senior officer will have his or her name appear first on the mandatory call back list followed, in order, by officers with more department seniority. The starting point for the subsequent call backs will begin with the officer at the top of the call back list and the officer who works or is assigned to the overtime will be placed at the bottom of the list.
4. Generally, when a shift shortage is anticipated in advance of the actual shortage the call back will be made more than 24 hours prior to the start of the actual shortage. However, the chief of police or designee may authorize a call back at any time on a case-by-case basis as circumstances may dictate.
5. The chief of police or designee will not use the call back list if circumstances require an officer with specialized training, experience, qualifications, or response time to meet the needs of the department or of a particular assignment.
6. Officers scheduled for duty during a voluntary overtime shift, or who are assigned to work a special detail, scheduled for training, or court during the overtime shift shall not be considered for

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Call Back Procedure; Voluntary and Mandatory

the overtime shift. Such officers maintain their position on the call back list. Any exceptions must be approved by command staff.

7. When the need for a particular overtime shift ceases to exist, for example when an officer returns from court, training, or a special detail, or the overtime shift is canceled; the supervisor or designee has the authority to relieve the overtime officer from duty or cancel the overtime officer. In this situation the officer accepting the overtime shift will be compensated per the contractual agreement and not by what the anticipated hours of the overtime shift would have been.

8. An officer is not eligible to accept a voluntary overtime shift if using approved benefit time during the hours of the overtime shift. For the purposes of this policy "Kelly Hours" are not considered benefit time.

9. Officers on sick leave will not be eligible to accept a volunteer overtime shift unless twenty-four hours have elapsed since the beginning of the last shift during which sick leave benefit was used.

10. In general, officers may work sixteen continuous hours but must be off a minimum of eight hours between their shifts ending time and the start time of their next scheduled shift. Any exceptions must be approved by command staff.

11. Officers may not volunteer to work an overtime shift if they have less than eight hours off in a twenty-four-hour period without the approval of the chief of police or designee.

12. Officers may use benefit time on their scheduled shift so that they may work an overtime shift provided their benefit usage has been approved according to established guidelines and procedures and the benefit usage does not cause an overtime shift of the officer's regularly scheduled shift.

13. Officers suspected of manipulating the call back procedure for their own financial gain or that of another will be subject to discipline.

14. Officers may list a primary and secondary telephone number for the purposes of the voluntary or mandatory call back lists. The same telephone numbers will apply to both lists and, in the event of a manual call back, both numbers will be called before moving on to the next officer on the list.

15. In the event of a manual call back, if there is no answer or a busy signal is received at the telephone number(s) listed by the officer the calling officer will so note on the call back list continuing with the call back.

16. In the event of a manual call back, if the call is forwarded to a voice mail box or is answered by another individual the officer conducting the call back will leave a message noting the current time and the date and time of the overtime shift.

17. In the event of a manual call back, prior to conducting a voluntary call back the officer making the call back should determine each officer's status relative to a possible mandatory call back and put those officers that may become subject to mandatory overtime, should it become necessary, on notice at the time of the voluntary call out. As soon as is practical after the voluntary call back is completed the calling officer will re-contact all officers put on notice to confirm their mandatory

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Call Back Procedure; Voluntary and Mandatory

status or release them. Officers put on notice should assume that they are assigned to work mandatory overtime until released.

18. Every two years the mandatory and voluntary call back lists will be reset at the beginning of a bid cycle. The voluntary list will reset from most senior officer to least senior officer. The mandatory list will reset from least senior officer to most senior officer. If an officer becomes certified for solo patrol prior to a reset year he or she will fall to the bottom of the list on the voluntary callback roster or at the top of the mandatory call back roster at the time of their solo patrol certification.

1010.3 VOLUNTARY CALL BACK

Call back conducted by mass communication technology:

(a) When an overtime shift exists, the calling officer will send out a communication to all eligible officers via the departmental mass notification tool that includes

(a) The date and time(s) of the overtime shift

(b) The contact number for the officer initiating the communication

(c) The deadline for responding directly back to the initiating officer

(b) The calling officer will tally the responses received, assign the overtime shift to the officer standing highest on the list, and communicate back to all responding with interest who was assigned the shift.

(c) In the event the initial mass notification fails to produce a response, a second notification will be sent.

(d) In the event the second mass notification fails to produce a response, the overtime shift will move to the mandatory callback list.

(e) If the overtime shift is filled using the voluntary call back list, the calling officer will record who was assigned the shift and that Officer will move to the bottom of the list for the future voluntary overtime shifts. The officer falling at the top of the voluntary call back will be the first eligible officer to the next voluntary call back.

Call back conducted manually using the call back list

1. When an overtime shift exists, and the calling officer is unable to use the mass notification system, the calling officer will begin the call back using the voluntary call back list with the starting point being the officer whose name appears on the top of the list.

2. If an officer agrees to work the overtime shift the overtime shift will be considered filled.

3. If there are no officers willing to accept the entire overtime shift but there are officers willing to work either the first or second half of the overtime shift, they will be assigned the overtime shift by their position on the voluntary call back list. Once this is done, the shortage will be filled. The next voluntary call back will begin with the officer who falls at the top of the list.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Call Back Procedure; Voluntary and Mandatory

1010.4 MANDATORY CALL BACK

1. Generally, the mandatory call back list will be used for filling shift shortages. However, the chief of police or designee may order any officer, without regard to the mandatory call back list, to work overtime for mandatory call backs or in any situation deemed to be an emergency. Additionally, the chief of police or designee can direct a particular officer or officers who, because of specialized training, experience or other qualifications required to meet the needs of the department; to work overtime on a mandatory callback or in a situation deemed to be an emergency.
2. As outlined in the section policy, a separate mandatory call back list will be maintained with officers listed by department seniority least senior to most senior. The mandatory call back list will be used to fill a shortage when no officer can be found that is willing to accept the overtime shift on a voluntary basis.
3. If an overtime shift is four hours or less, an officer from the shift on duty immediately preceding the shift having the shortage will have his or her shift extended to cover the shortage and/or an officer scheduled to work on the shift immediately following the shift containing the shortage will have his or her shift extended to cover the shortage. If an overtime shift is eight hours or less, an officer from the shift on duty immediately preceding the shift having the shortage will have his or her shift extended to cover the first part of the shortage and/or an officer scheduled to work on the shift immediately following the shift containing the shortage will have his or her shift extended to cover the last part of the shortage. The selection of the officer that will have their shift extended will be determined by their position on the voluntary callback list. Officers mandated to stay up to a four-hour extension of their shift to fill a shortage will move from their perspective position on the voluntary call back list to the bottom of the list. If a circumstance occurs where no officer is scheduled either immediately before or immediately after the shortage, the first off-duty officer (e.g. whose work schedule does not exceed sixteen hours within a twenty-four hour period; is not scheduled for court, training, or a department detail, etc.) on the mandatory callback will be mandated to cover the entire shortage. If an off-duty officer is mandated to cover a four-hour shift, their name will move to the bottom of the list.
4. If the overtime shift is more than four hours and cannot be filled by on duty staff, using the mandatory callback list, the first off-duty officer eligible (e.g. whose work schedule does not exceed sixteen hours within a twenty-four hour period; is not scheduled for court, training, or a department detail, etc.) following the mandated list will be assigned the mandatory overtime shift. The next mandatory call back will begin with the officer whose name falls at the top of the mandatory overtime list.
5. If the off-duty officer who would have been mandated to work the overtime shift cannot be located, the first eligible off-duty officer located will be mandated to work the overtime shift. The next mandatory call back will begin with the officer whose name falls at the top of the list. The officer whose name is at the top of the mandatory call back list will remain as the first call for mandatory overtime until that officer works a mandatory overtime shift.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Call Back Procedure; Voluntary and Mandatory

6. Generally, officers assigned to other units such as investigations or school resource will not be mandated to work a patrol shift shortage unless the assigned shift does not conflict with their normal duties but can be at the direction of the chief of police or designee.

7. If an officer contacted for assignment to mandatory overtime indicates that he or she is ill and unable to meet the mandatory obligation, that officer may be required to supply a physician's slip indicating the illness, any treatment received as well as a medical clearance to return to work. In all instances the officer, upon reporting for his or her next scheduled tour of duty, shall complete a written memo submitted to the Patrol Commander containing all facts and relevant information on the illness causing the officer's inability to report for the mandatory overtime shift.

8. If an officer contacted for assignment to mandatory overtime indicates that he or she is not available and unable to meet the mandatory obligation for any other reason, that officer shall complete a written memo submitted to the Patrol Commander upon reporting for his or her next scheduled tour of duty. The memo shall contain all facts and relevant information justifying the officer's inability to report for the mandatory overtime shift.

Outside Employment

1011.1 PURPOSE AND SCOPE

To avoid actual or perceived conflicts of interest for Department employees engaging in outside employment, all employees shall initially obtain approval from the Chief of Police prior to engaging in any outside employment. Approval of outside employment shall be at the discretion of the Chief of Police in accordance with the provisions of this policy.

1011.1.1 DEFINITIONS

Outside Employment - The employment of any member of this department who receives wages, compensation or other consideration of value from another employer, organization or individual not affiliated directly with this department for services, product(s) or benefits rendered. For purposes of this section, the definition of outside employment includes those employees who are self-employed and not affiliated directly with this department for services, product(s) or benefits rendered.

Outside Security Employment - The employment involving any member of this department who performs duties or services on behalf of an outside organization, company or individual within this jurisdiction on behalf of the Department. Such outside employment shall be requested and scheduled directly through this department.

1011.2 OBTAINING APPROVAL

No member of this department may engage in any outside employment without first obtaining prior approval of the Chief of Police. Failure to obtain prior approval for outside employment or engaging in outside employment prohibited by this policy is grounds for disciplinary action.

Any employee seeking approval of outside employment whose request has been denied shall be provided with a written reason for the denial of the application at the time of the denial and within 30 days of the application.

1011.2.1 APPEAL OF DENIAL OF OUTSIDE EMPLOYMENT

If an employee's Outside Employment Application is denied or rescinded by the Department, the employee may file a written notice of appeal to the Chief of Police within 10 days of the date of denial.

If the employee's appeal is denied, the employee may file a grievance pursuant to the procedure set forth in the current collective bargaining agreement.

1011.2.2 REVOCATION/SUSPENSION OF OUTSIDE EMPLOYMENT PERMITS

Any outside employment permission may be revoked or suspended after the employee has received written notification of the reasons for revocation or suspension. Revocation will be implemented after the employee has exhausted the appeal process.

The outside employment may be revoked:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Outside Employment

- (a) If an employee's performance declines to a point where it is evaluated by a supervisor as needing improvement to reach an overall level of minimum acceptable competency and the outside employment may be related to the employee's performance. The Chief of Police may, at his/her discretion, notify the employee of the intent to revoke any previously approved outside employment permissions. After the appeal process has concluded, the revocation will remain in force until the employee's performance directly related to the outside employment has been reestablished to the minimum level of acceptable competency.
- (b) If, at any time during the term of a valid outside employment permit, an employee's conduct or outside employment conflicts with the provisions of Department policy, or any law.
- (c) The outside employment creates an actual or apparent conflict of interest with the Department or City.

1011.3 PROHIBITED OUTSIDE EMPLOYMENT

The Department expressly reserves the right to deny any Outside Employment Application submitted by an employee seeking to engage in any activity that:

- (a) Involves the employee's use of Department time, facilities, equipment or supplies, the use of the Department badge, uniform, prestige or influence for private gain or advantage.
- (b) Involves the employee's receipt or acceptance of any money or other consideration from anyone other than this department for the performance of an act that the employee, if not performing such act, would be required or expected to render in the regular course or hours of employment or as a part of the employee's duties as a member of this department.
- (c) Involves the performance of an act in other than the employee's capacity as a member of this department that may later be subject directly or indirectly to the control, inspection, review, audit or enforcement of any other employee of this department.
- (d) Involves time demands that would render performance of the employee's duties for this department below minimum standards or would render the employee unavailable for reasonably anticipated overtime assignments and other job-related demands that occur outside regular working hours.

1011.3.1 OUTSIDE SECURITY EMPLOYMENT

Any private organization, entity or individual seeking special services for security or traffic control from members of this department must submit a request to the Chief of Police, or designee, in advance of the desired service. Such outside employment will be monitored by the patrol supervisor.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Outside Employment

- (a) The applicant will further be required to provide for the compensation of all employees requested for such outside security services.
- (b) If such a request is approved, any employee working outside employment shall be subject to the following conditions:
 - 1. The officer(s) shall wear the Department uniform/identification.
 - 2. The officer(s) shall be subject to all the rules and regulations of this department.
 - 3. No officer may engage in such outside employment during or at the site of a strike, lockout, picket or other physical demonstration of a labor dispute.
 - 4. Compensation for such approved outside security services shall be at the contracted overtime rate as specified in the employees bargaining unit agreement.
 - 5. Outside security services, outside employment or outside overtime shall not be subject to the collective bargaining process.
 - 6. No officer may engage in outside employment as a peace officer for any other public agency without prior written authorization of the Chief of Police.

1011.3.2 OUTSIDE OVERTIME ARREST AND REPORTING PROCEDURE

Any employee making an arrest or taking other official law enforcement action while working in an approved outside overtime assignment shall be required to complete all related reports in a timely manner pursuant to Department policy. Time spent on the completion of such reports shall be considered incidental to the outside overtime assignment.

1011.3.3 SPECIAL RESTRICTIONS

Except for emergency situations or with prior authorization from the Division Commander, undercover officers or officers assigned to covert operations shall not be eligible to work overtime or other assignments in a uniformed or other capacity that might reasonably disclose the officer's law enforcement status.

1011.4 DEPARTMENT RESOURCES

Employees are prohibited from using any Department equipment or resources in the course of or for the benefit of any outside employment. This shall include the prohibition of access to official records or databases of this department or other agencies through the use of the employee's position with this department.

1011.5 CHANGES IN OUTSIDE EMPLOYMENT STATUS

If an employee terminates his/her outside employment during the period of a valid permit, the employee shall promptly submit written notification of such termination to the Chief of Police through the appropriate chain of command. Any subsequent request for renewal or continued outside employment must thereafter be processed and approved through normal procedures set forth in this policy.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Outside Employment

Employees shall also promptly submit in writing to the Chief of Police any material changes in outside employment including any change in the number of hours, type of duties or demands of any approved outside employment. Employees who are uncertain whether a change in outside employment is material shall report the change.

1011.6 OUTSIDE EMPLOYMENT WHILE ON DISABILITY OR ADMINISTRATIVE LEAVE

Department members engaged in outside employment who are placed on disability or administrative leave or modified/light-duty shall inform their immediate supervisor in writing within five days whether they intend to continue to engage in outside employment while on such leave or light-duty status. The immediate supervisor shall review the duties of the outside employment along with any work-related doctor's orders and make a recommendation to the Chief of Police whether such outside employment should continue or be suspended or revoked.

In the event the Chief of Police determines that the outside employment should be discontinued or if the employee fails to promptly notify his/her supervisor of his/her intentions regarding the work permit, a notice of intent to revoke the employee's permit will be forwarded to the involved employee and a copy attached to the original work permit. The revocation process outlined in this policy shall be followed.

Criteria for revoking or suspending the outside employment permit while on disability status or administrative leave include, but are not limited to, the following:

- (a) The outside employment is medically detrimental to the total recovery of the disabled employee, as indicated by the City's professional medical advisors.
- (b) The outside employment performed requires the same or similar physical ability, as would be required of an on-duty employee.
- (c) The employee's failure to make timely notice of his/her intentions to their supervisor.
- (d) The outside employment is not compatible with the reason the employee is on administrative leave.

Occupational Disease, Personal Injury and Death Reporting

1012.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance regarding the timely reporting of occupational diseases, personal injuries and deaths.

1012.1.1 DEFINITIONS

Definitions related to this policy include (Minn. Stat. § 176.011):

Occupational disease – A mental impairment or physical disease arising out of and in the course of employment peculiar to the occupation in which the member is engaged and due to causes in excess of the hazards ordinary of employment. The term includes diagnosis of post-traumatic stress disorder (PTSD) by a psychiatrist or psychologist; however, mental impairment is not considered a disease if it results from a disciplinary action, work evaluation, job transfer, layoff, demotion, promotion, termination, retirement or similar action taken in good faith by the Department.

Personal injury – Any mental impairment or physical injury arising out of and in the course of employment, including personal injury caused by occupational disease, while engaged in, on or about the premises where the member's services require the member's presence as part of that service at the time of the injury and during the hours of that service. Personal injury does not include an injury caused by the act of a third person or fellow department member who intended to injure the member because of personal reasons, and not directed against the member as a member of the South Saint Paul Police Department, or because of the employment with the South Saint Paul Police Department. Mental impairment is not considered a personal injury if it results from a disciplinary action, work evaluation, job transfer, layoff, demotion, promotion, termination, retirement or similar action taken in good faith by the Department.

1012.2 POLICY

The South Saint Paul Police Department will address occupational diseases, personal injuries and deaths appropriately, and will comply with applicable state workers' compensation requirements (Minn. Stat. § 176.231).

1012.3 RESPONSIBILITIES

1012.3.1 MEMBER RESPONSIBILITIES

Any member sustaining any occupational disease or personal injury shall report such event as soon as practicable, but within 24 hours, to a supervisor, and shall seek medical care when appropriate.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Occupational Disease, Personal Injury and Death Reporting

1012.3.2 SUPERVISOR RESPONSIBILITIES

A supervisor learning of any occupational disease or personal injury should ensure the member receives medical care as appropriate.

Supervisors shall ensure that required documents regarding workers' compensation are completed and forwarded promptly. Any related Citywide disease- or injury-reporting protocol shall also be followed.

Supervisors shall determine whether the Major Incident Notification and Workplace Accident and Injury Reduction policies apply and take additional action as required.

1012.3.3 DIVISION COMMANDER RESPONSIBILITIES

The Division Commander who receives a report of an occupational disease, personal injury or death should review the report for accuracy and determine what additional action should be taken. The report shall then be forwarded to the Chief of Police, and the City's risk management entity to ensure any required Minnesota Occupational Safety and Health Administration (MNOSHA) reporting is made as required in the illness and injury prevention plan identified in the Workplace Accident and Injury Reduction Policy.

1012.3.4 CHIEF OF POLICE RESPONSIBILITIES

The Chief of Police shall review and forward copies of the report to the Department of Human Resources. Copies of the report and related documents retained by the Department shall be filed in the member's confidential medical file.

1012.4 OTHER DISEASE OR INJURY

Diseases, injuries or deaths caused or occurring on-duty that do not qualify for workers' compensation reporting shall be documented on the designated report of injury form, which shall be signed by a supervisor. A copy of the completed form shall be forwarded to the appropriate Division Commander through the chain of command and a copy sent to the Administration Division Commander.

Unless the injury is extremely minor, this report shall be signed by the affected member, indicating that he/she desired no medical attention at the time of the report. By signing, the member does not preclude his/her ability to later seek medical attention.

1012.5 SETTLEMENT OFFERS

When a member sustains an occupational disease or personal injury that is caused by another person and is subsequently contacted by that person, his/her agent, insurance company or attorney and offered a settlement, the member shall take no action other than to submit a written report of this contact to his/her supervisor as soon as possible.

1012.5.1 NO SETTLEMENT WITHOUT PRIOR APPROVAL

No less than 10 days prior to accepting and finalizing the settlement of any third-party claim arising out of or related to an occupational disease or personal injury, the member shall provide the Chief of Police with written notice of the proposed terms of such settlement. In no case shall the member

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Occupational Disease, Personal Injury and Death Reporting

accept a settlement without first providing written notice to the Chief of Police. The purpose of such notice is to permit the City to determine whether the offered settlement will affect any claim the City may have regarding payment for damage to equipment or reimbursement for wages against the person who caused the disease or injury, and to protect the City's right of subrogation, while ensuring that the member's right to receive compensation is not affected.

Personal Appearance Standards

1013.1 PURPOSE AND SCOPE

To project uniformity and neutrality toward the public and other members of the Department, employees shall maintain their personal hygiene and appearance to project a professional image appropriate for this department and for their assignment.

1013.2 GROOMING

Unless otherwise stated and because deviations from these standards could present officer health safety issues, the following appearance standards shall apply to all members, except those whose current assignment would deem them not appropriate, and where the Chief of Police has granted exception.

1013.2.1 HAIR

Hair shall be clean, neatly trimmed or arranged, and of a natural hair color. Hairstyles with shaved designs in the scalp are prohibited. Hair adornments shall be primarily for the purpose of securing the hair and must present a professional image.

Hairstyles for male department members must not extend below the top edge of a uniform or dress shirt collar while assuming a normal stance.

When working a field assignment, hairstyles for female department members must not extend below the bottom edge of a uniform or dress shirt collar while assuming a normal stance. Longer hair shall be worn up or in a tightly wrapped braid or ponytail that is secured to the head above the bottom edge of the shirt collar.

1013.2.2 FACIAL HAIR

A groomed and maintained mustache, goatee or beard is authorized. Beards must be worn with a mustache. Facial hair must not be longer than a quarter (1/4) (#2 guard) inch in length. No portion of the beard may be exceptionally longer than the rest. Facial hair that prevents any officer from passing a mask "fit test" is prohibited.

1013.2.3 JEWELRY

For the purpose of this policy, jewelry refers to rings, earrings, necklaces, bracelets, wristwatches, and tie tacks or tie bars. Jewelry shall present a professional image and may not create a safety concern for the department member or others. Jewelry that depicts racial, sexual, discriminatory, gang-related, or obscene language is not allowed.

- (a) Necklaces shall not be visible above the shirt collar.
- (b) Earrings shall be small and worn only in or on the earlobe.
- (c) One ring or ring set may be worn on each hand of the department member. No rings should be of the type that would cut or pose an unreasonable safety risk to the member or others during a physical altercation, if the member is assigned to a position where that may occur.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Personal Appearance Standards

- (d) One small bracelet, including a bracelet identifying a medical condition, may be worn on one arm.
- (e) Wristwatches shall be conservative and present a professional image.
- (f) Tie tacks or tie bars worn with civilian attire shall be conservative and present a professional image.

1013.2.4 PERSONAL HYGIENE

All members must maintain proper personal hygiene. Examples of improper personal hygiene include but are not limited to dirty fingernails, bad breath, body odor, and dirty or unkempt hair. Any member who has a condition due to a protected category (e.g., race, physical disability) that affects any aspect of personal hygiene covered by this policy may qualify for an accommodation and should report any need for an accommodation to the Chief of Police.

1013.3 TATTOOS

Visible tattoos must be approved by the Chief of Police. Any tattoos deemed offensive or inappropriate by the Police Chief shall be covered and hidden from public view while on duty.

1013.4 BODY PIERCING OR ALTERATION

Body piercing or alteration to any area of the body that is visible in any authorized uniform or attire, and is a deviation from normal anatomical features and that is not medically required is prohibited. Such body alteration includes, but is not limited to:

- (a) Tongue splitting or piercing.
- (b) The complete or transdermal implantation of any material other than hair replacement or breast augmentation.
- (c) Abnormal shaping of the ears, eyes, nose or teeth.
- (d) Branding or scarification.

1013.5 POLICY

South Saint Paul Police Department members shall maintain their personal hygiene and appearance to project a professional image that is appropriate for this department and for their assignments. Department personal appearance standards are primarily based on safety requirements, appearance conformity, and the social norms of the community served, while considering matters important to members of the Department.

1013.6 EXEMPTIONS

Members who seek an exemption to this policy protected by law (e.g., culturally protective hairstyles) should generally be accommodated (Minn. Stat. § 363A.03). A member with an exemption may be ineligible for an assignment if the individual accommodation presents a security or safety risk. The Chief of Police should be advised any time a request for such an accommodation is denied or when a member with an exemption is denied an assignment based on a safety or security risk.

Uniform Regulations

1014.1 PURPOSE AND SCOPE

The uniform policy of the South Saint Paul Police Department is established to ensure that uniformed officers, special assignment personnel and non- licensed employees will be readily identifiable to the public through the proper use and wearing of department uniforms. Employees should also refer to the following associated policies:

- Firearms
- Department Owned and Personal Property
- Body Armor
- Personal Appearance Standards

The uniform and equipment specifications manual is maintained and periodically updated by the Chief of Police or the authorized designee. The manual, and associated procedures, should be consulted regarding authorized equipment and uniform specifications.

The South Saint Paul Police Department will provide uniforms for all employees who are required to wear them in the manner, quantity and frequency agreed upon in the respective employee group's collective bargaining agreement. The uniforms for officers of this department shall be a consistent color pursuant to Minn. Stat. § 626.88 Subd. 2.

1014.1.1 UNIFORM AND EQUIPMENT SPECIFICATIONS

(a) DEFINITIONS:

1. Uniform: means approved clothing, leatherwear and accouterments.
2. Uniform of the Day: means the authorized apparel and gear appropriate for an employee's or volunteer's assignment, rank and the season.

(b) ORDER: All Department employees and volunteers shall wear the complete Uniform appropriate to their rank and assignment during all tours of duty. The attire and manner of dress for those employees in special assignments (e.g. administration, investigations, school resource, clerical and police support, court, training, etc) will be appropriate to that assignment and at the direction of the Chief of Police or his or her designee. The Chief of Police may designate Uniform changes or policy deviation as needed.

1. Aside from the trousers and footwear, no component of the Uniform may be worn without the rest of the Uniform or in a civilian setting without prior approval. Exception: An authorized Department Jacket may be worn by plain clothes personnel during cold-weather situations where there is a need to be easily identified as a Police Officer.
2. Only those persons authorized by the Department will wear or allow any part of the Uniform to be worn or displayed.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

3. Only authorized pins, medallions, insignia, or other accouterments may be worn with or on Uniforms and other attire, however:
 - (a) Medical and religious necklaces may be worn under the shirt
 - (b) Medical bracelets may be worn
 - (c) Tasteful jewelry may be worn subject to the approval of the Chief of Police or designee.
 4. Uniforms will be kept neat, clean and well pressed.
 5. Uniform clothing items will not be torn, frayed, patched, nor noticeably faded or discolored.
 6. All leather gear will be of matching, authorized color and style and will be polished and free of excessive wear.
 7. All metal or brass items will be clean and properly polished.
 8. Shoes or boots will be of authorized color and style and will be shined/polished appropriately on a regular basis.
 9. Socks that are exposed should be black in color.
- (c) UNIFORM COMPONENTS:
- (a) Uniform shirts (long and short sleeve) will be of approved types and color and made of a cotton, polyester or similar material.
 - (a) Large bulges in the pockets will not be permitted.
 - (b) All of the shirt's buttons will be buttoned with the exception of the top button which will be fastened only when the tie is worn.
 - (c) The department patch will be sewn onto both shoulders, centered one inch below the shoulder seam.
 - (d) Corporal or Sergeant Chevrons will be gold in color, worn on both sleeves and centered approximately six inches below the shoulder seam.
 - (e) The American flag patch will be sewn onto the shirt, centered ½ inch above the right breast pocket.
 - (f) The officer's last name will be embroidered in 3/8" upper case letters just below the American flag and will be worn centered on the upper portion of the right pocket flap. The color of the embroidery will match the yellow border of the American Flag. *Exception: For an approved leather duty jacket, a metal name bar may be worn in place of the embroidery. This required name bar will have black letters on a gold background and will be worn centered on the upper portion of the right pocket flap.
 - (g) A seniority pin will be worn centered on the upper portion of the right pocket flap. (This pin is optional for everyday use, but required for the dress Uniform).

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

- (h) The department badge will be kept polished and worn above the left breast pocket.
- (i) Pins, medals and awards will be approved by the Chief of Police and worn neatly on the left pocket flap.
- (j) A ballistic vest carrier fashioned to appear as a uniform shirt is allowed and may be worn over the uniform shirt.
- (k) Other items not mentioned above are subject to prior approval.
- (b) Uniform Trousers will be of approved types, navy blue in color and made of a cotton, polyester or similar material.
 - (a) The trousers will be of a proper fit and length and hemmed to a plain bottom.
- (c) Turtleneck, mock turtleneck or dickies will be of approved types, dark navy blue in color and may have the five letter abbreviation "SSPPD" embroidered in a color matching the border of the Department issued shoulder patch (Maderia 1011). These articles of clothing will only be allowed to be worn with the Class A (winter) Uniform. Clothing manufacturer logos should not be visible.
- (d) Ties will be navy blue in color and constructed of cotton, polyester or similar material. The top button of the shirt will be fastened when wearing a tie.
 - (a) The Department issued tie bar will be worn with the tie.
- (e) Leather Gear will be constructed of genuine leather, laminate or composite material. The color will be black and the style will be basket weave or in plain black matte if basket weave is unavailable.
 - (a) Visible fasteners and belt keepers shall be black or gold colored. Hidden fasteners are allowed. All fasteners must match and shall be fastened at all times during use.
 - (b) Firearm duty holsters will be worn on the strong side of the officer's duty belt. Cross draw holsters will not be permitted. Duty belt holsters must be of a level II retention level or higher.
- (f) Required Equipment to be worn by all non-administrative Uniformed officers' while engaged in patrol or field activities includes:
 - (a) Department issued ballistic vest with the front and back panels installed. (Vests purchased after January 1, 2011 must be National Institute of Justice compliant.)
 - (b) Department-issued handgun, fully loaded with Department-issued ammunition
 - (c) Two spare magazines fully loaded with Department-issued ammunition
 - (d) Department-issued Taser
 - (e) Department-issued Oleoresin Capsicum (10%) Pepper Spray
 - (f) Handcuffs

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

- (g) Latex or latex-substitute examination gloves
- (g) Outer Gear means rain coat, parka, jacket or sweater.
 - (a) All raincoats shall be American National Standards Institute (ANSI) approved high- visibility and black reversible.
 - (b) All jacket styles must be approved for purchase and should be navy blue in color. Jackets will have the same requirements for patches and embroidery as the uniform shirt. A badge patch may be used in place of the Department issued badge.
 - (c) External Vest Carriers may be worn as an outer garment and worn over a Uniform shirt or vest undershirt. The vest carrier will be of an approved style and navy blue in color. A badge, American flag, and embroidered name must be worn on the officer's outermost garment.
- (h) Headgear includes the approved garrison style hat with approved hat badge, the navy blue mouton with approved hat badge or the approved navy blue baseball cap. These garments will be worn as appropriate to the officer's assignment.
- (i) Footwear will be conservative in nature and appropriate to an employee's assignment.
 - (a) Footwear will be kept polished when worn with the Uniform.
 - (b) Some all black leather athletic style shoes approved by the Chief or Police or designee, may be worn.
 - (c) Uniformed personnel, CSOs and Reserve Officers will wear approved black shoes or boots of a conservative nature which have a smooth leather appearance.
- (j) Gloves are optional but must be black or navy blue in color. Black or navy blue mittens may be worn in extremely cold weather.
- (d) CLASSIFICATIONS:
 - (a) Class A or Long Sleeve Uniform for Sworn Officers will be worn during the cooler months of the year. The Class A Uniform includes:
 - (a) Long sleeve Uniform shirt
 - (b) Navy blue tie w/ tie tack or tie bar or turtleneck, mock turtleneck or dickie.
 - (c) Patrol officers will be allowed to wear the long-sleeve shirt open-collared w/ o a tie only when engaged in normal patrol duties. Officers must, however, wear a white, dark navy blue or black crew neck t-shirt the collar of which shall be visible beneath the open collared Uniform shirt.
 - (d) Trousers
 - (e) Leather gear/equipment
 - (f) Black socks if they are visible while being worn
 - (g) Black polished shoes or boots

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

- (h) Approved rain coat and jacket
 - (i) Garrison hat, baseball hat or watch cap (optional)
- (b) Formal Dress Uniform is the same as the Class A Uniform (g,1) with the addition of:
 - (a) The dress Uniform will be worn on formal occasions (e.g. parades, funerals, award ceremonies, photographs, graduations, etc).
 - (b) Mandatory Uniform tie with tie bar or tie tack. (Mock turtlenecks and turtlenecks are not allowed).
 - (c) Seniority pin centered directly above the right pocket flap and below the flag patch.
 - (d) Approved medals, awards and pins worn centered on the left pocket flap.
 - (e) Uniform Garrison hat.
- (c) Class B Uniform or warm weather uniform for Sworn Officers will be worn during the warmer months. The Class B Uniform includes:
 - (a) Short sleeve Uniform shirt
 - (b) Dark navy blue or black crew neck t-shirt worn beneath the Uniform shirt
 - (c) Trousers
 - (d) Leather gear and equipment
 - (e) Black socks if they are visible while being worn.
 - (f) Black polished shoes or boots
 - (g) Rain coat or jacket (optional)
 - (h) Garrison hat or baseball style cap (optional)
- (d) Class C Uniform for Special Events and Bicycle Patrol Officers will consist of:
 - (a) Approved navy blue shorts for Bicycle Patrol and Uniform Cargo Style Trousers for Special Events
 - (b) Department Special Event "high-visibility" polo shirt
 - (c) White crew neck t-shirt worn beneath the Special Event polo shirt
 - (d) Black socks if they are visible while being worn.
 - (e) Black polished shoes or boots
 - (f) Complete duty belt
 - (g) Department approved bicycle helmet (Bicycle Patrol Only)
 - (h) Black gloves (Optional)
 - (i) Black athletic shoes (Bicycle Patrol Only)
- (e) Class D Uniform for Command Personnel will be one of two Uniforms:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

- (a) Class A or Class B Uniform described above with either a navy blue or white Uniform shirt, and two matching stars worn on the collar (Chief) or oakleaf insignias worn on the collar (Commander).). A fully loaded, Department-issued handgun is required. A full duty belt is optional for command personnel.
 - (b) Appropriate plain clothes (jacket/tie or dress casual) with visible badge or police identification card.
- (f) Class E Uniform for Community Service Officers (CSOs) will be worn by all CSOs during their tours of duty.
 - (a) Uniform shirts will be navy blue in color with epaulets on both of the shoulders. The details for this uniform will be the same as they are for the sworn officers with the exception being rocker patches worn above the Department patch will identify CSOs as such.
 - (b) Trousers for the CSOs will be navy blue in color.
 - (c) Leather gear for the CSOs will be the same as for officers with the exception of a firearms, holster and magazines.
- (g) Class F Uniform for Reserve Officers will be worn by all Reserve Officers during their tours of duty.
 - (a) Uniform shirts will be light blue in color with epaulets on both of the shoulders. The details for this uniform will be the same as they are for the sworn officers with the exception being rocker patches worn above the Department patch will identify Reserve Officers as such.
 - (b) Trousers for the Reserve Officers will be Navy blue in color.
 - (c) Leather gear for the Reserve Officers will be the same as officers with the exception of firearms, magazines and holster. If a Reserve Officer is also a CSO with the SSPPD than they are authorized to carry their department issued Taser as a Reserve Officers.
- (h) Office Staff:
 - (a) The preferred attire for office staff shall be one which will present a professional image with "business casual" being the generally excepted standard.
 - (b) Office staff may substitute "business casual" attire with a Department issued polo worn with approved slacks.
- (i) Court Appearances:
 - (a) The police Uniform(s) of the day are authorized dress for any court appearance except a tie is required when wearing a long sleeved uniform shirt.
 - (b) Male officers may substitute a suit for the Uniform when appearing in court. Minimum requirements for non-Uniform court attire include:
 - 1. Dress slacks

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

2. Dress shirt
 3. Tie
 4. Suit jacket or sports jacket
 5. Dress shoes
- (c) Female officers may substitute conservative business suits or ensembles for the uniform when appearing in court.
- (j) Non-Uniform Attire for sworn and non-sworn members of the Department engaged in temporary or special assignments. These assignments may include but are not limited to; a member of the Department attending training, an undercover officer, an investigator, a public relations officer, an FTO in phase IV training, a MAAG officer, a School Resource Officer, etc. In these cases, the Uniform of the Day will be one which will present a professional image and is appropriate to the assignment as dictated by the officer's immediate supervisor with "business casual" being the generally accepted minimum standard for most assignments.
- (e) UNIFORM ALLOWANCE: All articles and equipment listed below will be included as items for which the uniform allowance provided to sworn officers who are members of LELS may be spent: Note: Items noted with an "*" will be of a type approved by the Chief of Police. Annual purchasing limits as set by the Chief do not apply to the replacement of broken or damaged equipment.
1. Duty Belt:
 - (a) Outer leather/vinyl belt
 - (b) Inner leather/vinyl belt
 - (c) Belt Keepers
 - (d) Holster (For Department issued firearms only.)
 - (e) Magazine Holder
 - (f) Handcuff Case, Handcuffs, Handcuff Keys
 - (g) Radio Holder
 - (h) Chemical Agent Holder
 - (i) Baton Holder, ASP/Expandable Baton
 - (j) Flashlight Holder, Flashlight (Yearly limit of 1)
 - (k) Key Holder
 - (l) Latex Glove Case
 - (m) Knife Holder, Knife (Maximum purchase price of \$100, yearly limit of 1)
 - (n) Gun Repair/Cleaning Kit (Maximum purchase price of \$50, career limit of 1)
 - (o) Pistol Grip

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

- (p) Weapon light
- (q) Radio earpiece
- (r) Taser Holster
- 2. Uniform:
 - (a) Uniform Cleaning and Repair
 - (b) Uniform Pants
 - (c) Long and Short Sleeve Uniform Shirts
 - (d) Turtle Neck Shirt, approved t-shirts and dickies
 - (e) Ties
 - (f) Name Bar
 - (g) Badge, Badge Carrier
 - (h) Patches
 - (i) Jacket, Rain Jacket, Raid Jacket
 - (j) Footwear (approved types), Shoe Polish, Socks
 - (k) Garrison Hat and Hat Cover, *Baseball Hat (Department logo)
 - (l) Gloves
 - (m) Ballistic Vest and vest carrier
 - (n) Vest carrier clips to include mollyclips/molly attachments
 - (o) Thermal Underwear, T-shirts
 - (p) Bike Shorts (approved type), Bike Shorts Liner
 - (q) Polo type shirt (Department logo)
 - (r) Stocking cap/balaclava/ear muffs
 - (s) Heavy duty hanger for uniform/vest
 - (t) Class A police badge
 - (u) Eye Protection/sunglasses (under \$100)
 - (v) Ear protection
- 3. Squad Items:
 - (a) Duty Bag
 - (b) Hobble-type Restraint
 - (c) Personnel medical bag supplies

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

1014.2 WEARING AND CONDITION OF UNIFORM AND EQUIPMENT

Police employees wear the uniform to be identified as the law enforcement authority in society. The uniform also serves an equally important purpose, which is to identify the wearer as a source of assistance in an emergency, crisis or other time of need.

- (a) Uniform and equipment shall be maintained in a serviceable condition and shall be ready at all times for immediate use. Uniforms shall be neat, clean and appear professionally pressed.
- (b) All peace officers of this department shall possess and maintain at all times, a serviceable uniform and the necessary equipment to perform uniformed field duty.
- (c) Personnel shall wear only the uniform specified for their rank and assignment.
- (d) The uniform is to be worn in compliance with the specifications set forth in the Department's uniform specifications and procedures which are maintained separately from this policy.
- (e) All supervisors will perform periodic inspections of their personnel to ensure conformance to these regulations.
- (f) Civilian attire shall not be worn in combination with any distinguishable part of the uniform.
- (g) Uniforms are only to be worn while on-duty, while in transit to or from work, for court or at other official Department functions or events.
- (h) Employees are not to purchase or drink alcoholic beverages while wearing any part of the Department uniform, including the uniform pants.
- (i) Visible jewelry, other than those items listed below, shall not be worn with the uniform unless specifically authorized by the Chief of Police or designee.
 - 1. Wrist watch.
 - 2. Wedding ring(s), class ring or other ring of tasteful design. A maximum of one ring/set may be worn on each hand.
 - 3. Medical alert bracelet.

1014.2.1 DEPARTMENT ISSUED IDENTIFICATION

The Department issues each employee an official Department identification card bearing the employee's name, identifying information and photo likeness. All employees shall be in possession of their Department-issued identification card at all times while on-duty or when carrying a concealed weapon.

- (a) Whenever on-duty or acting in an official capacity representing the Department, employees shall display their Department issued identification in a courteous manner to any person upon request and as soon as practicable.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Uniform Regulations

- (b) Officers working specialized assignments may be excused from the possession and display requirements when directed by their Division Commander.

1014.3 POLITICAL ACTIVITIES, ENDORSEMENTS, ADVERTISEMENTS OR OTHER APPEARANCES IN UNIFORM

Unless specifically authorized by the Chief of Police, South Saint Paul Police Department employees may not wear any part of the uniform, be photographed wearing any part of the uniform, utilize a badge, patch or other official insignia of the Department, or cause to be posted, published or displayed, the image of another employee, or identify him/herself as an employee of the South Saint Paul Police Department to do any of the following:

- (a) Endorse, support, oppose or contradict any political campaign or initiative.
- (b) Endorse, support, oppose or contradict any social issue, cause or religion.
- (c) Endorse, support or oppose, any product, service, company or other commercial entity.
- (d) Appear in any commercial, social or nonprofit publication, or any motion picture, film, video, public broadcast, photo, any website or any other visual depiction.

1014.4 UNAUTHORIZED UNIFORMS, EQUIPMENT AND ACCESSORIES

South Saint Paul Police Department employees may not wear any uniform item, accessory or attachment unless specifically authorized in the Uniform and Equipment Specifications or by the Chief of Police or designee.

South Saint Paul Police Department employees may not use or carry any tool or other piece of equipment unless specifically authorized in the Uniform and Equipment Specifications or by the Chief of Police or designee.

Department Badges

1015.1 PURPOSE AND SCOPE

The South Saint Paul Police Department badge and uniform patch as well as the likeness of these items and the name of the South Saint Paul Police Department are property of the Department and their use shall be restricted as set forth in this policy.

1015.2 POLICY

The uniform badge shall be issued to Department members as a symbol of authority. The use and display of Department badges shall be in strict compliance with this policy. Only authorized badges issued by this department shall be displayed, carried or worn by members while on-duty or otherwise acting in an official or authorized capacity.

1015.2.1 FLAT BADGE

Licensed officers, with the written approval of the Chief of Police, may purchase at their own expense a flat badge capable of being carried in a wallet. The use of the flat badge is subject to all the same provisions of Department policy as the uniform badge.

- (a) An officer may sell, exchange or transfer the flat badge he/she purchased to another officer within the South Saint Paul Police Department with the written approval of the Chief of Police.
- (b) Should the flat badge become lost, damaged or otherwise removed from the officer's control he/she shall make the proper notifications as outlined in the Department-Owned and Personal Property Policy.
- (c) An honorably retired officer may keep his/her flat badge upon retirement.
- (d) The purchase, carrying or display of a flat badge is not authorized for non-licensed personnel.

1015.2.2 CIVILIAN PERSONNEL

Badges and Department identification cards issued to non- licensed personnel shall be clearly marked to reflect the position of the assigned employee (e.g. parking control, dispatcher).

- (a) Non-licensed personnel shall not display any Department badge except as a part of his/her uniform and while on-duty or otherwise acting in an official and authorized capacity.
- (b) Non-licensed personnel shall not display any Department badge or represent him/herself, on- or off-duty, in such a manner which would cause a reasonable person to believe that he/she is a licensed officer.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Department Badges

1015.2.3 RETIREE UNIFORM BADGE

Upon honorable retirement employees may purchase their assigned duty badge for display purposes. It is intended that the duty badge be used only as private memorabilia, as other uses of the badge may be unlawful or in violation of this policy.

1015.3 UNAUTHORIZED USE

Except as required for on-duty use by current employees, no badge designed for carry or display in a wallet, badge case or similar holder shall be issued to anyone other than a current or honorably retired peace officer.

Department badges are issued to all licensed employees and civilian uniformed employees for official use only. The Department badge, shoulder patch or the likeness thereof, or the Department name shall not be used for personal or private reasons including, but not limited to, letters, memoranda and electronic communications, such as electronic mail or websites and web pages.

The use of the badge, uniform patch and Department name for all material (e.g., printed matter, products or other items) developed for Department use shall be subject to approval by the Chief of Police.

Employees shall not loan the badge or identification card to others and shall not permit the badge or identification card to be reproduced or duplicated.

Temporary Modified-Duty Assignments

1016.1 PURPOSE AND SCOPE

This policy establishes procedures for providing temporary modified-duty assignments. This policy is not intended to affect the rights or benefits of employees under federal or state law, City rules, or current memorandums of understanding or collective bargaining agreements. For example, nothing in this policy affects the obligation of the Department to engage in a good faith, interactive process to consider reasonable accommodations for any employee with a temporary or permanent disability that is protected under federal or state law.

1016.2 POLICY

Subject to operational considerations, the South Saint Paul Police Department may identify temporary modified-duty assignments for employees who have an injury or medical condition resulting in temporary work limitations or restrictions. A temporary assignment allows the employee to work, while providing the Department with a productive employee during the temporary period.

1016.3 GENERAL CONSIDERATIONS

Priority consideration for temporary modified-duty assignments will be given to employees with work-related injuries or illnesses that are temporary in nature. Employees having disabilities covered under the Americans with Disabilities Act (ADA) or the Minnesota Human Rights Act (Minn. Stat. § 363A.01 et seq.) shall be treated equally, without regard to any preference for a work-related injury.

No position in the South Saint Paul Police Department shall be created or maintained as a temporary modified-duty assignment.

Temporary modified-duty assignments are a management prerogative and not an employee right. The availability of temporary modified-duty assignments will be determined on a case-by-case basis, consistent with the operational needs of the Department. Temporary modified-duty assignments are subject to continuous reassessment, with consideration given to operational needs and the employee's ability to perform in a modified-duty assignment.

The Chief of Police or the authorized designee may restrict employees working in temporary modified-duty assignments from wearing a uniform, displaying a badge, carrying a firearm, operating an emergency vehicle, engaging in outside employment, or being otherwise limited in employing their peace officer powers.

Temporary modified-duty assignments shall generally not exceed a cumulative total of 1,040 hours in any one-year period.

1016.4 PROCEDURE

Employees may request a temporary modified-duty assignment for short-term injuries or illnesses.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Modified-Duty Assignments

Employees seeking a temporary modified-duty assignment should submit a written request to their Division Commanders or the authorized designees. The request should, as applicable, include a certification from the treating medical professional containing:

- (a) An assessment of the nature and probable duration of the illness or injury.
- (b) The prognosis for recovery.
- (c) The nature and scope of limitations and/or work restrictions.
- (d) A statement regarding any required workplace accommodations, mobility aids or medical devices.
- (e) A statement that the employee can safely perform the duties of the temporary modified-duty assignment.

The Division Commander will make a recommendation through the chain of command to the Chief of Police regarding temporary modified-duty assignments that may be available based on the needs of the Department and the limitations of the employee. The Chief of Police or the authorized designee shall confer with the Department of Human Resources or the City Attorney as appropriate.

1016.5 ACCOUNTABILITY

Written notification of assignments, work schedules and any restrictions should be provided to employees assigned to temporary modified-duty assignments and their supervisors. Those assignments and schedules may be adjusted to accommodate department operations and the employee's medical appointments, as mutually agreed upon with the Division Commander.

1016.5.1 EMPLOYEE RESPONSIBILITIES

The responsibilities of employees assigned to temporary modified duty shall include, but not be limited to:

- (a) Communicating and coordinating any required medical and physical therapy appointments in advance with their supervisors.
- (b) Promptly notifying their supervisors of any change in restrictions or limitations after each appointment with their treating medical professionals.
- (c) Communicating a status update to their supervisors no less than once every 30 days while assigned to temporary modified duty.
- (d) Submitting a written status report to the Division Commander that contains a status update and anticipated date of return to full-duty when a temporary modified-duty assignment extends beyond 60 days.

1016.5.2 SUPERVISOR RESPONSIBILITIES

The employee's immediate supervisor shall monitor and manage the work schedule of those assigned to temporary modified duty.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Temporary Modified-Duty Assignments

The responsibilities of supervisors shall include, but not be limited to:

- (a) Periodically apprising the Division Commander of the status and performance of employees assigned to temporary modified duty.
- (b) Notifying the Division Commander and ensuring that the required documentation facilitating a return to full duty is received from the employee.
- (c) Ensuring that employees returning to full duty have completed any required training and certification.

1016.6 MEDICAL EXAMINATIONS

Prior to returning to full-duty status, employees shall be required to provide certification from their treating medical professionals stating that they are medically cleared to perform the essential functions of their jobs without restrictions or limitations.

The Department may require a fitness-for-duty examination prior to returning an employee to full-duty status, in accordance with the Fitness for Duty Policy.

1016.7 PREGNANCY

If an employee is temporarily unable to perform regular duties due to a pregnancy, childbirth or a related medical condition, the employee will be treated the same as any other temporarily disabled employee (42 USC § 2000e(k)). A pregnant employee shall not be involuntarily transferred to a temporary modified-duty assignment.

1016.7.1 NOTIFICATION

Pregnant employees should notify their immediate supervisors as soon as practicable and provide a statement from their medical providers identifying any pregnancy-related job restrictions or limitations. If at any point during the pregnancy it becomes necessary for the employee to take a leave of absence, such leave shall be granted in accordance with the City's personnel rules and regulations regarding family and medical care leave.

1016.8 PROBATIONARY EMPLOYEES

Probationary employees who are assigned to a temporary modified-duty assignment shall have their probation extended by a period of time equal to their assignment to temporary modified duty.

1016.9 MAINTENANCE OF CERTIFICATION AND TRAINING

Employees assigned to temporary modified duty shall maintain all certification, training and qualifications appropriate to both their regular and temporary duties, provided that the certification, training or qualifications are not in conflict with any medical limitations or restrictions. Employees who are assigned to temporary modified duty shall inform their supervisors of any inability to maintain any certification, training or qualifications.

Employee Speech, Expression and Social Networking

1017.1 PURPOSE AND SCOPE

This policy is intended to address issues associated with employee use of social networking sites and to provide guidelines for the regulation and balance of employee speech and expression with the needs of the Department.

Nothing in this policy is intended to prohibit or infringe upon any communication, speech or expression that is protected or privileged under law. This includes speech and expression protected under state or federal constitutions as well as labor or other applicable laws. For example this policy does not limit an employee from speaking as a private citizen, including acting as an authorized member of a recognized bargaining unit or officer associations, about matters of public concern such as misconduct or corruption.

Employees are encouraged to consult with their supervisor regarding any questions arising from the application or potential application of this policy.

1017.1.1 APPLICABILITY

This policy applies to all forms of communication including but not limited to film, video, print media, public or private speech, use of all Internet services, including the World Wide Web, e-mail, file transfer, remote computer access, news services, social networking, social media, instant messaging, blogs, forums, wikis, video and other file sharing sites.

1017.2 POLICY

Because public employees occupy a trusted position in the community their statements have the potential to contravene the policies and performance of this department. Due to the nature of the work and influence associated with the law enforcement profession it is necessary that employees of this department be subject to certain reasonable limitations on their speech and expression. To achieve its mission and efficiently provide service to the public the South Saint Paul Police Department will carefully balance the individual employee's rights against the organization's needs and interests when exercising a reasonable degree of control over its employees' speech and expression.

1017.3 SAFETY

Employees should carefully consider the implications of their speech or any other form of expression when using the Internet. Speech and expression that may negatively affect the safety of South Saint Paul Police Department employees such as posting personal information in a public forum can result in compromising an employee's home address or family ties. Employees should therefore not disseminate or post any information on any forum or medium that could reasonably be expected to compromise the safety of any employee, employee's family or associates or persons that this agency has had professional contact with such as crime victims or staff of

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Employee Speech, Expression and Social Networking

other organizations. Examples of the type of information that could reasonably be expected to compromise safety include:

- Disclosing a photograph and name or address of an employee.
- Disclosing the address, telephone number or email address of an employee.
- Otherwise disclosing where another employee can be located off-duty.

1017.4 PROHIBITED SPEECH, EXPRESSION AND CONDUCT

To meet the organization's safety, performance and public-trust needs the following are prohibited unless the speech is otherwise protected (for example an employee speaking as a private citizen, including acting as an authorized member of a recognized bargaining unit or officer associations, on a matter of public concern):

- (a) Speech or expression made pursuant to an official duty that tends to compromise or damage the mission, function, reputation or professionalism of the South Saint Paul Police Department or its employees.
- (b) Speech or expression that, while not made pursuant to an official duty, is significantly linked to or related to the South Saint Paul Police Department and tends to compromise or damage the mission, function, reputation or professionalism of the South Saint Paul Police Department or its employees. Examples may include:
 1. Statements that indicate disregard for the law or the state or U.S. Constitution.
 2. Expression that demonstrates support for criminal activity.
 3. Participating in sexually explicit photographs or videos for compensation or distribution.
- (c) Speech or expression that could reasonably be foreseen as having a negative impact on the credibility of the employee as a witness. For example posting statements or expressions to a website that glorify or endorse dishonesty or illegal behavior.
- (d) Speech or expression of any form that could reasonably be foreseen as having a negative impact on the safety of the employees of the Department. For example a statement on a blog that provides specific details as to how and when prisoner transportations are made could reasonably be foreseen to jeopardize employees by informing criminals of details that could facilitate an escape or attempted escape.
- (e) Speech or expression that is contrary to the canons of the Law Enforcement Code of Ethics as adopted by the South Saint Paul Police Department.
- (f) Use or disclosure, through whatever means, of any not public data, photograph, video or other recording obtained or accessible as a result of employment with the Department for financial or personal gain or data classified as not public by state or federal law or any disclosure of such materials without the express authorization of the Chief of Police or the authorized designee.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Employee Speech, Expression and Social Networking

- (g) Posting, transmitting or disseminating any photographs, video or audio recordings, likenesses or images of department logos, emblems, uniforms, badges, patches, marked vehicles, equipment or other material that specifically identifies the South Saint Paul Police Department on any personal or social networking or other website or web page without the express authorization of the Chief of Police.
- (h) Accessing websites for non-authorized purposes or use of any personal communication device, game device or media device, whether personally or department-owned, for personal purposes while on-duty except in the following circumstances:
 - 1. When brief personal communications may be warranted by the circumstances (e.g., inform family of extended hours).
 - 2. During authorized breaks; such usage should be limited as much as practicable to areas out of sight and sound of the public and shall not be disruptive to the work environment.

Employees must take reasonable and prompt action to remove any content, including content posted by others, that is in violation of this policy from any web page or website maintained by the employee (e.g., social or personal website).

1017.4.1 UNAUTHORIZED ENDORSEMENTS AND ADVERTISEMENTS

While employees are not restricted from engaging in the following activities as private citizens or as authorized members of a recognized bargaining unit or officer associations, employees may not represent the South Saint Paul Police Department or identify themselves in any way that could be reasonably perceived as representing the South Saint Paul Police Department in order to do any of the following, unless specifically authorized by the Chief of Police:

- (a) Endorse, support, oppose or contradict any political campaign or initiative.
- (b) Endorse, support, oppose or contradict any social issue, cause or religion.
- (c) Endorse, support, or oppose any product, service, company or other commercial entity.
- (d) Appear in any commercial, social or nonprofit publication or any motion picture, film, video, public broadcast or any website.

Additionally, when it can reasonably be construed that an employee acting in his/her individual capacity or through an outside group or organization (e.g. bargaining group) is affiliated with this department, the employee shall give a specific disclaiming statement that any such speech or expression is not representative of the South Saint Paul Police Department.

Employees retain their right to vote as they choose, to support candidates of their choice and to express their opinions as private citizens, including as authorized members of a recognized bargaining unit or officer associations, on political subjects and candidates at all times while off-

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Employee Speech, Expression and Social Networking

duty. However employees may not use their official authority or influence to interfere with or affect the result of an election or a nomination for office. Employees are also prohibited from directly or indirectly using their official authority to coerce, command or advise another employee to pay, lend or contribute anything of value to a party, committee, organization, agency or person for political purposes (5 USC § 1502).

1017.5 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to e-mails, texts, or anything published or maintained through file-sharing software or any Internet site (e.g., Facebook, MySpace) that is accessed, transmitted, received or reviewed on any department technology system (see the Information Technology Use Policy for additional guidance).

1017.6 CONSIDERATIONS

In determining whether to grant authorization of any speech or conduct that is prohibited under this policy, the factors that the Chief of Police or authorized designee should consider include:

- (a) Whether the speech or conduct would negatively affect the efficiency of delivering public services.
- (b) Whether the speech or conduct would be contrary to the good order of the Department or the efficiency or morale of its members.
- (c) Whether the speech or conduct would reflect unfavorably upon the Department.
- (d) Whether the speech or conduct would negatively affect the member's appearance of impartiality in the performance of his/her duties.
- (e) Whether similar speech or conduct has been previously authorized.
- (f) Whether the speech or conduct may be protected and outweighs any interest of the Department.

POST Licensing

1018.1 PURPOSE AND SCOPE

Maintaining a valid POST license is a critical element of an officer's ability to continue their employment and is their sole professional responsibility. Every officer and every part-time officer is required to complete the continuing education requirements to maintain a valid license every three years (Minn. R. § 6700.0900; Minn. R. 6700.1000).

1018.2 RENEWAL SCHEDULE

Any officer whose license expires is not authorized to work as a peace officer until the license status is valid. Officers renew their POST licenses according to a schedule established by Administrative Rule (Minn. R. 6700.1000).

1018.2.1 LICENSE RENEWAL CREDITS

A peace officer license may be renewed only upon the licensee or the licensee's appointing authority providing the POST board proof the licensee has successfully completed board-approved continuing education and posting of fees on or before June 30 of the year a license is due for renewal. Licensee required hours of continuing credit are (Minn. R. 6700.1000, Subd. 3):

- 16 hours for a peace officer or a part-time peace officer who has been licensed for at least six months but less than 18 months.
- 32 hours for a peace officer or a part-time peace officer who has been licensed for at least 18 months but less than 30 months.
- 48 hours for a peace officer or a part-time peace officer who has been licensed for at least 30 months.

1018.3 LICENSE PROCESS

A general schedule for the license renewal process is:

- February - The Department or officer will receive employment verification.
- March - The Department or officers are sent a license renewal application.
- June - A final notice will be sent from POST for those who have not renewed.
- June 30 - The deadline date for license renewal after which officers whose license expires will no longer be authorized to practice law enforcement or carry a firearm.

1018.4 INACTIVE LICENSE

Officers who fail to complete the requirements will have their license placed in the "Inactive" status. The employee may then be placed in a temporary administrative assignment until their license is "Valid". Those employees may also face administrative discipline up to and including termination.

Line-of-Duty Deaths

1019.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members of the South Saint Paul Police Department in the event of the death of a member occurring in the line of duty and to direct the Department in providing proper support for the member's survivors.

The Chief of Police may also apply some or all of this policy for a non-line-of-duty member death, or in situations where members are injured in the line of duty and the injuries are life-threatening.

1019.1.1 DEFINITIONS

Definitions related to this policy include:

Line-of-duty death - The death of an officer during the course of performing law enforcement-related functions while on- or off-duty, or a civilian member during the course of performing assigned duties.

For an officer, a line-of-duty death includes death that is the direct and proximate result of a personal injury sustained in the line of duty (34 USC § 10281).

Survivors - Immediate family members of the deceased member, which can include spouse, children, parents, other next of kin, or significant others. The determination of who should be considered a survivor for purposes of this policy should be made on a case-by-case basis given the individual's relationship with the member and whether the individual was previously designated by the deceased member.

1019.2 POLICY

It is the policy of the South Saint Paul Police Department to make appropriate notifications and to provide assistance and support to survivors and coworkers of a member who dies in the line of duty.

It is also the policy of this department to respect the requests of the survivors when they conflict with these guidelines, as appropriate.

1019.3 INITIAL ACTIONS BY COMMAND STAFF

- (a) Upon learning of a line-of-duty death, the deceased member's supervisor should provide all reasonably available information to the Sergeant and Dispatch.
 - 1. Communication of information concerning the member and the incident should be restricted to secure networks to avoid interception by the media or others (see the Police Chief section of this policy).
- (b) The Sergeant should ensure that notifications are made in accordance with the Officer-Involved Shootings and Deaths and Major Incident Notification policies as applicable.
- (c) If the member has been transported to the hospital, the Sergeant or the authorized designee should respond to the hospital to assume temporary responsibilities as the Hospital Liaison.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

- (d) The Chief of Police or the authorized designee should assign members to handle survivor notifications and assign members to the roles of Hospital Liaison (to relieve the temporary Hospital Liaison) and the Department Liaison as soon as practicable (see the Notifying Survivors section and the Department Liaison and Hospital Liaison subsections in this policy).
- (e) The Law Enforcement Memorial Association (LEMA) may be notified and potentially requested to assist with funeral arrangements and coordination.

1019.4 NOTIFYING SURVIVORS

Survivors should be notified as soon as possible in order to avoid the survivors hearing about the incident in other ways.

The Chief of Police or the authorized designee should review the deceased member's emergency contact information and make accommodations to respect the member's wishes and instructions specific to notifying survivors. However, notification should not be excessively delayed because of attempts to assemble a notification team in accordance with the member's wishes.

The Chief of Police, Sergeant, or the authorized designee should select at least two members to conduct notification of survivors, one of which may be the Department chaplain.

Notifying members should:

- (a) Make notifications in a direct and compassionate manner, communicating as many facts of the incident as possible, including the current location of the member. Information that is not verified should not be provided until an investigation has been completed.
- (b) Determine the method of notifying surviving children by consulting with other survivors and taking into account factors such as the child's age, maturity, and current location (e.g., small children at home, children in school).
- (c) Plan for concerns such as known health concerns of survivors or language barriers.
- (d) Offer to transport survivors to the hospital, if appropriate. Survivors should be transported in department vehicles. Notifying members shall inform the Hospital Liaison over a secure network that the survivors are on their way to the hospital. Notifying members should remain at the hospital while the survivors are present.
- (e) When survivors are not at their residences or known places of employment, actively seek information and follow leads from neighbors, other law enforcement, postal authorities, and other sources of information in order to accomplish notification in as timely a fashion as possible. Notifying members shall not disclose the reason for their contact other than a family emergency.
- (f) If making notification at a survivor's workplace, ask a workplace supervisor for the use of a quiet, private room to meet with the survivor. Members shall not inform the workplace supervisor of the purpose of their visit other than to indicate that it is a family emergency.
- (g) Offer to call other survivors, friends, or clergy to support the survivors and to avoid leaving survivors alone after notification.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

- (h) Assist the survivors with meeting child care or other immediate needs.
- (i) Provide other assistance to survivors and take reasonable measures to accommodate their needs, wishes, and desires. Care should be taken not to make promises or commitments to survivors that cannot be met.
- (j) Inform the survivors of the name and phone number of the Survivor Support Liaison (see the Survivor Support Liaison section of this policy), if known, and the Department Liaison.
- (k) Provide their contact information to the survivors before departing.
- (l) Document the survivors' names and contact information, as well as the time and location of notification. This information should be forwarded to the Department Liaison.
- (m) Inform the Chief of Police or the authorized designee once survivor notifications have been made so that other South Saint Paul Police Department members may be apprised that survivor notifications are complete.

1019.4.1 OUT-OF-AREA NOTIFICATIONS

The Department Liaison should request assistance from law enforcement agencies in appropriate jurisdictions for in-person notification to survivors who are out of the area.

- (a) The Department Liaison should contact the appropriate jurisdiction using a secure network and provide the assisting agency with the name and telephone number of the department member that the survivors can call for more information following the notification by the assisting agency.
- (b) The Department Liaison may assist in making transportation arrangements for the member's survivors, but will not obligate the Department to pay travel expenses without the authorization of the Chief of Police.

1019.5 NOTIFYING DEPARTMENT MEMBERS

Supervisors or members designated by the Chief of Police are responsible for notifying department members of the line-of-duty death as soon as possible after the survivor notification is made. Notifications and related information should be communicated in person or using secure networks and should not be transmitted over the radio.

Notifications should be made in person and as promptly as possible to all members on-duty at the time of the incident. Members reporting for subsequent shifts within a short amount of time should be notified in person at the beginning of their shifts. Members reporting for duty from their residences should be instructed to contact their supervisors as soon as practicable. Those members who are working later shifts or are on days off should be notified by phone as soon as practicable.

Members having a close bond with the deceased member should be notified of the incident in person. Supervisors should consider assistance (e.g., peer support, modifying work schedules, approving sick leave) for members who are especially affected by the incident.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

Supervisors should direct members not to disclose any information outside the Department regarding the deceased member or the incident.

1019.6 LIAISONS AND COORDINATORS

The Chief of Police or the authorized designee should select members to serve as liaisons and coordinators to handle responsibilities related to a line-of-duty death, including but not limited to:

- (a) Department Liaison.
- (b) Hospital Liaison.
- (c) Survivor Support Liaison.
- (d) Wellness Support Liaison.
- (e) Funeral Liaison.
- (f) Mutual aid coordinator.
- (g) Benefits Liaison.
- (h) Finance coordinator.

Liaisons and coordinators will be directed by the Department Liaison and should be given sufficient duty time to complete their assignments.

Members may be assigned responsibilities of more than one liaison or coordinator position depending on available department resources. The Department Liaison may assign separate liaisons and coordinators to accommodate multiple family units, if needed. The Department should consider seeking assistance from surrounding law enforcement agencies to fill liaison and coordinator positions, as appropriate.

1019.6.1 DEPARTMENT LIAISON

The Department Liaison should be a Division Commander or of sufficient rank to effectively coordinate department resources, and should serve as a facilitator between the deceased member's survivors and the Department. The Department Liaison reports directly to the Chief of Police. The Department Liaison's responsibilities include but are not limited to:

- (a) Directing the other liaisons and coordinators in fulfilling survivors' needs and requests. Consideration should be given to organizing the effort using the National Incident Management System.
- (b) Establishing contact with survivors within 24 hours of the incident and providing them contact information.
- (c) Advising survivors of the other liaison and coordinator positions and their roles and responsibilities.
- (d) Identifying locations that will accommodate a law enforcement funeral and presenting the options to the appropriate survivors, who will select the location.
- (e) Coordinating all official law enforcement notifications and arrangements.
- (f) Making necessary contacts for authorization to display flags at half-staff.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

- (g) Reminding department members of appropriate information-sharing restrictions regarding the release of information that could undermine future legal proceedings.
- (h) Coordinating security checks of the member's residence as necessary and reasonable.
- (i) Serving as a liaison with visiting law enforcement agencies during memorial and funeral services.

1019.6.2 HOSPITAL LIAISON

The Hospital Liaison should work with hospital personnel to:

- (a) Establish a command post or incident command system, as appropriate, to facilitate management of the situation and its impact on hospital operations (e.g., influx of people, parking).
- (b) Arrange for appropriate and separate waiting areas for:
 - 1. The survivors and others whose presence is requested by the survivors.
 - 2. Department members and friends of the deceased member.
 - 3. Media personnel.
- (c) Ensure, as practicable, that any suspects who are in the hospital and their families or friends are not in proximity to the member's survivors or South Saint Paul Police Department members (except for members who may be guarding a suspect).
- (d) Arrange for survivors to receive timely updates regarding the member before information is released to others.
- (e) Arrange for survivors to have private time with the member, if requested.
 - 1. The Hospital Liaison or hospital personnel may need to explain the condition of the member to the survivors to prepare them accordingly.
 - 2. The Hospital Liaison should accompany the survivors into the room, if requested.
- (f) Stay with survivors and provide them with other assistance as needed at the hospital.
- (g) If applicable, explain to the survivors why an autopsy may be needed.
- (h) Make arrangements for hospital bills to be directed to the Department, that the survivors are not asked to sign as guarantor of payment for any hospital treatment, and that the member's residence address, insurance information, and next of kin are not included on hospital paperwork.

Other responsibilities of the Hospital Liaison include but are not limited to:

- Arranging transportation for the survivors back to their residence.
- Working with investigators to gather and preserve the deceased member's equipment and other items that may be of evidentiary value.
- Documenting their actions at the conclusion of duties.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

1019.6.3 SURVIVOR SUPPORT LIAISON

The Survivor Support Liaison should work with the Department Liaison to fulfill the immediate needs and requests of the survivors of any member who has died in the line of duty, and serve as the long-term department contact for survivors.

The Survivor Support Liaison should be selected by the deceased member's Division Commander. The following should be considered when selecting the Survivor Support Liaison:

- The liaison should be an individual the survivors know and with whom they are comfortable working.
- The selection may be made from names recommended by the deceased member's supervisor and/or coworkers. The deceased member's partner or close friends may not be the best selections for this assignment because the emotional connection to the member or survivors may impair their ability to conduct adequate liaison duties.
- The liaison must be willing to assume the assignment with an understanding of the emotional and time demands involved.

The responsibilities of the Survivor Support Liaison include but are not limited to:

- (a) Arranging for transportation of survivors to hospitals, places of worship, funeral homes, and other locations, as appropriate.
- (b) Communicating with the Department Liaison regarding appropriate security measures for the family residence, as needed.
- (c) If requested by the survivors, providing assistance with instituting methods of screening telephone calls made to their residence after the incident.
- (d) Providing assistance with travel and lodging arrangements for out-of-town survivors.
- (e) Returning the deceased member's personal effects from the Department and the hospital to the survivors. The following should be considered when returning the personal effects:
 - 1. Items should not be delivered to the survivors until they are ready to receive the items.
 - 2. Items not retained as evidence should be delivered in a clean, unmarked box.
 - 3. All clothing not retained as evidence should be cleaned and made presentable (e.g., items should be free of blood or other signs of the incident).
 - 4. The return of some personal effects may be delayed due to ongoing investigations.
- (f) Assisting with the return of department-issued equipment that may be at the deceased member's residence.
 - 1. Unless there are safety concerns, the return of the equipment should take place after the funeral at a time and in a manner considerate of the survivors' wishes.
- (g) Working with the Wellness Support Liaison for survivors to have access to available counseling services.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

- (h) Coordinating with the department's Police Chief ([PIO]) to brief the survivors on pending press releases related to the incident and to assist the survivors with media relations in accordance with their wishes (see the Police Chief section of this policy).
- (i) Briefing survivors on investigative processes related to the line-of-duty death, such as criminal, internal, and administrative investigations.
- (j) Informing survivors of any related criminal proceedings and accompanying them to such proceedings.
- (k) Introducing survivors to prosecutors, victim's assistance personnel, and other involved personnel as appropriate.
- (l) Maintaining long-term contact with survivors and taking measures to sustain a supportive relationship (e.g., follow-up visits, phone calls, cards on special occasions, special support during holidays).
- (m) Inviting survivors to department activities, memorial services (e.g., as applicable, the Annual Candlelight Vigil at the National Law Enforcement Officers Memorial), or other functions as appropriate.

Survivor Support Liaisons providing services after an incident resulting in multiple members being killed should coordinate with and support each other through conference calls or meetings as necessary.

The Department recognizes that the duties of a Survivor Support Liaison will often affect regular assignments over many years, and is committed to supporting members in the assignment.

If needed, the Survivor Support Liaison should be issued a personal communication device (PCD) owned by the Department to facilitate communications necessary to the assignment. The department-issued PCD shall be used in accordance with the Personal Communication Devices Policy.

1019.6.4 WELLNESS SUPPORT LIAISON

The Wellness Support Liaison should work with the department wellness coordinator or the authorized designee and other liaisons and coordinators to make wellness support and counseling services available to members and survivors who are impacted by a line-of-duty death. The responsibilities of the Wellness Support Liaison include but are not limited to:

- (a) Identifying members who are likely to be significantly affected by the incident and may have an increased need for wellness support and counseling services, including:
 - 1. Members involved in the incident.
 - 2. Members who witnessed the incident.
 - 3. Members who worked closely with the deceased member but were not involved in the incident.
- (b) Making arrangements for members who were involved in or witnessed the incident to be relieved of department responsibilities until they can receive wellness support.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

- (c) Making wellness support and counseling resources (e.g., peer support, Critical Incident Stress Debriefing) available to members as soon as reasonably practicable following the line-of-duty death.
- (d) Coordinating with the Survivor Support Liaison to inform survivors of available wellness support and counseling services and assisting with arrangements as needed.
- (e) Following up with members and the Survivor Support Liaison in the months following the incident to determine if additional wellness support or counseling services are needed.

1019.6.5 FUNERAL LIAISON

The Funeral Liaison should work with the Department Liaison, Survivor Support Liaison, and survivors to coordinate funeral arrangements to the extent the survivors wish. The Funeral Liaison's responsibilities include but are not limited to:

- (a) Assisting survivors in working with the funeral director regarding funeral arrangements and briefing them on law enforcement funeral procedures.
- (b) Completing funeral notification to other law enforcement agencies.
- (c) Coordinating the funeral activities of the Department, including but not limited to the following:
 - 1. Honor Guard
 - (a) Casket watch
 - (b) Color guard
 - (c) Pallbearers
 - (d) Bell/rifle salute
 - 2. Bagpipers/bugler
 - 3. Uniform for burial
 - 4. Flag presentation
 - 5. Last radio call
- (d) Briefing the Chief of Police and command staff concerning funeral arrangements.
- (e) Assigning an officer to remain at the family home during the viewing and funeral.
- (f) Arranging for transportation of the survivors to and from the funeral home and interment site using department vehicles and drivers.
- (g) Addressing event-related logistical matters (e.g., parking, visitor overflow, public assembly areas).

1019.6.6 MUTUAL AID COORDINATOR

The mutual aid coordinator should work with the Department Liaison and the Funeral Liaison to request and coordinate any assistance from outside law enforcement agencies needed for, but not limited to:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

- (a) Traffic control during the deceased member's funeral.
- (b) Area coverage so that as many South Saint Paul Police Department members can attend funeral services as possible.

The mutual aid coordinator should perform duties in accordance with the Outside Agency Assistance Policy.

Where practicable, the Chief of Police should appoint a mutual aid coordinator to identify external resources in advance of any need (e.g., regional honor guard teams, county- or state-wide resources).

1019.6.7 BENEFITS LIAISON

The Benefits Liaison should provide survivors with information concerning available benefits and will assist them in applying for benefits. Responsibilities of the Benefits Liaison include but are not limited to:

- (a) Confirming the filing of workers' compensation claims and related paperwork (see the Occupational Disease, Personal Injury and Death Reporting Policy).
- (b) Researching and assisting survivors with application for federal government survivor benefits, such as those offered through the following:
 - 1. Public Safety Officers' Benefits Program, including financial assistance available through the Public Safety Officers' Educational Assistance (PSOEA) Program, as applicable (34 USC § 10281 et seq.).
 - 2. Social Security Administration.
 - 3. Department of Veterans Affairs.
- (c) Researching and assisting survivors with application for state and local government survivor benefits.
 - 1. Survivor benefits (Minn. Stat. § 353.657).
 - 2. Disability survivor benefits (Minn. Stat. § 353.656).
 - 3. Continued health insurance coverage benefit (Minn. Stat. § 299A.465).
 - 4. Death benefit (Minn. Stat. § 299A.44).
 - 5. Education benefit (Minn. Stat. § 299A.45).
- (d) Researching and assisting survivors with application for other survivor benefits such as:
 - 1. Private foundation survivor benefits programs.
 - 2. Survivor scholarship programs.
- (e) Researching and informing survivors of support programs sponsored by police associations and other organizations.
- (f) Documenting and informing survivors of inquiries and interest regarding public donations to the survivors.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

1. If requested, working with the finance coordinator to assist survivors with establishing a process for the receipt of public donations.
- (g) Providing survivors with a summary of the nature and amount of benefits applied for, including the name of a contact person at each benefit office. Printed copies of the summary and benefit application documentation should be provided to affected survivors.
- (h) Maintaining contact with the survivors and assisting with subsequent benefit questions and processes as needed.

1019.6.8 FINANCE COORDINATOR

The finance coordinator should work with the Chief of Police and the Department Liaison to manage financial matters related to the line-of-duty death. The finance coordinator's responsibilities include, but are not limited to:

- (a) Establishing methods for purchasing and monitoring costs related to the incident.
- (b) Providing information on finance-related issues, such as:
 1. Paying survivors' travel costs if authorized.
 2. Transportation costs for the deceased.
 3. Funeral and memorial costs.
 4. Related funding or accounting questions and issues.
- (c) Working with the Benefits Liaison to establish a process for the receipt of public donations to the deceased member's survivors.
- (d) Providing accounting and cost information as needed.

1019.7 POLICE CHIEF

In the event of a line-of-duty death, the department's [PIO] should be the department's contact point for the media. As such, the [PIO] should coordinate with the Department Liaison to:

- (a) Collect and maintain the most current incident information and determine what information should be released.
- (b) Instruct department members to direct any media inquiries to the [PIO].
- (c) Prepare necessary press releases.
 1. Coordinate with other entities having media roles (e.g., outside agencies involved in the investigation or incident).
 2. Disseminate important public information, such as information on how the public can show support for the department and deceased member's survivors.
- (d) Arrange for community and media briefings by the Chief of Police or the authorized designee as appropriate.
- (e) Respond, or coordinate the response, to media inquiries.
- (f) If requested, assist the member's survivors with media inquiries.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

1. Brief the survivors on handling sensitive issues such as the types of questions that reasonably could jeopardize future legal proceedings.
- (g) Release information regarding memorial services and funeral arrangements to department members, other agencies, and the media as appropriate.
- (h) If desired by the survivors, arrange for the recording of memorial and funeral services via photos and/or video.

The identity of deceased members should be withheld until the member's survivors have been notified. If the media have obtained identifying information for the deceased member prior to survivor notification, the [PIO] should request that the media withhold the information from release until proper notification can be made to survivors. The [PIO] should notify media when survivor notifications have been made.

1019.8 DEPARTMENT CHAPLAIN

The Department chaplain may serve a significant role in line-of-duty deaths. Chaplain duties may include but are not limited to:

- Assisting with survivor notifications and assisting the survivors with counseling, emotional support, or other matters, as appropriate.
- Assisting liaisons and coordinators with their assignments, as appropriate.
- Assisting department members with counseling or emotional support, as requested and appropriate.

Further information on the potential roles and responsibilities of the chaplain is in the Chaplains Policy.

1019.9 INVESTIGATION OF THE INCIDENT

The Chief of Police should make necessary assignments to conduct thorough investigations of any line-of-duty death and may choose to use the investigation process outlined in the Officer-Involved Shootings and Deaths Policy.

Investigators from other agencies may be assigned to work on any criminal investigation related to line-of-duty deaths. Partners, close friends, or personnel who worked closely with the deceased member should not have any investigative responsibilities because such relationships may impair the objectivity required for an impartial investigation of the incident.

Involved department members should be kept informed of the progress of the investigations and provide investigators with any information that may be pertinent to the investigations.

1019.10 LINE-OF-DUTY DEATH OF A LAW ENFORCEMENT ANIMAL

The Chief of Police may authorize appropriate memorial and funeral services for law enforcement animals killed in the line of duty.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Line-of-Duty Deaths

1019.11 NON-LINE-OF-DUTY DEATH

The Chief of Police may authorize certain support services for the death of a member not occurring in the line of duty.

Wellness Program

1022.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance on establishing and maintaining a proactive wellness program for department members and consortium agency members.

The wellness program is intended to be a holistic approach to a member's well-being and encompasses aspects such as physical fitness, mental health, and overall wellness.

Additional information on member wellness is provided in the:

- Chaplains Policy.
- Line-of-Duty Deaths Policy.
- Drug- and Alcohol-Free Workplace Policy.

1022.1.1 DEFINITIONS

Definitions related to this policy include:

Critical incident – An event or situation that may cause a strong emotional, cognitive, or physical reaction that has the potential to interfere with daily life.

Critical Incident Stress - Any change in the environment that produces physical and/or psychological reactions. These reactions include but are not limited to: increased heart rate, rise in blood pressure, muscular tension, irritability, and heightened or reduced awareness.

Critical Incident Stress Debriefing (CISD) – A standardized approach using a discussion format to provide education, support, and emotional release opportunities for members involved in work-related critical incidents.

Peer Support Counselor –An employee of the police department selected by the Chief or designee to perform peer counseling services to other members of the agency. These services will be in accordance with standards that are both established by an accredited mental health organization or network and recognized by the Commissioner of Public Safety. Peer Support Counselors are trained to recognize and refer employees that require professional intervention or support beyond the scope of their training to a licensed mental health professional.

Privacy - The expectation of an individual that disclosure of personal information is confined to or intended for the Peer Support Counselor only.

Confidentiality - A professional or ethical duty for the Peer Support Counselor to refrain from disclosing information from or about a recipient of peer support services, barring any exceptions that should be disclosed at the outset.

Privilege - The legal protection from being compelled to disclose communications in certain protected relationships, such as attorney and client, doctor and patient, priest and confessor; and in Minnesota, Peer Support Counselor and recipient of peer support services.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Wellness Program

Mental Health Professional - A licensed and in good standing Psychologist, Psychiatrist, Licensed Independent Clinical Social Worker, or Licensed Professional Clinical Counselor.

Defusing - A discussing to stabilize people affected by the critical incident so that they can return to their normal routine without unusual stress. A defusing is best conducted within one to four hours after a critical incident but no more than twelve hours.

Consortium - The Peer Support Team Consortium consists of the Farmington Police Department, Inver Grove Heights Police Department, South St. Paul Police Department, and West St. Paul Police Department.

1022.2 POLICY

It is the policy of the South Saint Paul Police Department to prioritize member wellness to support a healthy quality of life for department members and consortium agency members. The Department will maintain a wellness program that supports its members with proactive wellness resources, critical incident response, and follow-up support.

1022.3 WELLNESS COORDINATOR

The Chief of Police should appoint a trained wellness coordinator. The coordinator should report directly to the Chief of Police or the authorized designee and should collaborate with advisers (e.g., Department of Human Resources, legal counsel, licensed psychotherapist, qualified health professionals), as appropriate, to fulfill the responsibilities of the position, including but not limited to:

- (a) Identifying wellness support providers (e.g., licensed psychotherapists, external peer support providers, physical therapists, dietitians, physical fitness trainers holding accredited certifications).
 - 1. As appropriate, selected providers should be trained and experienced in providing mental wellness support and counseling to public safety personnel.
 - 2. When practicable, the Department should not use the same licensed psychotherapist for both member wellness support and fitness for duty evaluations.
- (b) Developing management and operational procedures for department peer support counselors, such as:
 - 1. Peer support counselor selection and retention.
 - 2. Training and applicable certification requirements.
 - 3. Deployment.
 - 4. Managing potential conflicts between peer support counselor and those seeking service.
 - 5. Monitoring and mitigating peer support counselor emotional fatigue (i.e., compassion fatigue) associated with providing peer support.
 - 6. Using qualified peer support personnel from other public safety agencies or outside organizations for department peer support, as appropriate.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Wellness Program

- (c) Verifying members have reasonable access to peer support or licensed psychotherapist support.
- (d) Establishing procedures for CISDs, including:
 - 1. Defining the types of incidents that may initiate debriefings.
 - 2. Steps for organizing debriefings.
- (e) Facilitating the delivery of wellness information, training, and support through various methods appropriate for the situation (e.g., phone hotlines, electronic applications).
- (f) Verifying a confidential, appropriate, and timely Employee Assistance Program (EAP) is available for members. This also includes:
 - 1. Obtaining a written description of the program services.
 - 2. Providing for the methods to obtain program services.
 - 3. Providing referrals to the EAP for appropriate diagnosis, treatment, and follow-up resources.
 - 4. Obtaining written procedures and guidelines for referrals to, or mandatory participation in, the program.
 - 5. Obtaining training for supervisors in their role and responsibilities, and identification of member behaviors that would indicate the existence of member concerns, problems, or issues that could impact member job performance.
- (g) Assisting members who have become disabled with application for federal government benefits such as those offered through the Public Safety Officers' Benefits Program (34 USC § 10281 et seq.).
 - 1. The coordinator should work with appropriate Department liaisons to assist qualified members and survivors with benefits, wellness support, and counseling services, as applicable, when there has been a member death (see the Line-of-Duty Deaths Policy for additional guidance).

1022.4 DEPARTMENT PEER SUPPORT

1022.4.1 PEER SUPPORT COUNSELOR SELECTION CRITERIA

The selection of a department peer support counselor will be at the discretion of the coordinator. Selection should be based on the member's:

- Desire to be a peer support counselor.
- Experience or tenure.
- Demonstrated ability as a positive role model.
- Ability to communicate and interact effectively.
- Evaluation by supervisors and any current peer support counselors.

1022.4.2 PEER SUPPORT COUNSELOR RESPONSIBILITIES

The responsibilities of department peer support counselors include:

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Wellness Program

- Convey trust and ensure confidentiality within the guidelines to employees who seek assistance from the Peer Support Program;
- Provide emotional support during and after times of personal and/or professional crisis to employees who express the need for assistance;
- Support employees during tragedies or critical incidents;
- Make proper referrals to professional resources;
- Check-in with employees who are off work due to extended illness or injury and provide support for those who express the need for assistance;
- Be available to employees for additional follow-up support;
- Maintain contact with the Program Director regarding program activities without breaching confidentiality;
- Agree to be contacted and, if necessary, respond at any hour to assist an employee in need;
- Attend Peer Support trainings and meetings
- Providing referrals to licensed psychotherapists and other resources, where appropriate.
 - (a) Referrals should be made to department-designated resources in situations that are beyond the scope of the peer support member's training.

1022.4.3 PEER SUPPORT COUNSELOR TRAINING

Peer Support Counselors will be required to attend a Peer Support training course approved by the Coordinator that meets the Minnesota Department of Public Safety approved training requirements. Peer Support Counselors may be required to advance their skills through continuing training as scheduled by the Program Director.

1022.4.4 PEER SUPPORT TEAM CLINICAL LEAD

The Peer Support Team Clinical Lead is a contracted mental health provider who services as the clinical expert for the team.

The Peer Support Team Clinical Lead should report directly to the Chief of Police or the authorized designee and should collaborate with advisers (e.g. Department of Human Resources, legal counsel, licensed psychotherapist, qualified health professionals), as appropriate, to fulfill the responsibilities of the position including but not limited to:

- (a) Developing management and operational procedures for department peer support counselors, such as;
 - 1. Managing potential conflicts between peer support counselors and those seeking service.
 - 2. Monitoring and mitigating peer support member emotional fatigue (i.e., compassion fatigue) associated with providing peer support.
 - 3. Program and policy development.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Wellness Program

4. Available for consultation with peer support team counselors.
5. Available to peer support team counselors for debriefing
6. Available for debriefing with peer support team counselors
7. Ability to provide customized peer support team training and education.

1022.5 CRITICAL INCIDENT STRESS DEBRIEFINGS

A Critical Incident Stress Debriefing should occur as soon as practicable following a critical incident. The coordinator is responsible for organizing the debriefing. Notes and recorded statements shall not be taken because the sole purpose of the debriefing is to help mitigate the stress-related effects of a critical incident.

The debriefing is not part of any investigative process. Care should be taken not to release or repeat any communication made during a debriefing unless otherwise authorized by policy, law, or a valid court order.

Attendance at the debriefing should only include peer support counselors, and/or critical incident stress management team members, and those directly involved in the incident.

Members who witness a critical incident are prohibited from providing critical incident stress management services at a debriefing about an incident that they witnessed (Minn. Stat. § 181.9732).

1022.5.1 PEER SUPPORT COUNSELOR COMMUNICATIONS

Communications with peer support counselors are confidential and shall not be disclosed except as provided in Minn. Stat. § 181.9731. A peer support counselor is an individual who is designated by the Department and trained to provide peer counseling services (Minn. Stat. § 181.9731).

Confidentiality is the core foundation of the Peer Support Counseling Program.

- The contents of communication in a peer support counseling environment are considered private information pursuant to the Minnesota Data Practices Act, Chapter 13.
- Conversations are considered private and protected by MSS 13.43 Subd. 9 and 11 and MSS 181.9731.
- Limits to confidentiality must be consistent with state and federal laws as well as department policy. It is essential that Peer Support Counselor inform the employee, prior to any discussion, what the limitations and exceptions are regarding information revealed.
- Recipients of peer support should be advised that confidentiality may be broken for the following situations:
 - Threats to self
 - Threats to others
 - Suspected child or elder abuse

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Wellness Program

- Where disclosure is requested by peer
- In the event information is disclosed in a peer support counseling session that an employee is an immediate threat to themselves or others, the Peer Support Counselor shall notify the clinical lead or appropriate resources.
- The acceptance and success of the Peer Support Program will be largely dependent upon the observance of strict confidentiality. Peer Support Counselors shall be entrusted to maintain the confidential nature of conversations.
- Disclosures under these exceptions will be made directly to the designated Peer Support Clinical Lead assigned to the program.
- In cases where a question regarding confidentiality arises, the Peer Support Counselor shall immediately contact the Program Director or Designated Peer Support Clinical Lead, who shall take the appropriate action.
- Peer Support Counselors must not provide information to supervisors or fellow peer support members obtained through peer support contact.
- Peer Support Counselors who may be involved in conducting a criminal or internal investigation of another employee shall remove themselves from the peer support role on that particular incident in order to avoid conflict of interest.
- Peer Support Counselors must not keep written, formal or private records of supportive contacts other than non-identifying statistical records that help document the general productivity of the program.
- Peer Support Counselors found to have violated the confidentiality of the program shall be immediately removed from the program and subject to disciplinary action, in addition to potential criminal charges for willful violations of the Minnesota Government Data Practices Act.

1022.5.2 CRITICAL INCIDENT STRESS MANAGEMENT TEAM MEMBER COMMUNICATIONS

Communications with critical incident stress management team members are confidential and shall not be disclosed except as provided in Minn. Stat. § 181.9732. A critical incident stress management team member is an individual who is designated by the Department and trained to provide critical incident stress management services (Minn. Stat. § 181.9732).

1022.6 PHYSICAL WELLNESS PROGRAM

The coordinator is responsible for establishing guidelines for any on-duty physical wellness program, including the following:

- (a) Voluntary participation by members
- (b) Allowable physical fitness activities
- (c) Permitted times and locations for physical fitness activities
- (d) Acceptable use of department-provided physical fitness facilities and equipment
- (e) Individual health screening and fitness assessment

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Wellness Program

- (f) Individual education (e.g., nutrition, sleep habits, proper exercise, injury prevention) and goal-setting
- (g) Standards for fitness incentive programs. The coordinator should collaborate with the appropriate entities (e.g., human resources, legal counsel) to verify that any standards are nondiscriminatory.
- (h) Maintenance of physical wellness logs (e.g., attendance, goals, standards, progress)
- (i) Ongoing support and evaluation

1022.7 WELLNESS PROGRAM AUDIT

At least annually, the coordinator or the authorized designee should review the effectiveness of the department's wellness program. The review should include the following factors:

- Data on the types of support services provided
- Wait times for support services
- Participant feedback, if available
- Program improvement recommendations
- Policy revision recommendations

The coordinator may present a memo to the Chief of Police for review and consideration of updates to improve program effectiveness.

1022.8 TRAINING

The coordinator or the authorized designee should collaborate with the Support Services Commander to provide all members with regular education and training on topics related to member wellness, including but not limited to:

- The availability and range of department wellness support systems.
- Suicide Prevention.
- Recognizing and managing mental distress, emotional fatigue, post-traumatic stress, and other possible reactions to trauma.
- Alcohol and substance disorder awareness.
- Countering sleep deprivation and physical fatigue.
- Anger management.
- Marriage and family wellness.
- Benefits of exercise and proper nutrition.
- Effective time and personal financial management skills.

Training materials, curriculum, and attendance records should be forwarded to the Support Services Commander as appropriate for inclusion in training records.

South Saint Paul Police Department

S Saint Paul PD Policy Manual

Wellness Program

1022.8.1 ADDITIONAL WELLNESS TRAINING FOR OFFICERS

Officers shall complete in-service wellness training approved by POST as provided in Minn. Stat. § 626.8478.

The Chief of Police shall ensure that wellness training records are maintained in compliance with Minn. Stat. § 626.8478 and are made available as requested by POST (Minn. Stat. § 626.8478).

South Saint Paul Police Department Policy Manual

S Saint Paul PD Policy Manual

Attachments

MN POST Professional Conduct of Peace Officers Model Policy.pdf

PROFESSIONAL CONDUCT OF PEACE OFFICERS MODEL POLICY
MN STAT 626.8457

I. POLICY

It is the policy of the _____ (law enforcement agency) to investigate circumstances that suggest an officer has engaged in unbecoming conduct, and impose disciplinary action when appropriate.

II. PROCEDURE

This policy applies to all officers of this agency engaged in official duties whether within or outside of the territorial jurisdiction of this agency. Unless otherwise noted this policy also applies to off duty conduct. Conduct not mentioned under a specific rule but that violates a general principle is prohibited.

A. PRINCIPLE ONE

Peace officers shall conduct themselves, whether on or off duty, in accordance with the Constitution of the United States, the Minnesota Constitution, and all applicable laws, ordinances and rules enacted or established pursuant to legal authority.

1. Rationale: Peace officers conduct their duties pursuant to a grant of limited authority from the community. Therefore, officers must understand the laws defining the scope of their enforcement powers. Peace officers may only act in accordance with the powers granted to them.

2. Rules

- a) Peace officers shall not knowingly exceed their authority in the enforcement of the law.
- b) Peace officers shall not knowingly disobey the law or rules of criminal procedure in such areas as interrogation, arrest, detention, searches, seizures, use of informants, and preservation of evidence, except where permitted in the performance of duty under proper authority.
- c) Peace officers shall not knowingly restrict the freedom of individuals, whether by arrest or detention, in violation of the Constitutions and laws of the United States and the State of Minnesota.
- d) Peace officers, whether on or off duty, shall not knowingly commit any criminal offense under any laws of the United States or any state or local jurisdiction.
- e) Peace officers will not, according to MN STAT 626.863, knowingly allow a person who is not a peace officer to make a representation of being a peace officer or perform any act, duty or responsibility reserved by law for a peace officer.

B. PRINCIPLE TWO

Peace officers shall refrain from any conduct in an official capacity that detracts from the public's faith in the integrity of the criminal justice system.

1. Rationale: Community cooperation with the police is a product of its trust that officers will act honestly and with impartiality. The peace officer, as the public's initial contact with the criminal justice system, must act in a manner that instills such trust.

2. Rules

- a) Peace officers shall carry out their duties with integrity, fairness and impartiality.

- b) Peace officers shall not knowingly make false accusations of any criminal, ordinance, traffic or other law violation. This provision shall not prohibit the use of deception during criminal investigations or interrogations as permitted under law.
- c) Peace officers shall truthfully, completely, and impartially report, testify and present evidence, including exculpatory evidence, in all matters of an official nature.
- d) Peace officers shall take no action knowing it will violate the constitutional rights of any person.
- e) Peace officers must obey lawful orders but a peace officer must refuse to obey any order the officer knows would require the officer to commit an illegal act. If in doubt as to the clarity of an order the officer shall, if feasible, request the issuing officer to clarify the order. An officer refusing to obey an order shall be required to justify his or her actions.
- f) Peace officers learning of conduct or observing conduct that is in violation of any law or policy of this agency shall take necessary action and report the incident to the officer's immediate supervisor who shall forward the information to the CLEO. If the officer's immediate supervisor commits the misconduct the officer shall report the incident to the immediate supervisor's supervisor.

C. PRINCIPLE THREE

Peace officers shall perform their duties and apply the law impartially and without prejudice or discrimination.

- 1. **Rationale:** Law enforcement effectiveness requires public trust and confidence. Diverse communities must have faith in the fairness and impartiality of their police. Peace officers must refrain from fostering disharmony in their communities based upon diversity and perform their duties without regard to race, color, creed, religion, national origin, gender, marital status, or status with regard to public assistance, disability, sexual orientation or age.
- 2. **Rules**
 - a) Peace officers shall provide every person in our society with professional, effective and efficient law enforcement services.
 - b) Peace officers shall not allow their law enforcement decisions to be influenced by race, color, creed, religion, national origin, gender, marital status, or status with regard to public assistance, disability, sexual orientation or age.

D. PRINCIPLE FOUR

Peace officers shall not, whether on or off duty, exhibit any conduct which discredits themselves or their agency or otherwise impairs their ability or that of other officers or the agency to provide law enforcement services to the community.

- 1. **Rationale:** A peace officer's ability to perform his or her duties is dependent upon the respect and confidence communities have for the officer and law enforcement officers in general. Peace officers must conduct themselves in a manner consistent with the integrity and trustworthiness expected of them by the public.
- 2. **Rules**

- a) Peace officers shall not consume alcoholic beverages or chemical substances while on duty except as permitted in the performance of official duties, and under no circumstances while in uniform, except as provided for in **c**).
- b) Peace officers shall not consume alcoholic beverages to the extent the officer would be rendered unfit for the officer's next scheduled shift. A peace officer shall not report for work with the odor of an alcoholic beverage on the officer's breath.
- c) Peace officers shall not use narcotics, hallucinogens, or other controlled substances except when legally prescribed. When medications are prescribed, the officer shall inquire of the prescribing physician whether the medication will impair the officer in the performance of the officer's duties. The officer shall immediately notify the officer's supervisor if a prescribed medication is likely to impair the officer's performance during the officer's next scheduled shift.
- d) Peace officers, whether on or off duty, shall not engage in any conduct which the officer knows, or should reasonably know, constitutes sexual harassment as defined under Minnesota law, including but not limited to; making unwelcome sexual advances, requesting sexual favors, engaging in sexually motivated physical contact or other verbal or physical conduct or communication of a sexual nature.
- e) Peace officers shall not commit any acts which constitute sexual assault or indecent exposure as defined under Minnesota law. Sexual assault does not include a frisk or other search done in accordance with proper police procedures.
- f) Peace officers shall not commit any acts which, as defined under Minnesota law, constitute (1) domestic abuse, or (2) the violation of a court order restraining the officer from committing an act of domestic abuse or harassment, having contact with the petitioner, or excluding the peace officer from the petitioner's home or workplace.
- g) Peace officers, in the course of performing their duties, shall not engage in any sexual contact or conduct constituting lewd behavior including but not limited to, showering or receiving a massage in the nude, exposing themselves, or making physical contact with the nude or partially nude body of any person, except as pursuant to a written policy of the agency.
- h) Peace officers shall avoid regular personal associations with persons who are known to engage in criminal activity where such associations will undermine the public trust and confidence in the officer or agency. This rule does not prohibit those associations that are necessary to the performance of official duties or where such associations are unavoidable because of the officer's personal or family relationships.

E. PRINCIPLE FIVE

Peace officers shall treat all members of the public courteously and with respect.

- 1. **Rationale:** Peace officers are the most visible form of local government. Therefore, peace officers must make a positive impression when interacting with the public and each other.
- 2. **Rules**
 - a) Peace officers shall exercise reasonable courtesy in their dealings with the public, other officers, superiors and subordinates.

- b) No peace officer shall ridicule, mock, deride, taunt, belittle, willfully embarrass, humiliate, or shame any person to do anything reasonably calculated to incite a person to violence.
- c) Peace officers shall promptly advise any inquiring citizen of the agency's complaint procedure and shall follow the established agency policy for processing complaints.

F. PRINCIPLE SIX

Peace officers shall not compromise their integrity nor that of their agency or profession by accepting, giving or soliciting any gratuity which could be reasonably interpreted as capable of influencing their official acts or judgments or by using their status as a peace officer for personal, commercial or political gain.

1. Rationale: For a community to have faith in its peace officers, officers must avoid conduct that does or could cast doubt upon the impartiality of the individual officer or the agency.

2. Rules

- a) Peace officers shall not use their official position, identification cards or badges for: (1) personal or financial gain for themselves or another person; (2) obtaining privileges not otherwise available to them except in the performance of duty; and (3) avoiding consequences of unlawful or prohibited actions.
- b) Peace officers shall not lend to another person their identification cards or badges or permit these items to be photographed or reproduced without approval of the chief law enforcement officer.
- c) Peace officers shall refuse favors or gratuities which could reasonably be interpreted as capable of influencing official acts or judgments.
- d) Unless required for the performance of official duties, peace officers shall not, while on duty, be present at establishments that have the primary purpose of providing sexually oriented adult entertainment. This rule does not prohibit officers from conducting walk-throughs of such establishments as part of their regularly assigned duties.
- e) Peace officers shall:
 - not authorize the use of their names, photographs or titles in a manner that identifies the officer as an employee of this agency in connection with advertisements for any product, commodity or commercial enterprise;
 - maintain a neutral position with regard to the merits of any labor dispute, political protest, or other public demonstration while acting in an official capacity;
 - not make endorsements of political candidates while on duty or while wearing the agency's official uniform.

This section does not prohibit officers from expressing their views on existing, proposed or pending criminal justice legislation in their official capacity.

G. PRINCIPLE SEVEN

Peace officers shall not compromise their integrity, nor that of their agency or profession, by taking or attempting to influence actions when a conflict of interest exists.

1. Rationale: For the public to maintain its faith in the integrity and impartiality of peace officers and their agencies officers must avoid taking or influencing official actions

where those actions would or could conflict with the officer's appropriate responsibilities.

2. Rules

- a) Unless required by law or policy a peace officer shall refrain from becoming involved in official matters or influencing actions of other peace officers in official matters impacting the officer's immediate family, relatives, or persons with whom the officer has or has had a significant personal relationship.
- b) Unless required by law or policy a peace officer shall refrain from acting or influencing official actions of other peace officers in official matters impacting persons with whom the officer has or has had a business or employment relationship.
- c) A peace officer shall not use the authority of their position as a peace officer or information available to them due to their status as a peace officer for any purpose of personal gain including but not limited to initiating or furthering personal and/or intimate interactions of any kind with persons with whom the officer has had contact while on duty.
- d) A peace officer shall not engage in any off-duty employment if the position compromises or would reasonably tend to compromise the officer's ability to impartially perform the officer's official duties.

H. PRINCIPLE EIGHT

Peace officers shall observe the confidentiality of information available to them due to their status as peace officers.

- 1. **Rationale:** Peace officers are entrusted with vast amounts of private and personal information or access thereto. Peace officers must maintain the confidentiality of such information to protect the privacy of the subjects of that information and to maintain public faith in the officer's and agency's commitment to preserving such confidences.

2. Rules

- a) Peace officers shall not knowingly violate any legal restriction for the release or dissemination of information.
- b) Peace officers shall not, except in the course of official duties or as required by law, publicly disclose information likely to endanger or embarrass victims, witnesses or complainants.
- c) Peace officers shall not divulge the identity of persons giving confidential information except as required by law or agency policy.

I. APPLICATION

Any disciplinary actions arising from violations of this policy shall be investigated in accordance with MN STAT 626.89, Peace Officer Discipline Procedures Act and the law enforcement agency's policy on Allegations of Misconduct as required by *MN RULES* 6700.2000 to 6700.2600.

PB Rev 01/2011

Model Sexual Assault Investigation Policy 02.16.21.pdf

I. PURPOSE

The purpose of this policy is to provide employees with guidelines for responding to reports of sexual assault. This agency will strive:

- a) To afford maximum protection and support to victims of sexual assault or abuse through a coordinated program of law enforcement and available victim services with an emphasis on a victim centered approach;
- b) To reaffirm peace officers' authority and responsibility to conducting thorough preliminary and follow up investigations and to make arrest decisions in accordance with established probable cause standards;
- c) To increase the opportunity for prosecution and victim services.

II. POLICY

It is the policy of the _____ (law enforcement agency) to recognize sexual assault as a serious problem in society and to protect victims of sexual assault by ensuring its peace officers understand the laws governing this area. Sexual assault crimes are under-reported to law enforcement and the goal of this policy is in part to improve victim experience in reporting so that more people are encouraged to report.

All employees should take a professional, victim-centered approach to sexual assaults, protectively investigate these crimes, and coordinate with prosecution in a manner that helps restore the victim's dignity and autonomy. While doing so, it shall be this agency's goal to decrease the victim's distress, increase the victim's understanding of the criminal justice system and process, and promote public safety.

Peace officers will utilize this policy in response to sexual assault reported to this agency. This agency will aggressively enforce the laws without bias and prejudice based on race, marital status, sexual orientation, economic status, age, disability, gender, religion, creed, or national origin.

III. DEFINITIONS

For purpose of this policy, the words and phrases in this section have the following meaning given to them, unless another intention clearly appears.

A. **Consent:** As defined by Minn. Stat. 609.341, which states:

- (1) Words or overt actions by a person indicating a freely given present agreement to perform a particular sexual act with the actor. Consent does not mean the existence of a prior or current social relationship between the actor and the complainant or that the complainant failed to resist a particular sexual act.
- (2) A person who is mentally incapacitated or physically helpless as defined by Minnesota Statute 609.341 cannot consent to a sexual act.

- (3) Corroboration of the victim's testimony is not required to show lack of consent.
- B. **Child or Minor:** a person under the age of 18.
- C. **Medical Forensic Examiner:** The health care provider conducting a sexual assault medical forensic examination.
- D. **Sexual Assault:** A person who engages in sexual contact or penetration with another person in a criminal manner as identified in MN Statute 609.342 to 609.3451.
- E. **Family and Household Member:** As defined in Minn. Stat. 518.B.01 Subd.2.b. to include:
- (1) spouses or former spouses;
 - (2) parents and children;
 - (3) persons related by blood;
 - (4) persons who are presently residing together or who have resided together in the past;
 - (5) persons who have a child in common regardless of whether they have been married or have lived together at any time;
 - (6) a man and woman if the woman is pregnant and the man is alleged to be the father, regardless of whether they have been married or have lived together at any time; and
 - (7) persons involved in a significant romantic or sexual relationship
- F. **Sexual Assault Medical Forensic Examination:** An examination of a sexual assault patient by a health care provider, ideally one who has specialized education and clinical experience in the collection of forensic evidence and treatment of these patients.
- G. **Victim Advocate:** A Sexual Assault Counselor defined by Minn. Stat. 595.02, subd. 1(k) and/or Domestic Abuse Advocate as defined by Minn. Stat. 595.02, subd. 1(1) who provide confidential advocacy services to victims of sexual assault and domestic abuse. Victim advocates as defined provide coverage in all counties in Minnesota. Minnesota Office of Justice Programs (MN OJP) can assist departments in locating their local victim advocacy agency for the purposes outlined in this policy.
- H. **Victim Centered:** A victim-centered approach prioritizes the safety, privacy and well-being of the victim and aims to create a supportive environment in which the victim's rights are respected and in which they are treated with dignity and respect. This approach acknowledges and respects a victims' input into the criminal justice response and recognizes victims are not responsible for the crimes committed against them.
- I. **Vulnerable Adult:** any person 18 years of age or older who:
- (1) is a resident inpatient of a facility as defined in Minn. Stat. 626.5572. Subd. 6;

- (2) receives services at or from a facility required to be licensed to serve adults under sections [245A.01](#) to [245A.15](#), except that a person receiving outpatient services for treatment of chemical dependency or mental illness, or one who is committed as a sexual psychopathic personality or as a sexually dangerous person under chapter 253B, is not considered a vulnerable adult unless the person meets the requirements of clause (4);
- (3) receives services from a home care provider required to be licensed under sections [144A.43](#) to [144A.482](#); or from a person or organization that exclusively offers, provides, or arranges for personal care assistance services under the medical assistance program as authorized under sections [256B.0625, subdivision 19a](#), [256B.0651](#) to [256B.0654](#), and [256B.0659](#); or
- (4) regardless of residence or whether any type of service is received, possesses a physical or mental infirmity or other physical, mental, or emotional dysfunction:
 - (i) that impairs the individual's ability to provide adequately for the individual's own care without assistance, including the provision of food, shelter, clothing, health care, or supervision; and
 - (ii) because of the dysfunction or infirmity and the need for assistance, the individual has an impaired ability to protect the individual from maltreatment.

IV. PROCEDURES

A. Communications Personnel Response/Additional Actions by Responding Officers

Communications personnel and/or law enforcement officers should inform the victim of ways to ensure critical evidence is not lost, to include the following:

- 1) Suggest that the victim not bathe, or clean him or herself if the assault took place recently.
- 2) Recommend that if a victim needs to relieve themselves, they should collect urine in a clean jar for testing, and should avoid wiping after urination.
- 3) Asking the victim to collect any clothing worn during or after the assault and if possible, place in a paper bag, instructing the victim not to wash the clothing (per department policy).
- 4) Reassure the victim that other evidence may still be identified and recovered even if they have bathed or made other physical changes.

B. Initial Officer Response

When responding to a scene involving a sexual assault, officers shall follow standard incident response procedures. In addition, when interacting with victims, officers shall do the following:

- 1) Recognize that the victim experienced a traumatic incident and may not be willing or able to immediately assist with the criminal investigation.

- 2) The officer shall attempt to determine the location/jurisdiction where the assault took place.
- 3) Explain the reporting process including the roles of the first responder, investigator, and anyone else with whom the victim will likely interact during the course of the investigation.
- 4) Officers are encouraged to connect the victim with local victim advocates as soon as possible. Inform the victim that there are confidential victim advocates available to address any needs they might have and to support them through the criminal justice system process. Provide the victim with contact information for the local victim advocate. Upon victim request the officer can offer to contact local victim advocate on behalf of the victim.
- 5) Ask about and document signs and symptoms of injury, to include strangulation. Officers shall attempt to obtain a signed medical release from the victim.
- 6) Ensure that the victim knows they can go to a designated facility for a forensic medical exam. Offer to arrange for transportation for the victim.
- 7) Identify and attempt to interview potential witnesses to the sexual assault and/or anyone the victim told about the sexual assault.
- 8) Request preferred contact information for the victim for follow-up.

C. Victim Interviews

This agency recognizes that victims of sexual assault due to their age or physical, mental or emotional distress, are better served by utilizing trauma informed interviewing techniques and strategies. Such interview techniques and strategies eliminate the duplication of interviews and use a question and answer interviewing format with questioning nondirective as possible to elicit spontaneous responses.

In recognizing the need for non-traditional interviewing techniques for sexual assault victims, officers should consider the following:

- Offer to have a confidential victim advocate present (if possible) if the victim would benefit from additional support during the process
- Whenever possible, conduct victim interviews in person
- Make an effort to conduct the interview in a welcoming environment
- Let the victim share the details at their own pace
- Recognize victims of trauma may have difficulty remembering incidents in a linear fashion and may remember details in days and weeks following the assault
- After the initial interview, consider reaching out to the victim within a few days, after at least one sleep cycle to ask if they remember any additional details.

- Depending on the victim, additional interviews might be needed to gather additional information. Offer support from a victim advocate to the victim to help facilitate engagement with the investigative process and healing.
- Some victims do remember details vividly and might want to be interviewed immediately.
- During initial and subsequent victim interviews, officers should note the following information as victims share it, recognizing that a victim may not be able to recall all the details of the assault during a particular interview.
 - 1) Whether the suspect was known to the victim
 - 2) How long the victim knew the suspect
 - 3) The circumstances of their meeting and if there is any indication of the use of drugs or alcohol to facilitate the sexual assault
 - 4) The extent of their previous or current relationship
 - 5) Any behavioral changes that led the situation from one based on consent to one of submission, coercion, fear, or force
 - 6) Specific actions, statements, and/or thoughts of both victim and suspect immediately prior, during, and after assault
 - 7) Relevant communication through social media, email, text messages, or any other forms of communication

D. Special Considerations—Minors and Vulnerable Adults/Domestic Abuse Victims

1. Minors and Vulnerable Adults

This agency recognizes that certain victims, due to their age or a physical, mental, or emotional distress, are better served by utilizing interview techniques and strategies that eliminate the duplication of interviews and use a question and answer interviewing format with questioning as nondirective as possible to elicit spontaneous responses. Members of this agency will be alert for victims who would be best served by the use of these specialized interview techniques. Officers, in making this determination, should consider the victim's age, level of maturity, communication skills, intellectual capacity, emotional state, and any other observable factors that would indicate specialized interview techniques would be appropriate for a particular victim. When an officer determines that a victim requires the use of these specialized interview techniques, the officer should follow the guidance below.

- a. Officers responding to reports of sexual assaults involving these sensitive population groups shall limit their actions to the following:
 - (1) Ensuring the safety of the victim;
 - (2) Ensuring the scene is safe;
 - (3) Safeguarding evidence where appropriate;
 - (4) Collecting any information necessary to identify the suspect; and
 - (5) Addressing the immediate medical needs of individuals at the scene

- b. Initial responding officers should not attempt to interview the victim in these situations, but should instead attempt to obtain basic information and facts about the situation, including the jurisdiction where the incident occurred and that a crime most likely occurred. Officers should seek to obtain this information from parents, caregivers, the reporting party, or other adult witnesses, unless those individuals are believed to be the perpetrators.
- c. Officers responding to victims with special considerations must comply with the mandated reporting requirements of Minnesota Statute Section 260E.06 and 626.557, as applicable. Officers investigating cases involving victims with special considerations should coordinate these investigations with the appropriate local human services agency where required. Any victim or witness interviews conducted with individuals having special considerations must be audio and video recorded whenever possible. All other interviews must be audio recorded whenever possible.

Not all sexual assaults of minor victims require a mandatory report to social services. This policy recognizes that in certain cases, notifying and/or the involvement of a parent/guardian can cause harm to the minor and/or impede the investigation. Officers responding to the sexual assault of a minor victim that does not trigger a mandated report under Minnesota Statute Section 260E.22 should assess for the impact on the victim and the investigation if parents/guardians were notified before making a decision to involve them.

- d. Officers should obtain necessary contact information for the victim's caregiver, guardian or parents and where the victim may be located at a later time. Officers should advise the victim and/or any accompanying adult(s), guardians or caregivers that an investigating officer will follow up with information on a forensic interview.
 - e. The officer should advise the victim's caregiver, guardian or parent that if the victim starts to talk about the incident they should listen to them but not question them as this may influence any future statements.
2. Victims of Domestic Abuse
- Officers responding to a report of sexual assault committed against a family and household member must also follow the requirements and guidelines in this agency's domestic abuse policy and protocol, in addition to the guidelines in this policy.

E. Protecting Victim Rights

- 1) Confidentiality: Officers should explain to victims the limitations of confidentiality in a criminal investigation and that the victim's identifying information is not accessible to the public, as specified in Minn. Stat. section 13.82, subd. 17(b)
- 2) Crime Victim Rights: Officers must provide the following information to the victim:
 - a. Crime victim rights and resource information required to be provided to all victims as specified by Minn. Stat. section 611A.02, subd. 2(b)
 - b. If the suspect is a family or household member to the victim, crime victim rights and resource information required to be provided to domestic abuse victims, as specified by Minn. Stat. section 629.341, subd. 3.
 - c. The victim's right to be informed of the status of a sexual assault examination kit upon request as provided for under Minn. Stat. section 611A.27, subd. 1.
 - d. Pursuant to Minn. Stat. 611A.26, subd. 1, no law enforcement agency or prosecutor shall require that a complainant of a criminal sexual conduct or sex trafficking offense submit to a polygraph examination as part of or a condition to proceeding with the investigation, charging or prosecution of such offense.
- 3) Other information: Officers should provide to the victim the agency's crime report/ICR number, and contact information for the reporting officer and/or investigator or person handling the follow up.
- 4) Language access: All officers shall follow agency policy regarding limited English proficiency.

F. Evidence Collection

- 1) Considerations for Evidence Collection

Officers shall follow this agency's policy on crime scene response. In addition, officers may do the following:

 - a. Collect evidence regarding the environment in which the assault took place, including indications of isolation and soundproofing. The agency should consider utilizing their agency or county crime lab in obtaining or processing the scene where the assault took place. This should be in accordance to any/all other policies and procedures relating to evidence collections.
 - b. Document any evidence of threats or any communications made by the suspect, or made on behalf of the suspect, to include those made to individuals other than the victim.

- c. In situations where it is suspected that drugs or alcohol may have facilitated the assault, officers should assess the scene for evidence such as drinking glasses, alcohol bottles or cans, or other related items.
- d. If the victim has declined or a medical forensic exam will not be conducted, the officer should obtain victim consent and attempt to take photographs of visible physical injuries, including any healing or old injuries. Victim should be given directions about how to document any bruising or injury that becomes evidence later after these photographs are taken.

G. Sexual Assault Medical Forensic Examinations

- 1) Prior to the sexual assault medical forensic examination the investigating officer should do the following:
 - a. Ensure the victim understands the purpose of the sexual assault medical forensic exam and its importance to both their general health and wellness and to the investigation. Offer assurance to the victim that they will not incur any out-of-pocket expenses for forensic medical exams and provide information about evidence collection, storage and preservation in sexual assault cases.
 - b. Provide the victim with general information about the procedure, and encourage them to seek further detail and guidance from the forensic examiner, health care professional, or a victim advocate. Officers and investigators cannot deny a victim the opportunity to have an exam.
 - c. Officers should be aware and if necessary, relay to victims who do not want to undergo an exam that there might be additional treatments or medications they are entitled to even if they do not want to have an exam done or have evidence collected. Victims can seek that information from a health care provider or a victim advocate. If possible, transport or arrange transportation for the victim to the designated medical facility.
 - d. Ask the victim for a signed release for access to medical records from the exam.
- 2) Officers should not be present during any part of the exam, including during the medical history.
- 3) Following the exam, evidence collected during the exam shall be handled according to the requirements of agency policy and Minnesota Statute 299C.106.

H. Contacting and Interviewing Suspects

Prior to contacting the suspect, officers should consider the following:

- 1) Conduct a background and criminal history check specifically looking for accusations, criminal charges, and convictions for interconnected crimes, especially crimes involving violence.

- 2) Consider conducting a pretext or confrontational call or messaging depending on jurisdictional statutes. Involvement of a victim should be based on strong consideration of the victim's emotional and physical state. A victim advocate should be present whenever possible to offer support.
- 3) When possible, an attempt would be made to interview the suspect in person.
- 4) In situations where suspects do not deny that a sexual act occurred, but rather assert that it was with the consent of the victim, officers should do the following:
 - a. Collect evidence of past communication, including but not limited to all relevant interaction (including social media) between the suspect and victim.
 - b. Identify events that transpired prior to, during, and after the assault in an effort to locate additional witnesses and physical locations that might lead to additional evidence.
- 5) For sexual assaults involving strangers, officers should focus investigative efforts on the collection of video, DNA, and other trace evidence used for analysis to identify the perpetrator (handle evidence collection per agency policy).

I. Forensic Examination and/or the Collection of Evidence from the Suspect

Note: A suspect's forensic examination and/or the collection of evidence from a suspect may be done by either an investigating officer/investigator, Forensic Medical Examiner, or the agency/county crime lab personnel.

- 1) Prior to or immediately after the preliminary suspect interview, photograph any injuries.
- 2) Determine whether a sexual assault medical forensic examination should be conducted.
- 3) Ask for the suspect's consent to collect evidence from their body and clothing. However, officers/investigators should consider obtaining a search warrant, with specific details about what evidence will be collected, and should be prepared in advance to eliminate the opportunity for the suspect to destroy or alter evidence if consent is denied.
- 4) During the suspect's sexual assault medical forensic examination, the investigator, evidence technician, or forensic examiner should do the following:
 - a. Strongly consider penile swabbing, pubic hair combings, and collection of other potential DNA evidence;
 - b. Collect biological and trace evidence from the suspect's body;
 - c. Document information about the suspect's clothing, appearance, scars, tattoos, piercings, and other identifiable marks;
 - d. Seize all clothing worn by the suspect during the assault, particularly any clothing touching the genital area;
 - e. Document the suspect's relevant medical condition and injuries.

J. Role of the Supervisor

Supervisors may do the following:

- 1) Assist officers investigating incidents of sexual assault when possible or if requested by an officer.
- 2) Provide guidance and direction as needed.
- 3) Review sexual assault reports to ensure that necessary steps were taken during initial response and investigations.

K. Case Review/Case Summary

A supervisor should ensure cases are reviewed on an on-going basis. The review process should include an analysis of:

- 1) Case dispositions
- 2) Decisions to collect evidence
- 3) Submissions of evidence for lab testing
- 4) Interviewing decisions

Confidential Informants Model Policy .pdf

CONFIDENTIAL INFORMANTS MODEL POLICY

MN STAT 626.8476

I. POLICY

It is the policy of the (**law enforcement agency**) to establish procedures and protocols that take necessary precautions concerning the recruitment, control and use of confidential informants.

II. DEFINITIONS

- A. Confidential Informant (CI):** A person who cooperates with a law enforcement agency confidentially in order to protect the person or the agency's intelligence gathering or investigative efforts and;
1. seeks to avoid arrest or prosecution for a crime, mitigate punishment for a crime in which a sentence will be or has been imposed, or receive a monetary or other benefit; and
 2. is able, by reason of the person's familiarity or close association with suspected criminals, to:
 - i. make a controlled buy or controlled sale of contraband, controlled substance, or other items that are material to a criminal investigation;
 - ii. supply regular or constant information about suspected or actual criminal activities to a law enforcement agency; or
 - iii. otherwise provide information important to ongoing criminal intelligence gathering or criminal investigative efforts.
- B. Controlled Buy:** means the purchase of contraband, controlled substances, or other items that are material to a criminal investigation from a target offender that is initiated, managed, overseen, or participated in by law enforcement personnel with the knowledge of a confidential informant.
- C. Controlled Sale:** means the sale of contraband, controlled substances, or other items that are material to a criminal investigation to a target offender that is initiated, managed, overseen, or participated in by law enforcement personnel with the knowledge of a confidential informant.
- D. Mental Harm:** means a psychological injury that is not necessarily permanent but results in visibly demonstrable manifestations of a disorder of thought or mood that impairs a person's judgment or behavior.
- E. Target Offender:** means the person suspected by law enforcement personnel to be implicated in criminal acts by the activities of a confidential informant.
- F. Confidential Informant File:** means a file maintained to document all information that pertains to a confidential informant.
- G. Unreliable Informant File:** means a file containing information pertaining to an individual who has failed at following an established written confidential informant agreement and has been determined to be generally unfit to serve as a confidential informant.
- H. Compelling Public Interest:** means, for purposes of this policy, situations in which failure to act would result or likely result in loss of life, serious injury, or have some serious negative consequence for persons, property, or public safety and therefore demand action.
- I. Overseeing agent:** means the officer primarily responsible for supervision and management of a confidential informant.

III. PROCEDURES

A. Initial Suitability Determination

An initial suitability determination must be conducted on any individual being considered for a role as a CI. The initial suitability determination includes the following:

1. An officer requesting use of an individual as a CI must complete an Initial Suitability Report. The report must be submitted to the appropriate individual or entity, as determined by the agency chief executive, to review for potential selection as a CI. The report must include sufficient detail regarding the risks and benefits of using the individual so that a sound determination can be made. The following information must be addressed in the report, where applicable:
 - a. Age, sex, and residence
 - b. Employment status or occupation
 - c. Affiliation with legitimate businesses and illegal or suspicious enterprises
 - d. Extent to which potential information, associations, or other assistance could benefit a present or future investigation
 - e. Relationship with the target of an investigation
 - f. Motivation in providing information or assistance
 - g. Risk of adversely affecting an existing or future investigation
 - h. Extent to which provided information can be corroborated
 - i. Prior record as a witness
 - j. Criminal history, to include whether he or she is the subject of a pending investigation, is under arrest, or has been charged with a crime
 - k. Risk to the public or as a flight risk
 - l. Consultation with the individual's probation, parole, or supervised release agent, if any
 - m. Consideration and documentation of the individual's diagnosis of mental illness, substance use disorder, traumatic brain injury, or disability; and consideration and documentation of the individual's history of mental illness, substance use disorder, traumatic brain injury or disability
 - n. Relationship to anyone in law enforcement
 - o. Risk of physical harm to the potential CI or their immediate family or relatives for cooperating with law enforcement
 - p. Prior or current service as a CI with this or another law enforcement organization
2. Prior to an individual's use as a CI, a supervisor or other designated authority must review the Initial Suitability Report and determine if the individual is authorized to serve as a CI.
3. Any prospective or current CI must be excluded from engaging in a controlled buy or sale of a controlled substance if the prospective or current CI:
 - a. is receiving in-patient treatment or partial-hospitalization treatment administered by a licensed service provider for a substance use disorder or mental illness; or
 - b. is participating in a treatment-based drug court program or treatment court; except that
 - c. the prospective or current CI may provide confidential information while receiving treatment, participating in a treatment-based drug court program or treatment court.

4. Documentation and special consideration must be made of the risks involved in engaging a prospective or current CI in the controlled buy or sale of a controlled substance if the individual is known, or has reported, to have experienced a drug overdose in the previous 12 months.
5. Any prospective or current CI who is known to abuse substances, or is at risk for abusing substances, should be provided referral to prevention or treatment services.
6. Any prospective or current CI that has a physical or mental illness that impairs the ability of the individual to understand instructions and make informed decisions should be referred to a mental health professional or other appropriate medical professional, or a case manager/social worker from the county social services agency, or other substance abuse and mental health services.
7. Each CI's suitability must be reviewed every 6 months, at a minimum, during which time the CI's overseeing agent must submit a Continuing Suitability Report addressing the foregoing issues in III.A.1.a-p, and III.A.3-6, where applicable. An initial suitability determination must be conducted on a reactivated CI regardless of the length of inactivity.
8. Any information that may negatively affect a CI's suitability during the course of their use must be documented in the CI's file and forwarded to the appropriate authorized personnel as soon as possible.
9. Supervisors must review informant files regularly with the overseeing agent and must attend debriefings of CIs periodically as part of the informant management process. If a CI is active for more than 12 months, a supervisory meeting with the CI must be conducted without the overseeing agent.
10. CI contracts must be terminated, and the CI file placed in inactive status when the CI has not been utilized for 6 months or more.

B. Exigent Confidential Informants

1. Certain circumstance arise when an individual who has been arrested is willing to immediately cooperate and perform investigative activities under the direction of an overseeing agent. In these circumstances, the initial suitability determination can be deferred and an individual may be utilized as a CI for a period not to exceed 12 hours from the time of arrest if:
 - a. The individual is not excluded from utilization as a CI under III.A(3)(a-c) of this policy; and
 - b. There is compelling public interest or exigent circumstances exist that demand immediate utilization of the individual as a CI and any delay would significantly and negatively affect any investigation; and
 - c. A supervisor has reviewed and approved the individual for utilization as a CI under these circumstances.
2. Upon the conclusion of the 12-hour window, or at any time before, an initial suitability determination must be conducted before the individual engages in any further CI activities.

C. Special CI Approval Requirements

Certain individuals who are being considered for use as a CI require special review and approval. In all instances, the agency's chief executive or their designee and the office of the prosecutor or county attorney should be consulted prior to the use of these individuals as CIs. These individuals include the following:

1. Juveniles
 - a. Use of a juvenile under the age of 18 for participating in a controlled buy or sale of a controlled substance or contraband may be undertaken only with the written authorization of the individual's parent(s) or guardian(s), except that the juvenile informant may provide confidential information.

- b. Authorization for such use should be granted only when a compelling public interest can be demonstrated, *except that*
 - c. Juveniles under the guardianship of the State may not be used as a CI.
- 2. Individuals obligated by legal privilege of confidentiality.
- 3. Government officials.

D. General Guidelines for Overseeing CIs

General guidelines for overseeing CIs are as follows:

- 1. CIs must be treated as assets of the agency, not the individual overseeing agent.
- 2. No promises or guarantees of preferential treatment within the criminal justice system will be made to any informant without prior approval from the prosecuting authority.
- 3. CIs must not be used without authorization of the agency through procedures identified in this policy.
- 4. CIs must not be used to gather information purely of a political nature or for other information-gathering efforts that are not connected with a criminal investigation.
- 5. Under no circumstances must an informant be allowed access to restricted areas or investigators' work areas within a law enforcement agency.
- 6. All CIs must sign and abide by the provisions of the agency's CI agreement.
- 7. Any physical or mental illness that impairs the CI's ability to knowingly contract or otherwise protect the informant's self-interest must be taken into consideration before the CI signs the agreement.
- 8. The CI's overseeing agent must discuss each of the provisions of the agreement with the CI, with particular emphasis on the following:
 - a. CIs may voluntarily initiate deactivation, whereupon the protocols outlined in section E of this policy must be followed.
 - b. CIs are not law enforcement officers. They have no arrest powers, are not permitted to conduct searches and seizures, and may not carry a weapon while performing activities as a CI.
 - c. CIs found engaging in any illegal activity beyond what is authorized by the agency and conducted while under the supervision of an overseeing agent, will be subject to prosecution.
 - d. CIs are prohibited from engaging in actions or activities that could be deemed entrapment. The meaning of the term and implications of such actions must be explained to each CI.
 - e. CIs are prohibited from engaging in self-initiated information or intelligence gathering without agency direction and approval. The CI must not take any actions in furtherance of an investigation without receiving specific instruction(s) from the overseeing agent or agency.
 - f. Every reasonable effort will be taken to ensure the confidentiality of the CI but, upon judicial order, he or she may be required to testify in open court.
 - g. CIs may be directed to wear a listening and recording device.
 - h. CIs must be required to submit to a search before and after a controlled purchase.

- i. CIs who participate in unplanned or unanticipated activities or meet with a subject(s) under investigation in a location outside of the jurisdictional boundary of the handling agency must promptly report that activity or meeting to their overseeing agents.
9. CI activity outside jurisdictional boundaries:
 - a. Investigators handling CIs who engage in operational activity in locations outside the jurisdictional boundaries of the agency must coordinate with counterparts in law enforcement agencies that have jurisdiction in that location where the CI will operate before any activity occurs, or in a timely manner after unanticipated activity occurs and is brought to the attention of the overseeing agent.
 - b. Any decision to defer or delay notice to or coordinate with an outside agency having jurisdiction in the area where a CI has or may operate must be documented, reviewed, and approved by the agency's chief executive or their designee.
10. Officers must take the utmost care to avoid conveying any confidential investigative information to a CI, such as the identity of other CIs, surveillance activities, or search warrants, other than what is necessary and appropriate for operational purposes.
11. No member of this agency must knowingly maintain a social relationship with a CI, or otherwise become personally involved with a CI beyond actions required in the performance of duty.
12. Members of this agency must not solicit, accept gratuities from, or engage in any private business transaction with a CI.
13. Meetings with a CI must be conducted in private with another officer or agent present and with at least one officer or agent of the same sex, except when not practical. The meeting location should minimize the potential for discovery of the informant's cooperation and provide sufficient space to complete necessary administrative duties. The meetings must be documented and subsequently entered into the individual's CI file.
14. Overseeing agents must develop and follow a communications strategy and plan with the CI that minimizes, to the greatest extent possible, the risk of discovery or compromise of the relationship between the agency and the CI. This plan should also aim to prevent the detection, compromise, or interception of communications between the overseeing agent and the CI.
15. Procedures must be instituted to assist CIs with concealing their identity and maintaining their safety. Care should be given not to expose CIs to unnecessary safety risks.
16. Preceding or following every buy or sale of controlled substances, overseeing agents must screen the CI for any personal safety or mental health concerns, risk of substance abuse, and/or potential relapse in any substance abuse recovery.
 - a. At the request of the CI, or if the overseeing agent deems it necessary, reasonable efforts should be taken to provide the CI with referral to substance abuse and/or mental health services.
 - b. Overseeing agents must document:
 - i. the screening,
 - ii. any referral to services provided to, or requested by, the CI, and
 - iii. any refusal by the CI to participate in the screening and/or any refusal by the CI to accept referral to services. Reasons for the CI's refusal must be documented, where applicable.
 - c. No part of this subsection supersedes MN Stat. 253B.05, sub.2.

17. Reasonable protective measures must be provided for a CI when any member of this agency knows or should have known of a risk or threat of harm to a person serving as a CI and the risk or threat of harm is a result of the informant's service to this agency.
18. Overseeing agents must:
 - a. evaluate and document the criminal history and propensity for violence of target offenders; and
 - b. to the extent allowed, provide this information to the CI if there is a reasonable risk or threat of harm to the CI as a result of the CI's interaction with the target offender.
19. Reasonable efforts and precautions must be made to help protect the identity of a CI during the time the person is acting as an informant.
20. Whenever possible, officers must corroborate information provided by a CI and document efforts to do so.
21. The name of a CI must not be included in an affidavit for a warrant unless judicial authority is obtained to seal the document from the public record or the CI is a subject of the investigation upon which the affidavit is based.
22. Overseeing agents are responsible for ensuring that information of potential value to other elements of the agency is provided promptly to authorized supervisory personnel and/or other law enforcement agencies as appropriate.
23. Individuals leaving employment with the agency have a continuing obligation to maintain as confidential the identity of any CI and the information he or she provided unless obligated to reveal such identity or information by law or court order.

E. Establishment of an Informant File System

An informant file system must be established as follows:

1. The agency chief executive must designate a file supervisor who must be responsible for developing and maintaining master CI files and an indexing system.
2. A file must be maintained on each CI deemed suitable by the agency.
3. An additional Unreliable Informant File must be established for CIs deemed unsuitable during initial suitability determinations or at a later time.
4. Each file must be coded with an assigned informant control number for identification within the indexing system and must include the following information, where applicable:
 - a. Name, aliases, and date of birth
 - b. Height, weight, hair color, eye color, race, sex, scars, tattoos, or other distinguishing features
 - c. Emergency contact information
 - d. Name of the officer initiating use of the informant and any subsequent overseeing agents
 - e. Photograph and criminal history record
 - f. Current home address and telephone number(s)
 - g. Residential addresses in the last five years
 - h. Current employer, position, address, and telephone number
 - i. Social media accounts
 - j. Marital status and number of children

- k. Vehicles owned and their registration numbers
 - l. Places frequented
 - m. Gang affiliations or other organizational affiliations
 - n. Briefs of information provided by the CI and the CI's subsequent reliability
 - o. Special skills and hobbies
 - p. Special areas of criminal expertise or knowledge
 - q. A copy of the signed informant agreement
5. CI files must be maintained in a separate and secured area.
 6. The file supervisor must ensure that information concerning CIs is strictly controlled and distributed only to officers and other authorities who have a need and a right to such information.
 7. CI File Review
 - a. Sworn personnel may review an individual's CI file only upon the approval of the agency's chief executive or their designee.
 - b. The requesting officer must submit a written request explaining the need for review. A copy of this request, with the officer's name, must be maintained in the individual's CI file.
 - c. Officers must not remove, copy, or disseminate information from the CI file.
 - d. CI files must be reviewed only in designated areas of the law enforcement facility and returned as soon as possible to their secure file location.
 - e. All disclosures or access to CI files must be recorded by the file supervisor, to include information such as the requesting officer or agency, the purpose of access or disclosure, the information conveyed, and the date and time of access or dissemination.
 - f. No portion of an individual's CI file must be entered into any other electronic or related database without controls sufficient to exclude access to all but authorized personnel with a need and a right to know.

F. Deactivation of Confidential Informants

A CI deactivation procedure must be established as follows:

1. The overseeing agent must complete a deactivation form that includes, at minimum, the following:
 - a. The name of the agency.
 - b. The name of the CI.
 - c. The control number of the CI, where applicable.
 - d. The date of deactivation.
 - e. The reason for deactivation.
 - f. A notification that contractual agreements regarding monetary re-numeration, criminal justice assistance, or other considerations, specified or not, are terminated.
 - g. A notification that the agency will provide and assist the CI with referral to health services for assistance with any substance abuse disorder and/or physical, mental, or emotional health concerns, as requested or accepted by the CI.
 - h. A signature by the CI or documentation indicating the reason(s) why the CI was unable or unwilling to sign the form.

- i. A signature by the overseeing agent.
2. All reasonable efforts must be taken to maintain the safety and anonymity of the CI after deactivation.

G. Monetary Payments

Monetary payments must be managed as follows:

1. All monetary compensation paid to CIs must be commensurate with the value of the information or assistance provided to the agency.
2. All CI payments must be approved in advance by the officer in charge of confidential funds.
3. Officers must provide accounting of monies received and documentation for confidential funds expended. Any documentation of monies paid or received should not contain the true identity of the informant but should use the CI's control number.
4. Two officers must be present when making payments or providing funds to CIs.
5. The appropriate individual, as designated by the agency's chief executive, must ensure that the process for authorization, disbursement, and documentation of CI payments, as well as the accounting and reconciliation of confidential funds, is consistent with agency policy.
6. If a CI is authorized to work with another law enforcement or prosecutorial agency, financial payments must be coordinated between the agencies in a manner that is proportionate to the assistance rendered to each agency and consistent with provision III.F.1. of this policy.
7. Written records of receipts are retained, or justification for the exception is documented when a written receipt is not available.

Model Sexual Assault Investigation Policy.pdf

I. PURPOSE

The purpose of this policy is to provide employees with guidelines for responding to reports of sexual assault. This agency will strive:

- a) To afford maximum protection and support to victims of sexual assault or abuse through a coordinated program of law enforcement and available victim services with an emphasis on a victim centered approach;
- b) To reaffirm peace officers' authority and responsibility to conducting thorough preliminary and follow up investigations and to make arrest decisions in accordance with established probable cause standards;
- c) To increase the opportunity for prosecution and victim services.

II. POLICY

It is the policy of the _____ (law enforcement agency) to recognize sexual assault as a serious problem in society and to protect victims of sexual assault by ensuring its peace officers understand the laws governing this area. Sexual assault crimes are under-reported to law enforcement and the goal of this policy is in part to improve victim experience in reporting so that more people are encouraged to report.

All employees should take a professional, victim-centered approach to sexual assaults, protectively investigate these crimes, and coordinate with prosecution in a manner that helps restore the victim's dignity and autonomy. While doing so, it shall be this agency's goal to decrease the victim's distress, increase the victim's understanding of the criminal justice system and process, and promote public safety.

Peace officers will utilize this policy in response to sexual assault reported to this agency. This agency will aggressively enforce the laws without bias and prejudice based on race, marital status, sexual orientation, economic status, age, disability, gender, religion, creed, or national origin.

III. DEFINITIONS

For purpose of this policy, the words and phrases in this section have the following meaning given to them, unless another intention clearly appears.

A. **Consent:** As defined by Minn. Stat. 609.341, which states:

- (1) Words or overt actions by a person indicating a freely given present agreement to perform a particular sexual act with the actor. Consent does not mean the existence of a prior or current social relationship between the actor and the complainant or that the complainant failed to resist a particular sexual act.
- (2) A person who is mentally incapacitated or physically helpless as defined by Minnesota Statute 609.341 cannot consent to a sexual act.

- (3) Corroboration of the victim's testimony is not required to show lack of consent.
- B. **Child or Minor:** a person under the age of 18.
- C. **Medical Forensic Examiner:** The health care provider conducting a sexual assault medical forensic examination.
- D. **Sexual Assault:** A person who engages in sexual contact or penetration with another person in a criminal manner as identified in MN Statute 609.342 to 609.3451.
- E. **Family and Household Member:** As defined in Minn. Stat. 518.B.01 Subd.2.b. to include:
- (1) spouses or former spouses;
 - (2) parents and children;
 - (3) persons related by blood;
 - (4) persons who are presently residing together or who have resided together in the past;
 - (5) persons who have a child in common regardless of whether they have been married or have lived together at any time;
 - (6) a man and woman if the woman is pregnant and the man is alleged to be the father, regardless of whether they have been married or have lived together at any time; and
 - (7) persons involved in a significant romantic or sexual relationship
- F. **Sexual Assault Medical Forensic Examination:** An examination of a sexual assault patient by a health care provider, ideally one who has specialized education and clinical experience in the collection of forensic evidence and treatment of these patients.
- G. **Victim Advocate:** A Sexual Assault Counselor defined by Minn. Stat. 595.02, subd. 1(k) and/or Domestic Abuse Advocate as defined by Minn. Stat. 595.02, subd. 1(1) who provide confidential advocacy services to victims of sexual assault and domestic abuse. Victim advocates as defined provide coverage in all counties in Minnesota. Minnesota Office of Justice Programs (MN OJP) can assist departments in locating their local victim advocacy agency for the purposes outlined in this policy.
- H. **Victim Centered:** A victim-centered approach prioritizes the safety, privacy and well-being of the victim and aims to create a supportive environment in which the victim's rights are respected and in which they are treated with dignity and respect. This approach acknowledges and respects a victims' input into the criminal justice response and recognizes victims are not responsible for the crimes committed against them.
- I. **Vulnerable Adult:** any person 18 years of age or older who:
- (1) is a resident inpatient of a facility as defined in Minn. Stat. 626.5572. Subd. 6;

- (2) receives services at or from a facility required to be licensed to serve adults under sections [245A.01](#) to [245A.15](#), except that a person receiving outpatient services for treatment of chemical dependency or mental illness, or one who is committed as a sexual psychopathic personality or as a sexually dangerous person under chapter 253B, is not considered a vulnerable adult unless the person meets the requirements of clause (4);
- (3) receives services from a home care provider required to be licensed under sections [144A.43](#) to [144A.482](#); or from a person or organization that exclusively offers, provides, or arranges for personal care assistance services under the medical assistance program as authorized under sections [256B.0625, subdivision 19a](#), [256B.0651](#) to [256B.0654](#), and [256B.0659](#); or
- (4) regardless of residence or whether any type of service is received, possesses a physical or mental infirmity or other physical, mental, or emotional dysfunction:
 - (i) that impairs the individual's ability to provide adequately for the individual's own care without assistance, including the provision of food, shelter, clothing, health care, or supervision; and
 - (ii) because of the dysfunction or infirmity and the need for assistance, the individual has an impaired ability to protect the individual from maltreatment.

IV. PROCEDURES

A. Communications Personnel Response/Additional Actions by Responding Officers

Communications personnel and/or law enforcement officers should inform the victim of ways to ensure critical evidence is not lost, to include the following:

- 1) Suggest that the victim not bathe, or clean him or herself if the assault took place recently.
- 2) Recommend that if a victim needs to relieve themselves, they should collect urine in a clean jar for testing, and should avoid wiping after urination.
- 3) Asking the victim to collect any clothing worn during or after the assault and if possible, place in a paper bag, instructing the victim not to wash the clothing (per department policy).
- 4) Reassure the victim that other evidence may still be identified and recovered even if they have bathed or made other physical changes.

B. Initial Officer Response

When responding to a scene involving a sexual assault, officers shall follow standard incident response procedures. In addition, when interacting with victims, officers shall do the following:

- 1) Recognize that the victim experienced a traumatic incident and may not be willing or able to immediately assist with the criminal investigation.

- 2) The officer shall attempt to determine the location/jurisdiction where the assault took place.
- 3) Explain the reporting process including the roles of the first responder, investigator, and anyone else with whom the victim will likely interact during the course of the investigation.
- 4) Officers are encouraged to connect the victim with local victim advocates as soon as possible. Inform the victim that there are confidential victim advocates available to address any needs they might have and to support them through the criminal justice system process. Provide the victim with contact information for the local victim advocate. Upon victim request the officer can offer to contact local victim advocate on behalf of the victim.
- 5) Ask about and document signs and symptoms of injury, to include strangulation. Officers shall attempt to obtain a signed medical release from the victim.
- 6) Ensure that the victim knows they can go to a designated facility for a forensic medical exam. Offer to arrange for transportation for the victim.
- 7) Identify and attempt to interview potential witnesses to the sexual assault and/or anyone the victim told about the sexual assault.
- 8) Request preferred contact information for the victim for follow-up.

C. Victim Interviews

This agency recognizes that victims of sexual assault due to their age or physical, mental or emotional distress, are better served by utilizing trauma informed interviewing techniques and strategies. Such interview techniques and strategies eliminate the duplication of interviews and use a question and answer interviewing format with questioning nondirective as possible to elicit spontaneous responses.

In recognizing the need for non-traditional interviewing techniques for sexual assault victims, officers should consider the following:

- Offer to have a confidential victim advocate present (if possible) if the victim would benefit from additional support during the process
- Whenever possible, conduct victim interviews in person
- Make an effort to conduct the interview in a welcoming environment
- Let the victim share the details at their own pace
- Recognize victims of trauma may have difficulty remembering incidents in a linear fashion and may remember details in days and weeks following the assault
- After the initial interview, consider reaching out to the victim within a few days, after at least one sleep cycle to ask if they remember any additional details.

- Depending on the victim, additional interviews might be needed to gather additional information. Offer support from a victim advocate to the victim to help facilitate engagement with the investigative process and healing.
- Some victims do remember details vividly and might want to be interviewed immediately.
- During initial and subsequent victim interviews, officers should note the following information as victims share it, recognizing that a victim may not be able to recall all the details of the assault during a particular interview.
 - 1) Whether the suspect was known to the victim
 - 2) How long the victim knew the suspect
 - 3) The circumstances of their meeting and if there is any indication of the use of drugs or alcohol to facilitate the sexual assault
 - 4) The extent of their previous or current relationship
 - 5) Any behavioral changes that led the situation from one based on consent to one of submission, coercion, fear, or force
 - 6) Specific actions, statements, and/or thoughts of both victim and suspect immediately prior, during, and after assault
 - 7) Relevant communication through social media, email, text messages, or any other forms of communication

D. Special Considerations—Minors and Vulnerable Adults/Domestic Abuse Victims

1. Minors and Vulnerable Adults

This agency recognizes that certain victims, due to their age or a physical, mental, or emotional distress, are better served by utilizing interview techniques and strategies that eliminate the duplication of interviews and use a question and answer interviewing format with questioning as nondirective as possible to elicit spontaneous responses. Members of this agency will be alert for victims who would be best served by the use of these specialized interview techniques. Officers, in making this determination, should consider the victim's age, level of maturity, communication skills, intellectual capacity, emotional state, and any other observable factors that would indicate specialized interview techniques would be appropriate for a particular victim. When an officer determines that a victim requires the use of these specialized interview techniques, the officer should follow the guidance below.

- a. Officers responding to reports of sexual assaults involving these sensitive population groups shall limit their actions to the following:
 - (1) Ensuring the safety of the victim;
 - (2) Ensuring the scene is safe;
 - (3) Safeguarding evidence where appropriate;
 - (4) Collecting any information necessary to identify the suspect; and
 - (5) Addressing the immediate medical needs of individuals at the scene

- b. Initial responding officers should not attempt to interview the victim in these situations, but should instead attempt to obtain basic information and facts about the situation, including the jurisdiction where the incident occurred and that a crime most likely occurred. Officers should seek to obtain this information from parents, caregivers, the reporting party, or other adult witnesses, unless those individuals are believed to be the perpetrators.
- c. Officers responding to victims with special considerations must comply with the mandated reporting requirements of Minnesota Statute 626.556 and 626.557, as applicable. Officers investigating cases involving victims with special considerations should coordinate these investigations with the appropriate local human services agency where required. Any victim or witness interviews conducted with individuals having special considerations must be audio and video recorded whenever possible. All other interviews must be audio recorded whenever possible.

Not all sexual assaults of minor victims require a mandatory report to social services. This policy recognizes that in certain cases, notifying and/or the involvement of a parent/guardian can cause harm to the minor and/or impede the investigation. Officers responding to the sexual assault of a minor victim that does not trigger a mandated report under Minn. Stat. 626.556 should assess for the impact on the victim and the investigation if parents/guardians were notified before making a decision to involve them.

- d. Officers should obtain necessary contact information for the victim's caregiver, guardian or parents and where the victim may be located at a later time. Officers should advise the victim and/or any accompanying adult(s), guardians or caregivers that an investigating officer will follow up with information on a forensic interview.
 - e. The officer should advise the victim's caregiver, guardian or parent that if the victim starts to talk about the incident they should listen to them but not question them as this may influence any future statements.
2. Victims of Domestic Abuse
- Officers responding to a report of sexual assault committed against a family and household member must also follow the requirements and guidelines in this agency's domestic abuse policy and protocol, in addition to the guidelines in this policy.

E. Protecting Victim Rights

- 1) Confidentiality: Officers should explain to victims the limitations of confidentiality in a criminal investigation and that the victim's identifying information is not accessible to the public, as specified in Minn. Stat. section 13.82, subd. 17(b)
- 2) Crime Victim Rights: Officers must provide the following information to the victim:
 - a. Crime victim rights and resource information required to be provided to all victims as specified by Minn. Stat. section 611A.02, subd. 2(b)
 - b. If the suspect is a family or household member to the victim, crime victim rights and resource information required to be provided to domestic abuse victims, as specified by Minn. Stat. section 629.341, subd. 3.
 - c. The victim's right to be informed of the status of a sexual assault examination kit upon request as provided for under Minn. Stat. section 611A.27, subd. 1.
 - d. Pursuant to Minn. Stat. 611A.26, subd. 1, no law enforcement agency or prosecutor shall require that a complainant of a criminal sexual conduct or sex trafficking offense submit to a polygraph examination as part of or a condition to proceeding with the investigation, charging or prosecution of such offense.
- 3) Other information: Officers should provide to the victim the agency's crime report/ICR number, and contact information for the reporting officer and/or investigator or person handling the follow up.
- 4) Language access: All officers shall follow agency policy regarding limited English proficiency.

F. Evidence Collection

- 1) Considerations for Evidence Collection
Officers shall follow this agency's policy on crime scene response. In addition, officers may do the following:
 - a. Collect evidence regarding the environment in which the assault took place, including indications of isolation and soundproofing. The agency should consider utilizing their agency or county crime lab in obtaining or processing the scene where the assault took place. This should be in accordance to any/all other policies and procedures relating to evidence collections.
 - b. Document any evidence of threats or any communications made by the suspect, or made on behalf of the suspect, to include those made to individuals other than the victim.

- c. In situations where it is suspected that drugs or alcohol may have facilitated the assault, officers should assess the scene for evidence such as drinking glasses, alcohol bottles or cans, or other related items.
- d. If the victim has declined or a medical forensic exam will not be conducted, the officer should obtain victim consent and attempt to take photographs of visible physical injuries, including any healing or old injuries. Victim should be given directions about how to document any bruising or injury that becomes evidence later after these photographs are taken.

G. Sexual Assault Medical Forensic Examinations

- 1) Prior to the sexual assault medical forensic examination the investigating officer should do the following:
 - a. Ensure the victim understands the purpose of the sexual assault medical forensic exam and its importance to both their general health and wellness and to the investigation. Offer assurance to the victim that they will not incur any out-of-pocket expenses for forensic medical exams and provide information about evidence collection, storage and preservation in sexual assault cases.
 - b. Provide the victim with general information about the procedure, and encourage them to seek further detail and guidance from the forensic examiner, health care professional, or a victim advocate. Officers and investigators cannot deny a victim the opportunity to have an exam.
 - c. Officers should be aware and if necessary, relay to victims who do not want to undergo an exam that there might be additional treatments or medications they are entitled to even if they do not want to have an exam done or have evidence collected. Victims can seek that information from a health care provider or a victim advocate. If possible, transport or arrange transportation for the victim to the designated medical facility.
 - d. Ask the victim for a signed release for access to medical records from the exam.
- 2) Officers should not be present during any part of the exam, including during the medical history.
- 3) Following the exam, evidence collected during the exam shall be handled according to the requirements of agency policy and Minnesota Statute 299C.106.

H. Contacting and Interviewing Suspects

Prior to contacting the suspect, officers should consider the following:

- 1) Conduct a background and criminal history check specifically looking for accusations, criminal charges, and convictions for interconnected crimes, especially crimes involving violence.
- 2) Consider conducting a pretext or confrontational call or messaging depending on jurisdictional statutes. Involvement of a victim should be based on strong

consideration of the victim's emotional and physical state. A victim advocate should be present whenever possible to offer support.

- 3) When possible, an attempt would be made to interview the suspect in person.
- 4) In situations where suspects do not deny that a sexual act occurred, but rather assert that it was with the consent of the victim, officers should do the following:
 - a. Collect evidence of past communication, including but not limited to all relevant interaction (including social media) between the suspect and victim.
 - b. Identify events that transpired prior to, during, and after the assault in an effort to locate additional witnesses and physical locations that might lead to additional evidence.
- 5) For sexual assaults involving strangers, officers should focus investigative efforts on the collection of video, DNA, and other trace evidence used for analysis to identify the perpetrator (handle evidence collection per agency policy).

I. Forensic Examination and/or the Collection of Evidence from the Suspect

Note: A suspect's forensic examination and/or the collection of evidence from a suspect may be done by either an investigating officer/investigator, Forensic Medical Examiner, or the agency/county crime lab personnel.

- 1) Prior to or immediately after the preliminary suspect interview, photograph any injuries.
- 2) Determine whether a sexual assault medical forensic examination should be conducted.
- 3) Ask for the suspect's consent to collect evidence from their body and clothing. However, officers/investigators should consider obtaining a search warrant, with specific details about what evidence will be collected, and should be prepared in advance to eliminate the opportunity for the suspect to destroy or alter evidence if consent is denied.
- 4) During the suspect's sexual assault medical forensic examination, the investigator, evidence technician, or forensic examiner should do the following:
 - a. Strongly consider penile swabbing, pubic hair combings, and collection of other potential DNA evidence;
 - b. Collect biological and trace evidence from the suspect's body;
 - c. Document information about the suspect's clothing, appearance, scars, tattoos, piercings, and other identifiable marks;
 - d. Seize all clothing worn by the suspect during the assault, particularly any clothing touching the genital area;
 - e. Document the suspect's relevant medical condition and injuries.

J. Role of the Supervisor

Supervisors may do the following:

- 1) Assist officers investigating incidents of sexual assault when possible or if requested by an officer.
- 2) Provide guidance and direction as needed.
- 3) Review sexual assault reports to ensure that necessary steps were taken during initial response and investigations.

K. Case Review/Case Summary

A supervisor should ensure cases are reviewed on an on-going basis. The review process should include an analysis of:

- 1) Case dispositions
- 2) Decisions to collect evidence
- 3) Submissions of evidence for lab testing
- 4) Interviewing decisions

7 CJIS Security Policy_v5-7_20180816.pdf



Criminal Justice Information Services (CJIS) Security Policy

Version 5.7

08/16/2018

CJISD-ITS-DOC-08140-5.7



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council

SUMMARY OF CHANGES

Version 5.7

APB Approved Changes

1. Section 5.10.1.5 Cloud Computing: add language concerning data storage in cloud environments, Fall 2017, APB#17, SA#2, *CJIS Security Policy Restriction for Criminal Justice Information Stored in Offshore Cloud Computing Facilities*.
2. Section 5.10.1.5 Cloud Computing: add language concerning authorized uses of metadata, Spring 2017, APB#16, SA#10, *Collection and Use of Metadata by Cloud Service Providers*.
3. Section 5.12.1.2 Personnel Screening for Contractors and Vendors: add language allowing CSO delegation of duties, Spring 2017, APB#16, SA#7, *CJIS Systems Officer Delegation Authorization of Personnel Screening Requirements for Contractors and Vendors*.
4. Section 5.12.1 Personnel Security Policy and Procedures: rename section to “Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI” and combine previous Sections 5.12.1.1 and 5.12.1.2 into the single section, Fall 2017, APB#17, SA#1, *CJIS Security Policy Language Changes in Section 5.12*.
5. Appendix A Terms and Definitions: add definition of “Metadata”, Spring 2017, APB#16, SA#10, *Collection and Use of Metadata by Cloud Service Providers*.
6. Appendix B Acronyms: add “RCMP”, “Royal Canadian Mounted Police”, Fall 2017, APB#17, SA#2, *CJIS Security Policy Restriction for Criminal Justice Information Stored in Offshore Cloud Computing Facilities*.
7. Appendix J Noncriminal Justice Agency Supplemental Guidance: add language to clarify which personnel the requirements apply to and remove language referencing deleted language, Fall 2017, APB#17, SA#1, *CJIS Security Policy Language Changes in Section 5.12*.

Administrative Changes¹

1. Section 1.4, add bullet concerning “References/Citations/Directives.”
2. Section 4.1, change “FNU” to “UCN.”
3. Section 5.1.1.2, remove reference to DOJ Order 0904.
4. Section 5.1.1.6, remove reference to DOJ Order 0904.
5. Section 5.1.5, remove this section and all other like sections in each policy area (5.2.3, 5.3.5, 5.4.8, 5.5.7, 5.6.5, 5.7.3, 5.8.5, 5.9.3, 5.10.5, 5.11.5, 5.12.5).
6. Section 5.4.1.1, add clarifying language to #4.
7. Section 5.5.2.4, change cross-reference in bullet #3
8. Section 5.5.4, change bullet for consistency throughout policy.
9. Section 5.6.2.1.2, change bullet(s) for consistency throughout policy.
10. Section 5.6.2.1.3, change bullet(s) for consistency throughout policy.
11. Section 5.6.2.2.1, change bullet(s) for consistency throughout policy.
12. Section 5.10.1.2.1, change bullet(s) for consistency throughout policy.

¹ Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

13. Section 5.10.1.2.2, change bullet(s) for consistency throughout policy.
14. Section 5.10.1.2.3, change bullet(s) for consistency throughout policy.
15. Section 5.13.2, change bullet(s) for consistency throughout policy.
16. Appendix A, change “FNU” to “UCN” in definition of Criminal Justice Information.
17. Appendix A, move “W” definitions to correct location alphabetically.
18. Appendix B, add acronym “UCN.”
19. Appendix F, update contact information on form.
20. Appendix G.2, change word “securities” to “security.”
21. Appendix I, remove reference for DOJ Order 0904.
22. Appendix J, remove reference to DOJ Order 0904.

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB11, SA6, Future CSP for Mobile Devices”):

Fall 2013 – Advisory Policy Board cycle and year

APB## – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Topic Title

TABLE OF CONTENTS

Executive Summary	i
Change Management.....	ii
Summary of Changes.....	iii
Table of Contents	v
List of Figures.....	x
1 Introduction.....	1
1.1 Purpose.....	1
1.2 Scope.....	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document.....	2
1.5 Distribution of the CJIS Security Policy.....	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement	3
2.2 Architecture Independent.....	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy.....	4
3.2 Roles and Responsibilities for Agencies and Parties.....	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO).....	5
3.2.3 Terminal Agency Coordinator (TAC).....	6
3.2.4 Criminal Justice Agency (CJA).....	6
3.2.5 Noncriminal Justice Agency (NCJA).....	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC).....	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer.....	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI).....	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information.....	11
4.2.1 Proper Access, Use, and Dissemination of CHRI.....	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information.....	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information.....	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage.....	12
4.2.5 Justification and Penalties	12

4.2.5.1	Justification	12
4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
Policy Area 1:	Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services.....	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Awareness Topics	20
5.2.1.1	Level One Security Awareness Training	20
5.2.1.2	Level Two Security Awareness Training	20
5.2.1.3	Level Three Security Awareness Training	20
5.2.1.4	Level Four Security Awareness Training	21
5.2.2	Security Training Records.....	22
5.3	Policy Area 3: Incident Response	23
5.3.1	Reporting Security Events.....	23
5.3.1.1	Reporting Structure and Responsibilities.....	23
5.3.1.1.1	FBI CJIS Division Responsibilities	23
5.3.1.1.2	CSA ISO Responsibilities.....	23
5.3.2	Management of Security Incidents.....	24
5.3.2.1	Incident Handling.....	24
5.3.2.2	Collection of Evidence.....	24
5.3.3	Incident Response Training.....	24
5.3.4	Incident Monitoring.....	24
5.4	Policy Area 4: Auditing and Accountability.....	26
5.4.1	Auditable Events and Content (Information Systems).....	26
5.4.1.1	Events.....	26
5.4.1.1.1	Content.....	27
5.4.2	Response to Audit Processing Failures	27
5.4.3	Audit Monitoring, Analysis, and Reporting.....	27
5.4.4	Time Stamps.....	27
5.4.5	Protection of Audit Information	27
5.4.6	Audit Record Retention.....	27
5.4.7	Logging NCIC and III Transactions.....	28
5.5	Policy Area 5: Access Control.....	29

5.5.1	Account Management	29
5.5.2	Access Enforcement.....	29
5.5.2.1	Least Privilege	30
5.5.2.2	System Access Control	30
5.5.2.3	Access Control Criteria.....	30
5.5.2.4	Access Control Mechanisms.....	30
5.5.3	Unsuccessful Login Attempts	31
5.5.4	System Use Notification.....	31
5.5.5	Session Lock	31
5.5.6	Remote Access	32
5.5.6.1	Personally Owned Information Systems.....	32
5.5.6.2	Publicly Accessible Computers	32
5.6	Policy Area 6: Identification and Authentication	34
5.6.1	Identification Policy and Procedures.....	34
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	34
5.6.2	Authentication Policy and Procedures	34
5.6.2.1	Standard Authenticators.....	35
5.6.2.1.1	Password	35
5.6.2.1.2	Personal Identification Number (PIN).....	35
5.6.2.1.3	One-time Passwords (OTP)	36
5.6.2.2	Advanced Authentication.....	36
5.6.2.2.1	Advanced Authentication Policy and Rationale	36
5.6.2.2.2	Advanced Authentication Decision Tree	37
5.6.3	Identifier and Authenticator Management	39
5.6.3.1	Identifier Management.....	39
5.6.3.2	Authenticator Management.....	39
5.6.4	Assertions	39
5.7	Policy Area 7: Configuration Management	45
5.7.1	Access Restrictions for Changes	45
5.7.1.1	Least Functionality.....	45
5.7.1.2	Network Diagram.....	45
5.7.2	Security of Configuration Documentation	45
5.8	Policy Area 8: Media Protection.....	47
5.8.1	Media Storage and Access	47
5.8.2	Media Transport	47
5.8.2.1	Digital Media during Transport	47
5.8.2.2	Physical Media in Transit	47
5.8.3	Digital Media Sanitization and Disposal.....	47
5.8.4	Disposal of Physical Media.....	47
5.9	Policy Area 9: Physical Protection	49
5.9.1	Physically Secure Location	49
5.9.1.1	Security Perimeter.....	49
5.9.1.2	Physical Access Authorizations.....	49
5.9.1.3	Physical Access Control	49
5.9.1.4	Access Control for Transmission Medium	49

5.9.1.5	Access Control for Display Medium	49
5.9.1.6	Monitoring Physical Access	50
5.9.1.7	Visitor Control	50
5.9.1.8	Delivery and Removal	50
5.9.2	Controlled Area	50
5.10	Policy Area 10: System and Communications Protection and Information Integrity	51
5.10.1	Information Flow Enforcement	51
5.10.1.1	Boundary Protection	51
5.10.1.2	Encryption.....	52
5.10.1.2.1	Encryption for CJI in Transit	52
5.10.1.2.2	Encryption for CJI at Rest.....	53
5.10.1.2.3	Public Key Infrastructure (PKI) Technology.....	53
5.10.1.3	Intrusion Detection Tools and Techniques	53
5.10.1.4	Voice over Internet Protocol.....	54
5.10.1.5	Cloud Computing.....	54
5.10.2	Facsimile Transmission of CJI	55
5.10.3	Partitioning and Virtualization	55
5.10.3.1	Partitioning.....	55
5.10.3.2	Virtualization	55
5.10.4	System and Information Integrity Policy and Procedures.....	56
5.10.4.1	Patch Management.....	56
5.10.4.2	Malicious Code Protection.....	57
5.10.4.3	Spam and Spyware Protection	57
5.10.4.4	Security Alerts and Advisories	57
5.10.4.5	Information Input Restrictions.....	57
5.11	Policy Area 11: Formal Audits	59
5.11.1	Audits by the FBI CJIS Division.....	59
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	59
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	59
5.11.2	Audits by the CSA.....	59
5.11.3	Special Security Inquiries and Audits	60
5.11.4	Compliance Subcommittees	60
5.12	Policy Area 12: Personnel Security	61
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	61
5.12.2	Personnel Termination	62
5.12.3	Personnel Transfer.....	62
5.12.4	Personnel Sanctions.....	62
5.13	Policy Area 13: Mobile Devices	64
5.13.1	Wireless Communications Technologies	64
5.13.1.1	802.11 Wireless Protocols	64
5.13.1.2	Cellular Devices.....	65
5.13.1.2.1	Cellular Service Abroad.....	66
5.13.1.2.2	Voice Transmissions Over Cellular Devices	66
5.13.1.3	Bluetooth.....	66
5.13.1.4	Mobile Hotspots.....	66

5.13.2	Mobile Device Management (MDM)	67
5.13.3	Wireless Device Risk Mitigations	67
5.13.4	System Integrity	68
5.13.4.1	Patching/Updates	68
5.13.4.2	Malicious Code Protection	68
5.13.4.3	Personal Firewall	68
5.13.5	Incident Response	69
5.13.6	Access Control	69
5.13.7	Identification and Authentication	69
5.13.7.1	Local Device Authentication	69
5.13.7.2	Advanced Authentication	69
5.13.7.2.1	Compensating Controls	70
5.13.7.3	Device Certificates	70
Appendices		A-1
Appendix A Terms and Definitions		A-1
Appendix B Acronyms		B-1
Appendix C Network Topology Diagrams		C-1
Appendix D Sample Information Exchange Agreements		D-1
D.1	CJIS User Agreement	D-1
D.2	Management Control Agreement	D-9
D.3	Noncriminal Justice Agency Agreement & Memorandum of Understanding	D-10
D.4	Interagency Connection Agreement	D-16
Appendix E Security Forums and Organizational Entities		E-1
Appendix F Sample Forms		F-1
F.1	Security Incident Response Form	F-2
Appendix G Best practices		G-1
G.1	Virtualization	G-1
G.2	Voice over Internet Protocol	G-4
G.3	Cloud Computing	G-15
G.4	Mobile Appendix	G-32
G.5	Administrator Accounts for Least Privilege and Separation of Duties	G-53
G.6	Encryption	G-66
Appendix H Security Addendum		H-1
Appendix I References		I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance		J-1
Appendix K Criminal Justice Agency Supplemental Guidance		K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Use Cases	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	25
Figure 6 – Local Police Department's Use of Audit Logs	28
Figure 7 – A Local Police Department's Access Controls	33
Figure 8 – Advanced Authentication Use Cases.....	40
Figure 9 – Authentication Decision for Known Location	43
Figure 10 – Authentication Decision for Unknown Location	44
Figure 11 – A Local Police Department's Configuration Management Controls	46
Figure 12 – A Local Police Department's Media Management Policies.....	48
Figure 13 – A Local Police Department's Physical Protection Measures.....	50
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	58
Figure 15 – The Audit of a Local Police Department.....	60
Figure 16 – A Local Police Department's Personnel Security Controls	62

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- **References/Citations/Directives:** Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

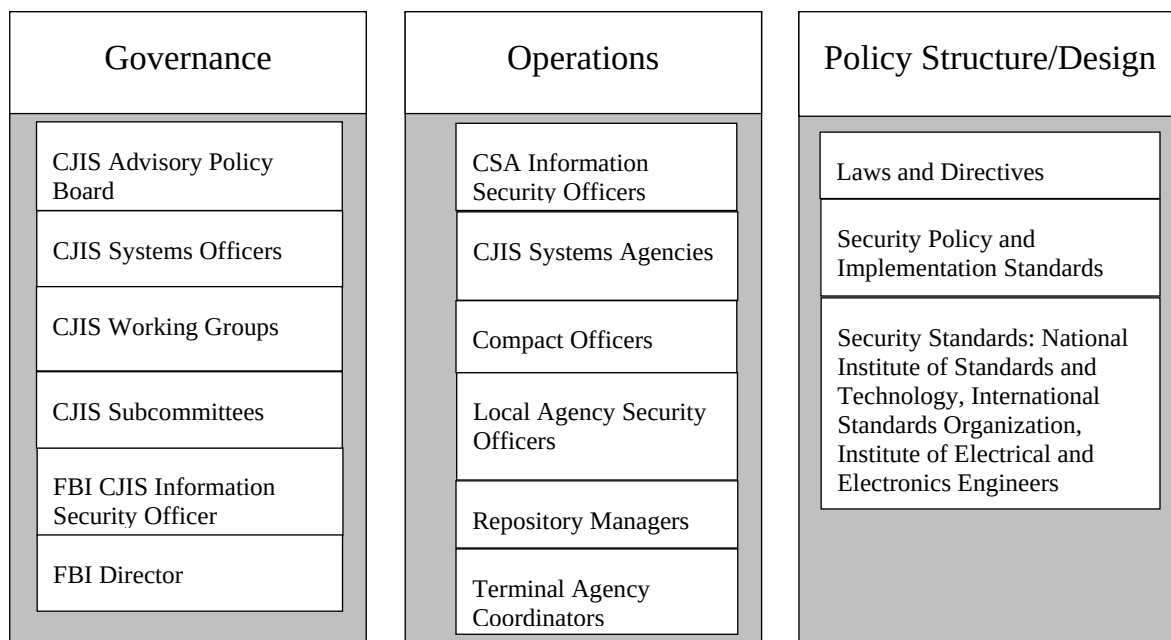


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
- d. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
- e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
- f. Approve access to FBI CJIS systems.
- g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
- h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.

3. Outsourcing of Criminal Justice Functions

- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
- b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to – employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

5.2.1 Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.

2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors’ view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.
3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
 - a. access the audit log file;

- b. modify the audit log file;
- c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJIS.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department’s Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
 - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g.

password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. **EXAMPLES:**

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Can request's physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2.

- a. The IP address is attributed to a physical structure; or
- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is "no". Skip to question number 4.

2. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

3. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement waived.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or

- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

4. Does request originate from an agency-controlled user device?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 5.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 3.

- a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or
- b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7.

6. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 7.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

7. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA requirement is waived.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual’s identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport

layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password (“something you know”), and a one-time password OTP (“something you have”) from a hardware token to satisfy the requirement for advanced authentication. Once the detective’s credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user’s identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user's profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. Using this collected data, the RBA presents challenge/response questions when changes to the user's profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user's job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

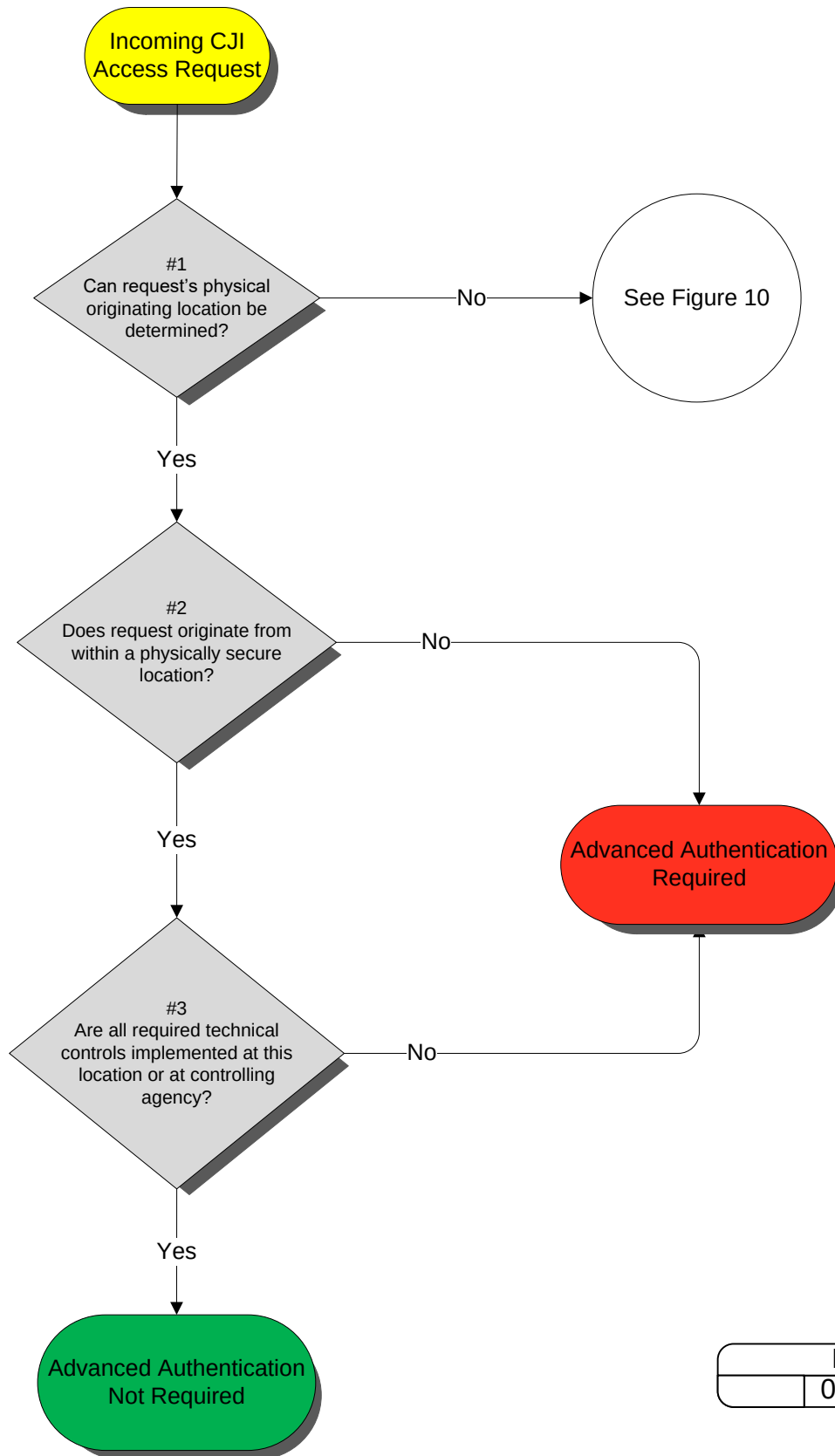


Figure 9		
08/04/2014		

Figure 10 – Authentication Decision for Unknown Location

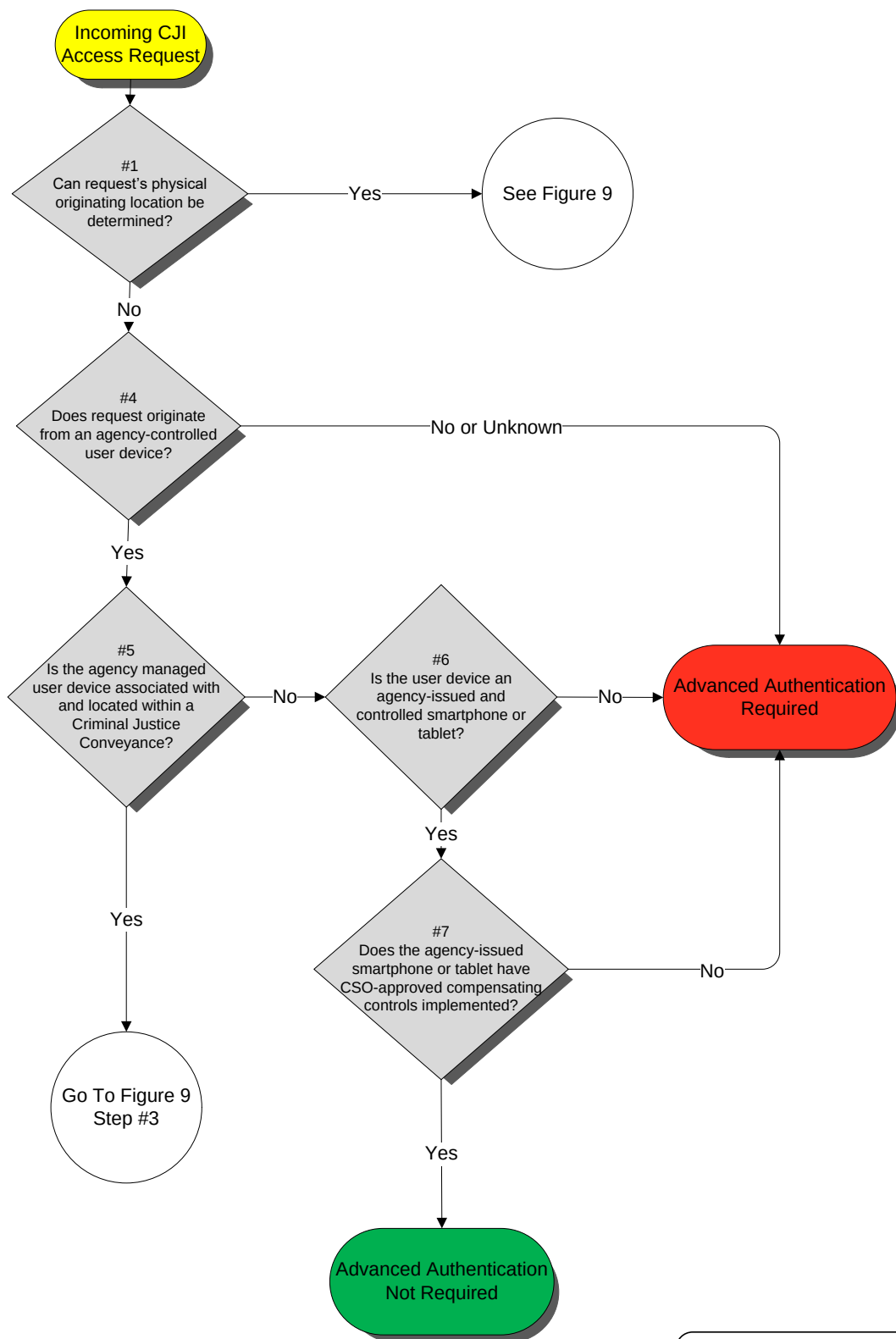


Figure 10

10/06/2015

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
 - a. The agency owns, operates, manages, or protects the medium.
 - b. Medium terminates within physically secure locations at both ends with no interconnections between.
 - c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
 - d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
 - e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA)
 - If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
 - a. Be at least 10 characters
 - b. Not be a dictionary word.
 - c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
 - d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.

2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.
5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department’s Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state’s CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
 - a. 5 CFR 731.106; and/or
 - b. Office of Personnel Management policy, regulations, and guidance; and/or
 - c. agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
 - a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
 - b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
 - c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated

policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular Devices

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
 - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. Agencies shall implement the following controls when allowing CJI access from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the:
 - a. Remote locking of device
 - b. Remote wiping of device
 - c. Setting and locking device configuration
 - d. Detection of “rooted” and “jailbroken” devices
 - e. Enforcement of folder or disk level encryption
 - f. Application of mandatory policy settings on the device
 - g. Detection of unauthorized configurations
 - h. Detection of unauthorized software or applications
 - i. Ability to determine the location of agency controlled devices
 - j. Prevention of unpatched devices from accessing CJI or CJI systems
 - k. Automatic device wiping after a specified number of failed access attempts

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.
2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.

5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.13.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
 - a. Device known to be locked, minimal duration of loss
 - b. Device lock state unknown, minimal duration of loss
 - c. Device lock state unknown, extended duration of loss
 - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Access Control

Multiple user accounts are not generally supported on limited feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.13.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited feature mobile operating systems, achieving compliance may require many different components.

5.13.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user.

5.13.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The proposed compensating controls for AA are a combination of controls that provide acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

At least two of the following examples of AA compensating controls for agency-issued smartphones and tablets with limited feature operating systems shall be implemented to qualify for compensating control consideration:

- Possession of the agency issued smartphone or tablet as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates as per Section 5.13.7.3 Device Certificates

5.13.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate – Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider – An organization that provides cloud computing services.

Cloud Subscriber – A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information

security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

In-Band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices — Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited feature operating system (e.g. tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary

purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system

administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone – See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices – Tablet devices are mobile devices with a limited feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

User Certificate (user-based) – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) – See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (WiFi) Hotspot – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
NCIC	National Crime Information Center

NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier

TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJI, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

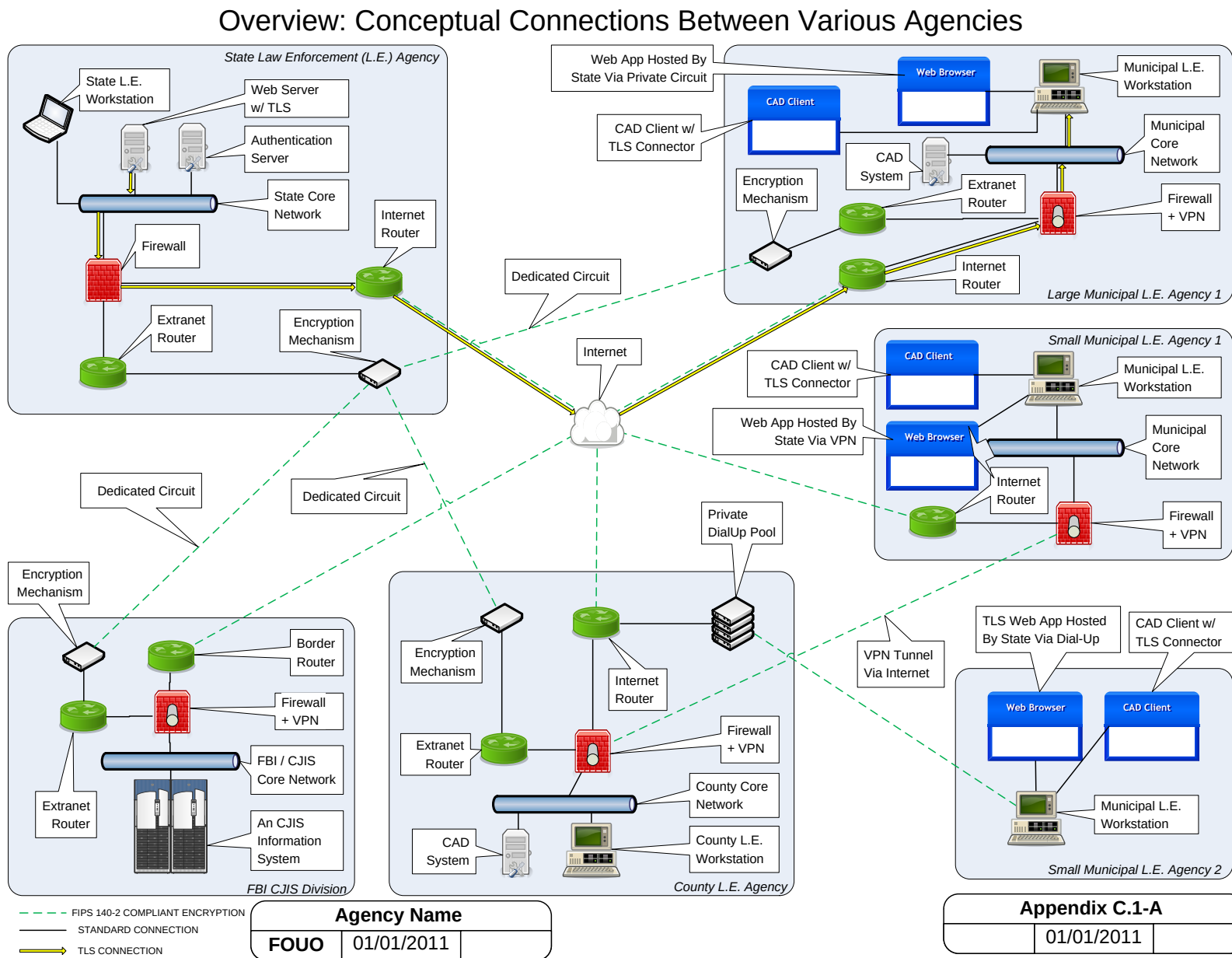
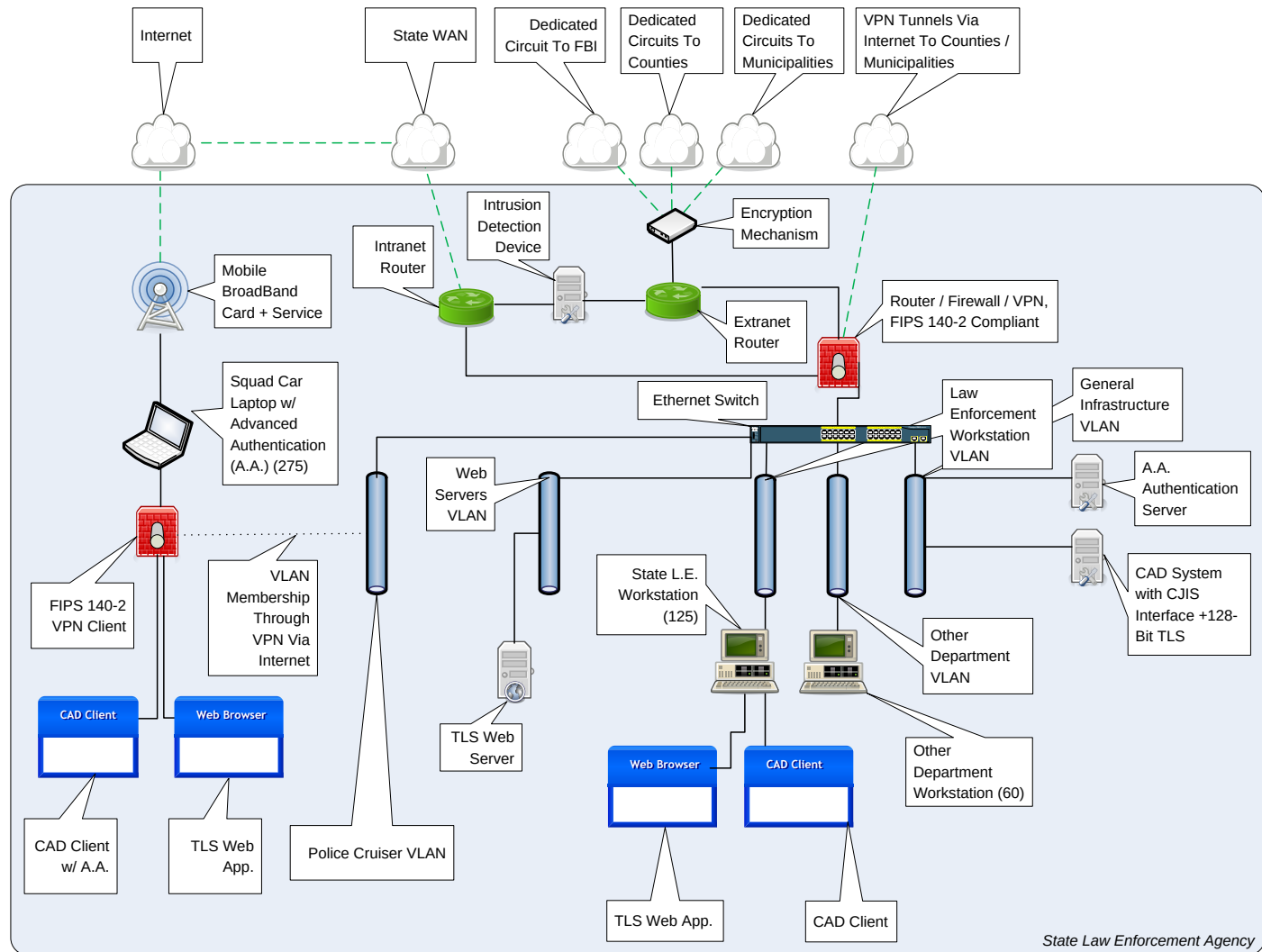


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

Conceptual Topology Diagram For A State Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample State Agency

FOUO

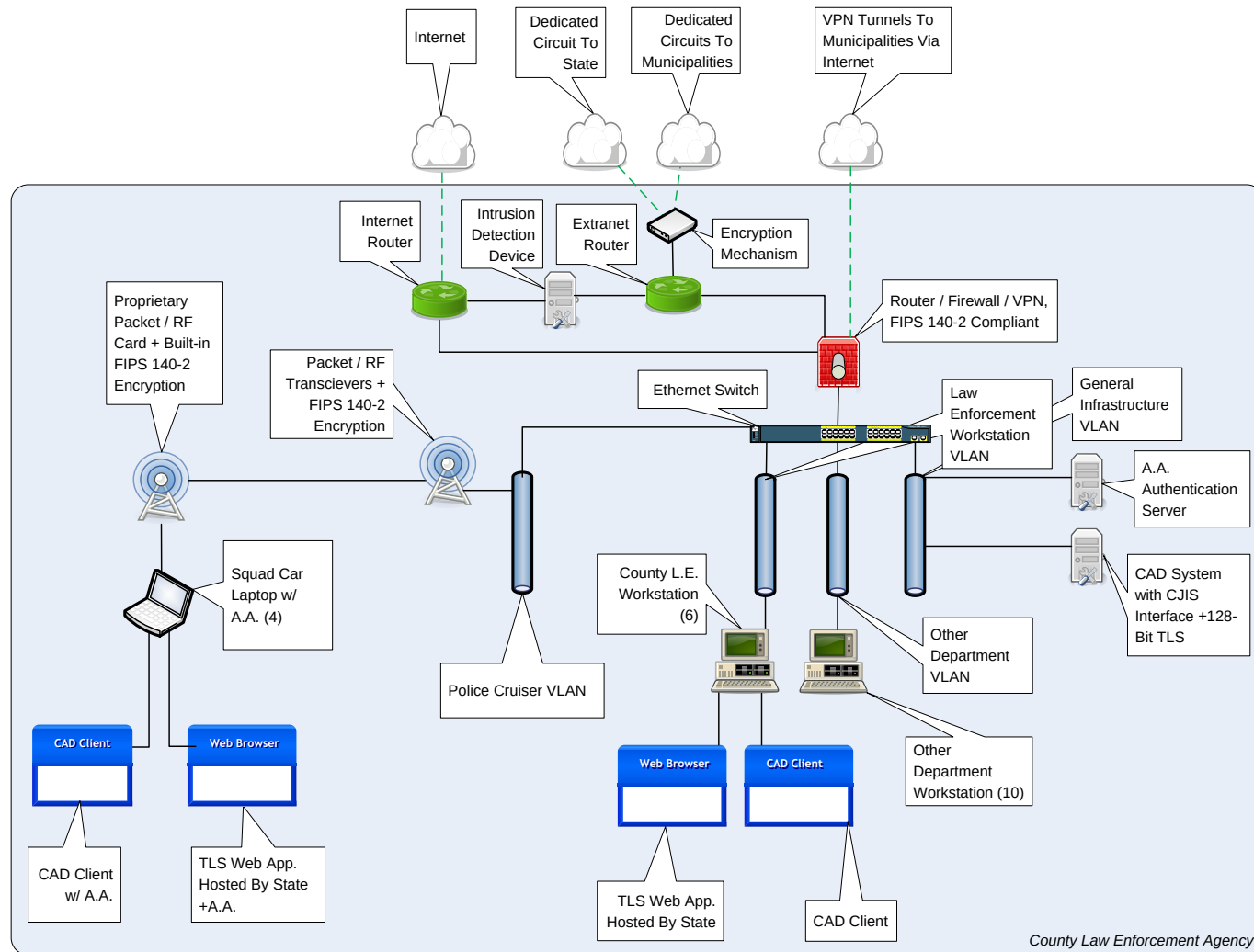
01/01/2011

Appendix C.1-B

01/01/2011

08/16/2018
CJISD-ITS-DOC-08140-5.7

Conceptual Topology Diagram For A County Law Enforcement Agency



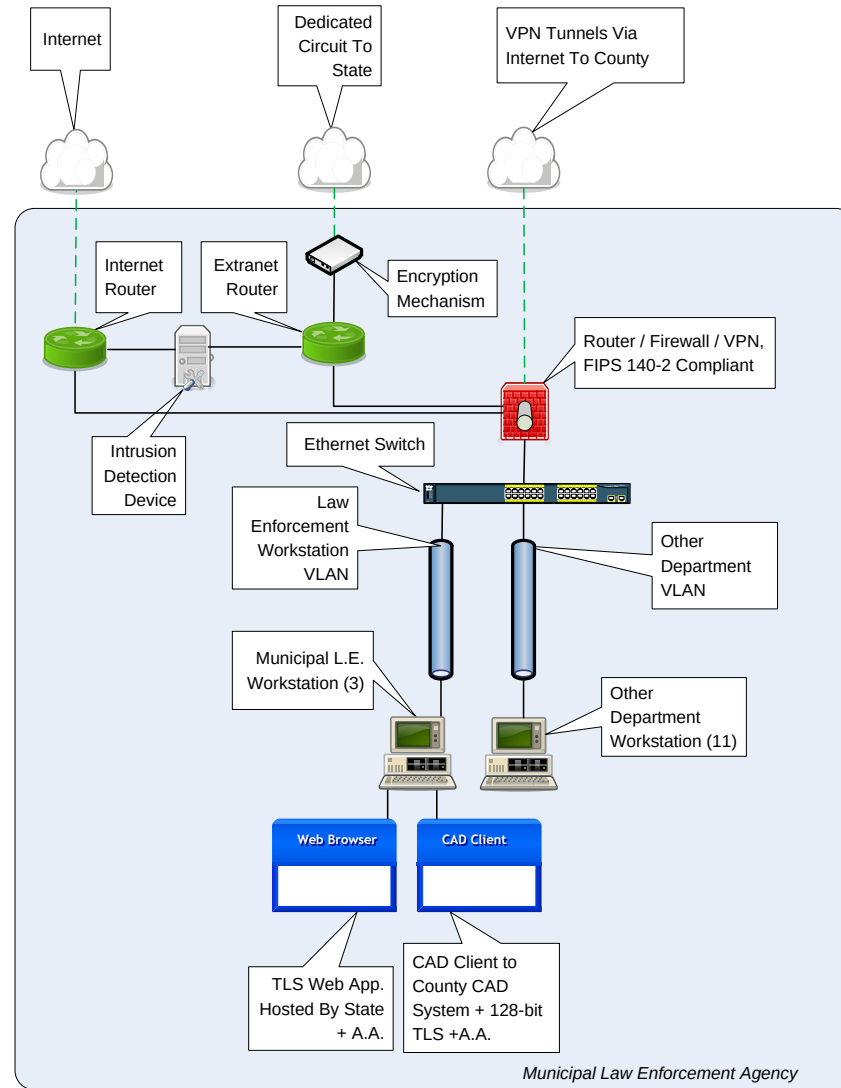
--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Sample County Agency		
FOUO	01/01/2011	

Appendix C.1-C		
	01/01/2011	

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 — STANDARD CONNECTION

Sample Municipal Agency		
FOUO	01/01/2011	

Appendix C.1-D		
	01/01/2011	

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
 - b. Each party will pay the costs it incurs as a result of termination.
 - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

CJIS Systems Officer

Date: _____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

CSA Head

Date: _____

Printed Name/Title

PART 2

CJIS WAN Official (or other CJIS Authorized Official)

Date: _____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

CJIS WAN Agency Head

Date: _____

Printed Name/Title

FBI CJIS DIVISION:

Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. SCOPE:

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. **FUNDING:** There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. **SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

[Name]

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Wide Area Network (WAN) USER AGREEMENT

BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability*; and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*

Signature

Print or Type

CJIS WAN Agency Official

Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*

Signature

Print or Type

*

Title

Date

State CSO

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director

Title

Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) ²
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

**FBI CJIS DIVISION
INFORMATION SECURITY OFFICER (ISO)
SECURITY INCIDENT REPORTING FORM**

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

SYSTEM(S) AFFECTED: _____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

John C. Weatherly

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

iso@fbi.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
- *"Type-2 Hypervisor which requires a separate application to run within an operating system*

“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”

“Sun Microsystems today announced the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”

“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious

information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer

and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
 - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

- a. Scenario 1–Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

- b. Scenario 2–Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3—CJI Impact from a Cloud Datacenter Critical Systems Crash—Core Dump² Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

² Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

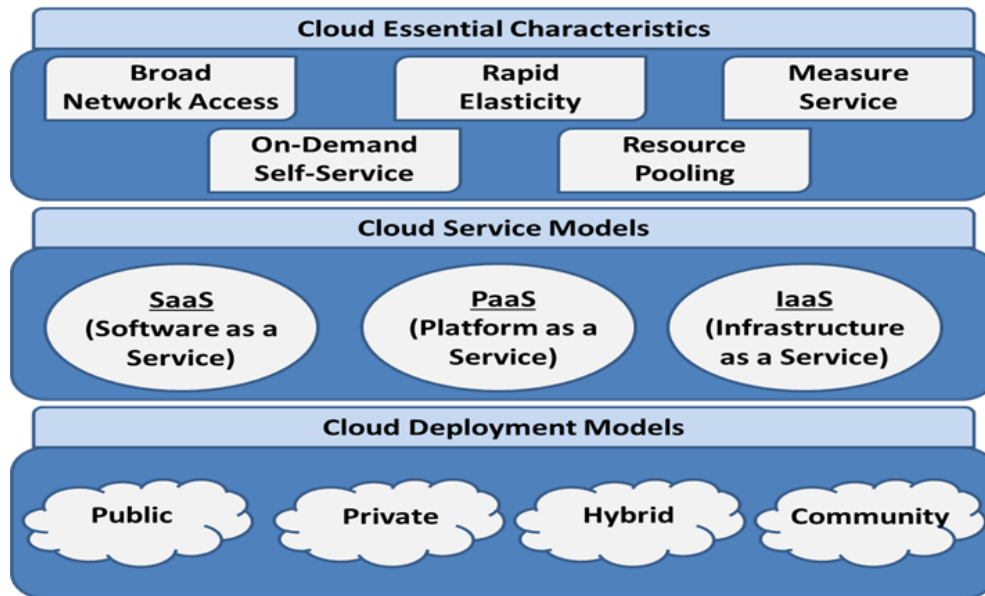


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction

(e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost

benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

	• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full featured computers running a traditional full featured operating system but without an attached keyboard. The main defining factor is the use of a full featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. ‘always on cellular’ vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes ‘on demand’ cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be

able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes ‘on-demand’ cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or ‘connected’ to the cellular network. They connect to the network or internet through WiFi ‘hotspots’ or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over ‘public’ WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with ‘on-demand’ cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking (‘bricking’) or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full featured laptops but may not be available for limited feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most ‘smartphones’. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and required a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to ‘unlock’ the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the ‘internal’ storage of the device, the Android OS does not provide secure separation of data stores on ‘external’ storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific ‘external’ media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via ‘always-on’ cellular data connections and the devices built-in GPS. Device tracking with WiFi only or ‘on-demand’ cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating system as long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of

the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS

The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES

The organization:

(a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION

The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)

**SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS)
CONSIDERATION FOR LEAST PRIVILEGE:**

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12---1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	Quick win (<u>One of the “First Five”</u>)
CSC 12---2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	Quick win
CSC 12---3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	Quick win

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	<i>Quick win</i>
CSC 12---5	Ensure that all service accounts have long and difficult--- to---guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	<i>Quick win</i>
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12---9	Configure operating systems so that passwords cannot be re---used within a timeframe of six months.	<i>Quick win</i>
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>

CSC 12---12	Use multifactor authentication for all administrative access, including domain administrative access. Multi--- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>
CSC 12---13 (NEW)	When using certificates to enable multi---factor certificate---based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12---14	Block access to a machine (either remotely or locally) for administrator---level accounts. Instead, administrators should be required to access a system using a fully logged and non---administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption. Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

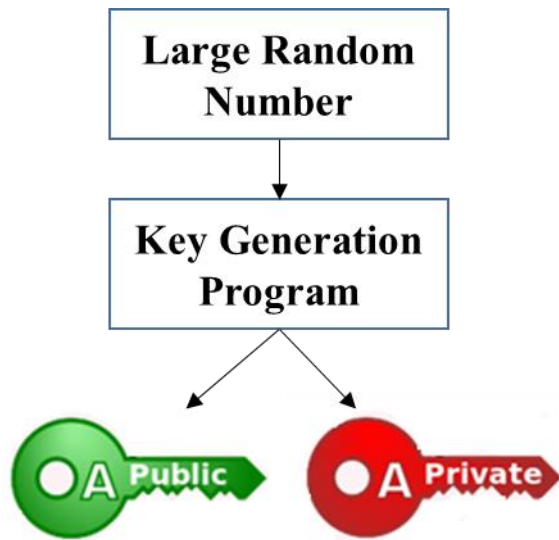


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

<u>Symmetric</u>		<u>Asymmetric</u>		
<u>Bits of security</u>	<u>Symmetric key algorithms</u>	<u>Finite-Field Cryptography (FFC)</u> <u>(e.g., DSA, D-H)</u> <u>Bits of security</u>	<u>Integer-Factorization Cryptography (IFC)</u> <u>(e.g., RSA)</u> <u>Bits of security</u>	<u>Elliptic-Curve Cryptography (ECC)</u> <u>(e.g., ECDSA)</u> <u>Bits of security</u>
<u>80</u>	<u>2TDEA18</u>	<u>Public key = 1024</u> <u>Private key = 160</u>	<u>Key size = 1024</u>	<u>Key size = 160-223</u>
<u>112</u>	<u>3TDEA</u>	<u>Public key = 2048</u> <u>Private key = 224</u>	<u>Key size = 2048</u>	<u>Key size = 224-255</u>
<u>128</u>	<u>AES-128</u>	<u>Public Key = 3072</u> <u>Private key = 256</u>	<u>Key size = 3072</u>	<u>Key size = 256-383</u>
<u>192</u>	<u>AES-192</u>	<u>Public key = 7680</u> <u>Private key = 384</u>	<u>Key size = 7680</u>	<u>Key size = 384-511</u>
<u>256</u>	<u>AES-256</u>	<u>Public key = 15360</u> <u>Private key = 512</u>	<u>Key size = 15360</u>	<u>Key size = 512+</u>

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <NO>
- Module has been pre-validated and is on the CMVP pre-validation list. <NO>
- The module will be submitted for testing. <NO>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
- The module meets all the requirements of FIPS 140-2. <NO>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
- The module follows the guidelines detailed in FIPS 140-2. <NO>
- The module has been validated and has received Certificate #XXXX. <YES>

A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link:
<http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf>

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website:
<http://csrc.nist.gov/cryptval/140-2.htm>

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44
- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code,
Title 44 - Public Printing and Documents; Chapter 35 - Coordination of
Federal Information Policy; Subchapter I - Federal Information Policy, Section
3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI) it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

- (i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative

to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Electronic media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record

information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies”.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

- (iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Digital media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency’s virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring access to CJI - listed in CSP Section 5.12.1.1. In addition to the requirements listed in CSP Section 5.12.1.1 contractors and vendors must undergo additional screening requirements as listed in CSP Section 5.12.1.2.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above “General CJI Guidance” section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

Model Sexual Assault Investigation Policy 03-03-21.pdf

I. PURPOSE

The purpose of this policy is to provide employees with guidelines for responding to reports of sexual assault. This agency will strive:

- a) To afford maximum protection and support to victims of sexual assault or abuse through a coordinated program of law enforcement and available victim services with an emphasis on a victim centered approach;
- b) To reaffirm peace officers' authority and responsibility to conducting thorough preliminary and follow up investigations and to make arrest decisions in accordance with established probable cause standards;
- c) To increase the opportunity for prosecution and victim services.

II. POLICY

It is the policy of the _____ (law enforcement agency) to recognize sexual assault as a serious problem in society and to protect victims of sexual assault by ensuring its peace officers understand the laws governing this area. Sexual assault crimes are under-reported to law enforcement and the goal of this policy is in part to improve victim experience in reporting so that more people are encouraged to report.

All employees should take a professional, victim-centered approach to sexual assaults, protectively investigate these crimes, and coordinate with prosecution in a manner that helps restore the victim's dignity and autonomy. While doing so, it shall be this agency's goal to decrease the victim's distress, increase the victim's understanding of the criminal justice system and process, and promote public safety.

Peace officers will utilize this policy in response to sexual assault reported to this agency. This agency will aggressively enforce the laws without bias and prejudice based on race, marital status, sexual orientation, economic status, age, disability, gender, religion, creed, or national origin.

III. DEFINITIONS

For purpose of this policy, the words and phrases in this section have the following meaning given to them, unless another intention clearly appears.

A. **Consent:** As defined by Minn. Stat. 609.341, which states:

- (1) Words or overt actions by a person indicating a freely given present agreement to perform a particular sexual act with the actor. Consent does not mean the existence of a prior or current social relationship between the actor and the complainant or that the complainant failed to resist a particular sexual act.
- (2) A person who is mentally incapacitated or physically helpless as defined by Minnesota Statute 609.341 cannot consent to a sexual act.

- (3) Corroboration of the victim's testimony is not required to show lack of consent.
- B. **Child or Minor:** a person under the age of 18.
- C. **Medical Forensic Examiner:** The health care provider conducting a sexual assault medical forensic examination.
- D. **Sexual Assault:** A person who engages in sexual contact or penetration with another person in a criminal manner as identified in MN Statute 609.342 to 609.3451.
- E. **Family and Household Member:** As defined in Minn. Stat. 518.B.01 Subd.2.b. to include:
- (1) spouses or former spouses;
 - (2) parents and children;
 - (3) persons related by blood;
 - (4) persons who are presently residing together or who have resided together in the past;
 - (5) persons who have a child in common regardless of whether they have been married or have lived together at any time;
 - (6) a man and woman if the woman is pregnant and the man is alleged to be the father, regardless of whether they have been married or have lived together at any time; and
 - (7) persons involved in a significant romantic or sexual relationship
- F. **Sexual Assault Medical Forensic Examination:** An examination of a sexual assault patient by a health care provider, ideally one who has specialized education and clinical experience in the collection of forensic evidence and treatment of these patients.
- G. **Victim Advocate:** A Sexual Assault Counselor defined by Minn. Stat. 595.02, subd. 1(k) and/or Domestic Abuse Advocate as defined by Minn. Stat. 595.02, subd. 1(1) who provide confidential advocacy services to victims of sexual assault and domestic abuse. Victim advocates as defined provide coverage in all counties in Minnesota. Minnesota Office of Justice Programs (MN OJP) can assist departments in locating their local victim advocacy agency for the purposes outlined in this policy.
- H. **Victim Centered:** A victim-centered approach prioritizes the safety, privacy and well-being of the victim and aims to create a supportive environment in which the victim's rights are respected and in which they are treated with dignity and respect. This approach acknowledges and respects a victims' input into the criminal justice response and recognizes victims are not responsible for the crimes committed against them.
- I. **Vulnerable Adult:** any person 18 years of age or older who:
- (1) is a resident inpatient of a facility as defined in Minn. Stat. 626.5572. Subd. 6;

- (2) receives services at or from a facility required to be licensed to serve adults under sections [245A.01](#) to [245A.15](#), except that a person receiving outpatient services for treatment of chemical dependency or mental illness, or one who is committed as a sexual psychopathic personality or as a sexually dangerous person under chapter 253B, is not considered a vulnerable adult unless the person meets the requirements of clause (4);
- (3) receives services from a home care provider required to be licensed under sections [144A.43](#) to [144A.482](#); or from a person or organization that exclusively offers, provides, or arranges for personal care assistance services under the medical assistance program as authorized under sections [256B.0625, subdivision 19a](#), [256B.0651](#) to [256B.0654](#), and [256B.0659](#); or
- (4) regardless of residence or whether any type of service is received, possesses a physical or mental infirmity or other physical, mental, or emotional dysfunction:
 - (i) that impairs the individual's ability to provide adequately for the individual's own care without assistance, including the provision of food, shelter, clothing, health care, or supervision; and
 - (ii) because of the dysfunction or infirmity and the need for assistance, the individual has an impaired ability to protect the individual from maltreatment.

IV. PROCEDURES

A. Communications Personnel Response/Additional Actions by Responding Officers

Communications personnel and/or law enforcement officers should inform the victim of ways to ensure critical evidence is not lost, to include the following:

- 1) Suggest that the victim not bathe, or clean him or herself if the assault took place recently.
- 2) Recommend that if a victim needs to relieve themselves, they should collect urine in a clean jar for testing, and should avoid wiping after urination.
- 3) Asking the victim to collect any clothing worn during or after the assault and if possible, place in a paper bag, instructing the victim not to wash the clothing (per department policy).
- 4) Reassure the victim that other evidence may still be identified and recovered even if they have bathed or made other physical changes.

B. Initial Officer Response

When responding to a scene involving a sexual assault, officers shall follow standard incident response procedures. In addition, when interacting with victims, officers shall do the following:

- 1) Recognize that the victim experienced a traumatic incident and may not be willing or able to immediately assist with the criminal investigation.

- 2) The officer shall attempt to determine the location/jurisdiction where the assault took place.
- 3) Explain the reporting process including the roles of the first responder, investigator, and anyone else with whom the victim will likely interact during the course of the investigation.
- 4) Officers are encouraged to connect the victim with local victim advocates as soon as possible. Inform the victim that there are confidential victim advocates available to address any needs they might have and to support them through the criminal justice system process. Provide the victim with contact information for the local victim advocate. Upon victim request the officer can offer to contact local victim advocate on behalf of the victim.
- 5) Ask about and document signs and symptoms of injury, to include strangulation. Officers shall attempt to obtain a signed medical release from the victim.
- 6) Ensure that the victim knows they can go to a designated facility for a forensic medical exam. Offer to arrange for transportation for the victim.
- 7) Identify and attempt to interview potential witnesses to the sexual assault and/or anyone the victim told about the sexual assault.
- 8) Request preferred contact information for the victim for follow-up.

C. Victim Interviews

This agency recognizes that victims of sexual assault due to their age or physical, mental or emotional distress, are better served by utilizing trauma informed interviewing techniques and strategies. Such interview techniques and strategies eliminate the duplication of interviews and use a question and answer interviewing format with questioning nondirective as possible to elicit spontaneous responses.

In recognizing the need for non-traditional interviewing techniques for sexual assault victims, officers should consider the following:

- Offer to have a confidential victim advocate present (if possible) if the victim would benefit from additional support during the process
- Whenever possible, conduct victim interviews in person
- Make an effort to conduct the interview in a welcoming environment
- Let the victim share the details at their own pace
- Recognize victims of trauma may have difficulty remembering incidents in a linear fashion and may remember details in days and weeks following the assault
- After the initial interview, consider reaching out to the victim within a few days, after at least one sleep cycle to ask if they remember any additional details.

- Depending on the victim, additional interviews might be needed to gather additional information. Offer support from a victim advocate to the victim to help facilitate engagement with the investigative process and healing.
- Some victims do remember details vividly and might want to be interviewed immediately.
- During initial and subsequent victim interviews, officers should note the following information as victims share it, recognizing that a victim may not be able to recall all the details of the assault during a particular interview.
 - 1) Whether the suspect was known to the victim
 - 2) How long the victim knew the suspect
 - 3) The circumstances of their meeting and if there is any indication of the use of drugs or alcohol to facilitate the sexual assault
 - 4) The extent of their previous or current relationship
 - 5) Any behavioral changes that led the situation from one based on consent to one of submission, coercion, fear, or force
 - 6) Specific actions, statements, and/or thoughts of both victim and suspect immediately prior, during, and after assault
 - 7) Relevant communication through social media, email, text messages, or any other forms of communication

D. Special Considerations—Minors and Vulnerable Adults/Domestic Abuse Victims

1. Minors and Vulnerable Adults

This agency recognizes that certain victims, due to their age or a physical, mental, or emotional distress, are better served by utilizing interview techniques and strategies that eliminate the duplication of interviews and use a question and answer interviewing format with questioning as nondirective as possible to elicit spontaneous responses. Members of this agency will be alert for victims who would be best served by the use of these specialized interview techniques. Officers, in making this determination, should consider the victim's age, level of maturity, communication skills, intellectual capacity, emotional state, and any other observable factors that would indicate specialized interview techniques would be appropriate for a particular victim. When an officer determines that a victim requires the use of these specialized interview techniques, the officer should follow the guidance below.

- a. Officers responding to reports of sexual assaults involving these sensitive population groups shall limit their actions to the following:
 - (1) Ensuring the safety of the victim;
 - (2) Ensuring the scene is safe;
 - (3) Safeguarding evidence where appropriate;
 - (4) Collecting any information necessary to identify the suspect; and
 - (5) Addressing the immediate medical needs of individuals at the scene

- b. Initial responding officers should not attempt to interview the victim in these situations, but should instead attempt to obtain basic information and facts about the situation, including the jurisdiction where the incident occurred and that a crime most likely occurred. Officers should seek to obtain this information from parents, caregivers, the reporting party, or other adult witnesses, unless those individuals are believed to be the perpetrators.
- c. Officers responding to victims with special considerations must comply with the mandated reporting requirements of Minnesota Statute Section 260E.06 and 626.557, as applicable. Officers investigating cases involving victims with special considerations should coordinate these investigations with the appropriate local human services agency where required. Any victim or witness interviews conducted with individuals having special considerations must be audio and video recorded whenever possible. All other interviews must be audio recorded whenever possible.

Not all sexual assaults of minor victims require a mandatory report to social services. This policy recognizes that in certain cases, notifying and/or the involvement of a parent/guardian pursuant to 260E.22 can cause harm to the minor and/or impede the investigation. Officers responding to the sexual assault of a minor victim that does not trigger a mandated report under Minnesota Statute Section 260E.06 should assess for the impact on the victim and the investigation if parents/guardians were notified before making a decision to involve them.

- d. Officers should obtain necessary contact information for the victim's caregiver, guardian or parents and where the victim may be located at a later time. Officers should advise the victim and/or any accompanying adult(s), guardians or caregivers that an investigating officer will follow up with information on a forensic interview.
 - e. The officer should advise the victim's caregiver, guardian or parent that if the victim starts to talk about the incident they should listen to them but not question them as this may influence any future statements.
2. Victims of Domestic Abuse
- Officers responding to a report of sexual assault committed against a family and household member must also follow the requirements and guidelines in this agency's domestic abuse policy and protocol, in addition to the guidelines in this policy.

E. Protecting Victim Rights

- 1) Confidentiality: Officers should explain to victims the limitations of confidentiality in a criminal investigation and that the victim's identifying information is not accessible to the public, as specified in Minn. Stat. section 13.82, subd. 17(b)
- 2) Crime Victim Rights: Officers must provide the following information to the victim:
 - a. Crime victim rights and resource information required to be provided to all victims as specified by Minn. Stat. section 611A.02, subd. 2(b)
 - b. If the suspect is a family or household member to the victim, crime victim rights and resource information required to be provided to domestic abuse victims, as specified by Minn. Stat. section 629.341, subd. 3.
 - c. The victim's right to be informed of the status of a sexual assault examination kit upon request as provided for under Minn. Stat. section 611A.27, subd. 1.
 - d. Pursuant to Minn. Stat. 611A.26, subd. 1, no law enforcement agency or prosecutor shall require that a complainant of a criminal sexual conduct or sex trafficking offense submit to a polygraph examination as part of or a condition to proceeding with the investigation, charging or prosecution of such offense.
- 3) Other information: Officers should provide to the victim the agency's crime report/ICR number, and contact information for the reporting officer and/or investigator or person handling the follow up.
- 4) Language access: All officers shall follow agency policy regarding limited English proficiency.

F. Evidence Collection

- 1) Considerations for Evidence Collection
Officers shall follow this agency's policy on crime scene response. In addition, officers may do the following:
 - a. Collect evidence regarding the environment in which the assault took place, including indications of isolation and soundproofing. The agency should consider utilizing their agency or county crime lab in obtaining or processing the scene where the assault took place. This should be in accordance to any/all other policies and procedures relating to evidence collections.
 - b. Document any evidence of threats or any communications made by the suspect, or made on behalf of the suspect, to include those made to individuals other than the victim.

- c. In situations where it is suspected that drugs or alcohol may have facilitated the assault, officers should assess the scene for evidence such as drinking glasses, alcohol bottles or cans, or other related items.
- d. If the victim has declined or a medical forensic exam will not be conducted, the officer should obtain victim consent and attempt to take photographs of visible physical injuries, including any healing or old injuries. Victim should be given directions about how to document any bruising or injury that becomes evidence later after these photographs are taken.

G. Sexual Assault Medical Forensic Examinations

- 1) Prior to the sexual assault medical forensic examination the investigating officer should do the following:
 - a. Ensure the victim understands the purpose of the sexual assault medical forensic exam and its importance to both their general health and wellness and to the investigation. Offer assurance to the victim that they will not incur any out-of-pocket expenses for forensic medical exams and provide information about evidence collection, storage and preservation in sexual assault cases.
 - b. Provide the victim with general information about the procedure, and encourage them to seek further detail and guidance from the forensic examiner, health care professional, or a victim advocate. Officers and investigators cannot deny a victim the opportunity to have an exam.
 - c. Officers should be aware and if necessary, relay to victims who do not want to undergo an exam that there might be additional treatments or medications they are entitled to even if they do not want to have an exam done or have evidence collected. Victims can seek that information from a health care provider or a victim advocate. If possible, transport or arrange transportation for the victim to the designated medical facility.
 - d. Ask the victim for a signed release for access to medical records from the exam.
- 2) Officers should not be present during any part of the exam, including during the medical history.
- 3) Following the exam, evidence collected during the exam shall be handled according to the requirements of agency policy and Minnesota Statute 299C.106.

H. Contacting and Interviewing Suspects

Prior to contacting the suspect, officers should consider the following:

- 1) Conduct a background and criminal history check specifically looking for accusations, criminal charges, and convictions for interconnected crimes, especially crimes involving violence.
- 2) Consider conducting a pretext or confrontational call or messaging depending on jurisdictional statutes. Involvement of a victim should be based on strong

consideration of the victim's emotional and physical state. A victim advocate should be present whenever possible to offer support.

- 3) When possible, an attempt would be made to interview the suspect in person.
- 4) In situations where suspects do not deny that a sexual act occurred, but rather assert that it was with the consent of the victim, officers should do the following:
 - a. Collect evidence of past communication, including but not limited to all relevant interaction (including social media) between the suspect and victim.
 - b. Identify events that transpired prior to, during, and after the assault in an effort to locate additional witnesses and physical locations that might lead to additional evidence.
- 5) For sexual assaults involving strangers, officers should focus investigative efforts on the collection of video, DNA, and other trace evidence used for analysis to identify the perpetrator (handle evidence collection per agency policy).

I. Forensic Examination and/or the Collection of Evidence from the Suspect

Note: A suspect's forensic examination and/or the collection of evidence from a suspect may be done by either an investigating officer/investigator, Forensic Medical Examiner, or the agency/county crime lab personnel.

- 1) Prior to or immediately after the preliminary suspect interview, photograph any injuries.
- 2) Determine whether a sexual assault medical forensic examination should be conducted.
- 3) Ask for the suspect's consent to collect evidence from their body and clothing. However, officers/investigators should consider obtaining a search warrant, with specific details about what evidence will be collected, and should be prepared in advance to eliminate the opportunity for the suspect to destroy or alter evidence if consent is denied.
- 4) During the suspect's sexual assault medical forensic examination, the investigator, evidence technician, or forensic examiner should do the following:
 - a. Strongly consider penile swabbing, pubic hair combings, and collection of other potential DNA evidence;
 - b. Collect biological and trace evidence from the suspect's body;
 - c. Document information about the suspect's clothing, appearance, scars, tattoos, piercings, and other identifiable marks;
 - d. Seize all clothing worn by the suspect during the assault, particularly any clothing touching the genital area;
 - e. Document the suspect's relevant medical condition and injuries.

J. Role of the Supervisor

Supervisors may do the following:

- 1) Assist officers investigating incidents of sexual assault when possible or if requested by an officer.
- 2) Provide guidance and direction as needed.
- 3) Review sexual assault reports to ensure that necessary steps were taken during initial response and investigations.

K. Case Review/Case Summary

A supervisor should ensure cases are reviewed on an on-going basis. The review process should include an analysis of:

- 1) Case dispositions
- 2) Decisions to collect evidence
- 3) Submissions of evidence for lab testing
- 4) Interviewing decisions

Eyewitness Identification Procedures Model Policy.pdf

EYEWITNESS IDENTIFICATION PROCEDURES MODEL POLICY

Minn. Stat. 626.8433

POLICY:

Officers shall adhere to the procedures for conducting eyewitness identifications set forth in this policy, in order to maximize the reliability of identifications, minimize erroneous identifications, and gather evidence that conforms to contemporary eyewitness identification protocols. Photo arrays and line-ups will be conducted by displaying the suspect and fillers sequentially using a blind or blinded administration.

Purpose:

It is the purpose of this policy to establish guidelines for eyewitness identification procedures involving show-ups, photo arrays, and line-ups. Erroneous eyewitness identifications have been cited as the factor most frequently associated with wrongful convictions. Therefore, in addition to eyewitness identification, all appropriate investigative steps and methods should be employed to uncover evidence that either supports or eliminates the suspect identification.

Definitions:

Show-up: The presentation of a suspect to an eyewitness within a short time frame following the commission of a crime to either confirm or eliminate him or her as a possible perpetrator. Show-ups, sometimes referred to as field identifications, are conducted in a contemporaneous time frame and proximity to the crime.

Line-up: The process of presenting live individuals to an eyewitness for the purpose of identifying or eliminating suspects.

Photo Array: A means of presenting photographs to an eyewitness for the purpose of identifying or eliminating suspects.

Administrator: The law enforcement official conducting the identification procedure.

Blinded Presentation: The administrator may know the identity of the suspect, but does not know which photo array member is being viewed by the eyewitness at any given time.

Confidence Statement: A statement in the witness's own words taken immediately after an identification is made stating his or her level of certainty in the identification.

Filler: A live person, or a photograph of a person, included in an identification procedure who is not considered a suspect.

Sequential: Presentation of a series of photographs or individuals to a witness one at a time.

Simultaneous: Presentation of a series of photographs or individuals to a witness all at once.

Procedure:

1. Show-ups

The use of show-ups should be avoided whenever possible in preference to the use of a lineup or photo array procedure. However, when circumstances require the prompt presentation of a suspect to a witness, the following guidelines shall be followed to minimize potential suggestiveness and increase reliability.

- a. Document the witness's description of the perpetrator prior to conducting the show up.
- b. Conduct a show-up only when the suspect is detained within a reasonably time frame after the commission of the offense and within a close physical proximity to the location of the crime.
- c. Do not use a show-up procedure if probable cause to arrest the suspect has already been established.
- d. If possible, avoid conducting a show-up when the suspect is in a patrol car, handcuffed, or physically restrained by officers, unless safety concerns make this impractical.
- e. Caution the witness that the person he or she is about to see may or may not be the perpetrator—and it is equally important to clear an innocent person. The witness should also be advised that the investigation will continue regardless of the outcome of the show-up.
- f. Do not conduct the show-up with more than one witness present at a time.
- g. Separate witnesses and do not allow communication between them before or after conducting a show-up.
- h. If one witness identifies the suspect, use a line-up or photo array for remaining witnesses.
- i. Do not present the same suspect to the same witness more than once.

- j. Do not require show-up suspects to put on clothing worn by, speak words uttered by, or perform other actions of the perpetrator.
- k. Officers should scrupulously avoid words or conduct of any type that may suggest to the witness that the individual is or may be the perpetrator.
- l. Ask the witness to provide a confidence statement.
- m. Remind the witness not to talk about the show-up to other witnesses until police or prosecutors deem it permissible.
- n. Videotape the identification process using an in-car camera or other recording device when feasible.
- o. Document the time and location of the show-up, the officers present, the result of the procedure, and any other relevant information.

Line-up and Photo Array Procedures

2. Basic Procedures for Conducting a Line-up or Photo Array

- a. Line-ups will not typically be utilized for investigations, unless conducting a photo array is not possible.
- b. Whenever possible, a blind presentation shall be utilized. In cases where a blind presentation is not feasible for a photo array, a blinded presentation should be used. Live line-ups must be conducted using a blind presentation.
- c. The line-up or photo array should consist of a minimum of six individuals or photographs. Use a minimum of five fillers and only one suspect.
- d. Fillers should be reasonably similar in age, height, weight, and general appearance and be of the same sex and race, in accordance with the witness's description of the offender.
- e. Avoid the use of fillers who so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers.
- f. Create a consistent appearance between the suspect and the fillers with respect to any unique or unusual feature (e.g., scars, tattoos, facial hair) used to describe the perpetrator by artificially adding or concealing that feature on the fillers.
- g. If there is more than one suspect, include only one in each line-up or photo array.

- h. During a blind presentation, no one who is aware of the suspect's identity should be present during the administration of the photo array. However, during a line-up, the suspect's attorney should be present.
- i. Place suspects in different positions in each line-up or photo array, both across cases and with multiple witnesses in the same case.
- j. Witnesses should not be permitted to see or be shown any photos of the suspect prior to the line-up or photo array.
- k. The witness shall be given a copy of the following instructions prior to viewing the line-up or photo array and the administrator shall read the instructions aloud before the identification procedure.

You will be asked to look at a series of individuals.

The perpetrator may or may not be present in the identification procedure.

It is just as important to clear innocent persons from suspicion as it is to identify guilty parties.

I don't know whether the person being investigated is included in this series.

Sometimes a person may look different in a photograph than in real life because of different hair styles, facial hair, glasses, a hat or other changes in appearance. Keep in mind that how a photograph was taken or developed may make a person's complexion look lighter or darker than in real life.

You should not feel that you have to make an identification. If you do identify someone, I will ask you to describe in your own words how certain you are.

The individuals are not configured in any particular order.

If you make an identification, I will continue to show you the remaining individuals or photos in the series.

Regardless of whether you make an identification, we will continue to investigate the incident.

Since this is an ongoing investigation, you should not discuss the identification procedures or results

- l. The line-up or photo array should be shown to only one witness at a time; officers should separate witnesses so they will not be aware of the responses of other witnesses.
- m. Multiple identification procedures should not be conducted in which the same witness views the same suspect more than once.
- n. Officers should scrupulously avoid the use of statements, cues, casual comments, or providing unnecessary or irrelevant information that in any manner may influence the witnesses' decision-making process or perception.
- o. Following an identification, the administrator shall ask the witness to provide a confidence statement and document the witness's response.
- p. The administrator shall ask the witness to complete and sign an Eyewitness Identification Procedure Form.
- q. Line-up and photo array procedures should be video or audio recorded whenever possible. If a procedure is not recorded, a written record shall be created and the reason for not recording shall be documented. In the case of line-ups that are not recorded, agents shall take and preserve a still photograph of each individual in the line-up.

3. Photographic Arrays

a. Creating a Photo Array

- 1. Use contemporary photos.
- 2. Do not mix color and black and white photos.
- 3. Use photos of the same size and basic composition.
- 4. Never mix mug shots with other photos and ensure consistent appearance of photograph backgrounds and sizing.
- 5. Do not include more than one photo of the same suspect.
- 6. Cover any portions of mug shots or other photos that provide identifying information on the subject – and similarly cover other photos used in the array.
- 7. Where the suspect has a unique feature, such as a scar, tattoo, or mole or distinctive clothing that would make him or her stand out in the photo array, filler photographs should include that unique feature either by selecting fillers who have the same features themselves or by altering the photographs of fillers to the extent necessary to achieve a consistent appearance.
- 8. Fillers should not be reused in arrays for different suspects shown to the same witness.

b. Conducting the Photo Array

- 1. The photo array should be preserved, together with full information about the identification process as part of the case file and documented in a report.

2. If a blind administrator is not available, the administrator shall ensure that a blinded presentation is conducted using the following procedures.
 - a. Place the suspect and at least five filler photos in separate folders for a total of six (or more depending on the number of fillers used).
 - b. The administrator will take one folder containing a known filler and place it to the side. This will be the first photo in the series. The administrator should then shuffle the remaining folders (containing one suspect and the remainder of fillers) such that he or she cannot see how the line-up members are ordered. These shuffled folders will follow the first filler photo. The stack of photos is now ready to be shown to the witness.
 - c. The administrator should position himself or herself so that he or she cannot see inside the folders as they are viewed by the witness.
3. The witness should be asked if he or she recognizes the person in the photo before moving onto the next photo. If an identification is made before all of the photos are shown, the administrator should tell the witness that he or she must show the witness all of the photos and finish showing the sequence to the witness, still asking after each photo if the witness recognizes the person in the photo.
4. If possible, the array should be shown to the witness only once. If, upon viewing the entire array the witness asks to see a particular photo or the entire array again, the witness should be instructed that he or she may view the entire array only one additional time. If a second viewing is permitted, it must be documented.

4. Line-ups

- a. Conducting the Line-up
 1. Live line-ups shall be conducted using a blind administrator.
 2. Ensure that all persons in the line-up are numbered consecutively and are referred to only by number.
- b. The primary investigating officer is responsible for the following:
 1. Scheduling the line-up on a date and at a time that is convenient for all concerned parties, to include the prosecuting attorney, defense counsel, and any witnesses.
 2. Ensuring compliance with any legal requirements for transfer of the subject to the line-up location if he or she is incarcerated at a detention center.
 3. Making arrangements to have persons act as fillers.
 4. Ensuring that the suspect's right to counsel is scrupulously honored and that he or she is provided with counsel if requested. Obtaining proper documentation of any waiver of the suspect's right to counsel.
 5. Allowing counsel representing the suspect sufficient time to confer with his or her client prior to the line-up and to observe the manner in which the line-up is conducted.

References:

Eyewitness Identification Procedure Form
Sequential Photo Display Form

**MN Public Assembly-First
Amendment Rights Model Policy .pdf**

Public Assembly and First Amendment Activity

References:

Minn. Rules 6700.1615

[First Amendment US Constitution](#)

[Minnesota Constitution](#)

[609.705. Unlawful Assembly](#)

[609.71 Riot](#)

[609. 066 Authorized Use of Force by Peace Officers](#)

[609.06 Authorized Use of Force](#)

1) PURPOSE

The First Amendment to the Constitution of the United States of America states, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, or abridging the freedom of speech or of the press, or the right of the people peaceably to assemble and to petition the Government for a redress of grievances."

The Bill of Rights in Article 1 of the [Minnesota Constitution](#) addresses the rights of free speech and the liberty of the press. However, neither the state nor federal constitutions protect criminal activity or threats against citizens, businesses, or critical infrastructure.

The [\(law enforcement agency\)](#) supports all people's fundamental right to peaceably assemble and their right to freedom of speech and expression.

The purpose of this policy is to provide guidelines to the [\(law enforcement agency\)](#) personnel regarding the application and operation of acceptable law enforcement actions addressing public assemblies and First Amendment Activity.

2) POLICY

The [\(law enforcement agency\)](#) will uphold the constitutional rights of free speech and assembly while using the minimum use of physical force and authority required to address a crowd management or crowd control issue.

The policy of the [\(law enforcement agency\)](#) ("department") regarding crowd management and crowd control is to apply the appropriate level of direction and control to protect life, property, and vital facilities while maintaining public peace and order during a public assembly or First Amendment activity. Department personnel must not harass, intimidate, or discriminate against or unreasonably interfere with persons engaged in the lawful exercise of their rights.

This policy concerning crowd management, crowd control, crowd dispersal, and police responses to violence and disorder applies to spontaneous demonstrations, crowd event situations, and planned demonstration or crowd events regardless of the permit status of

the event.

This policy is to be reviewed annually.

3) DEFINITIONS

- A. Chemical Agent Munitions: Munitions designed to deliver chemical agents from a launcher or hand thrown.
- B. Control Holds: Control holds are soft empty hand control techniques as they do not involve striking.
- C. Crowd Management: Techniques used to manage lawful public assemblies before, during, and after an event. Crowd management can be accomplished in part through coordination with event planners and group leaders, permit monitoring, and past event critiques.
- D. Crowd Control: Techniques used to address unlawful public assemblies.
- E. Deadly Force: Force used by an officer that the officer knows, or reasonably should know, creates a substantial risk of causing death or great bodily harm.
(Reference: (law enforcement agency's) Use of Force Policy, MN Statutes [609.06](#) and [609. 066](#))
- F. Direct Fired Munitions: Less-lethal impact munitions that are designed to be direct fired at a specific target.
- G. First Amendment Activities: First Amendment activities include all forms of speech and expressive conduct used to convey ideas and/or information, express grievances, or otherwise communicate with others and include both verbal and non-verbal expression. Common First Amendment activities include, but are not limited to, speeches, demonstrations, vigils, picketing, distribution of literature, displaying banners or signs, street theater, and other artistic forms of expression. All these activities involve the freedom of speech, association, and assembly and the right to petition the government, as guaranteed by the United States Constitution and the [Minnesota State Constitution](#).

The government may impose reasonable restrictions on the time, place, or manner of protected speech, provided the restrictions are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information.

- H. Great Bodily Harm: Bodily injury which creates a high probability of death, or which causes serious, permanent disfigurement, or which causes a permanent or protracted loss or impairment of the function of any bodily member or organ or other serious bodily harm. (Reference: (law enforcement agency's) Use of Force Policy, MN Statutes [609.06](#) and [609. 066](#))
- I. Legal Observers – Individuals, usually representatives of civilian human rights agencies, who attend public demonstrations, protests and other activities. The following may be indicia of a legal observer: Wearing a green National Lawyers' Guild issued or authorized Legal Observer hat and/or vest (a green NLG hat and/or black vest with green labels) or wearing a blue ACLU issued or authorized legal observer vest.
- J. Less-lethal Impact Munitions. Impact munitions which can be fired, launched, or

otherwise propelled for the purpose of encouraging compliance, overcoming resistance or preventing serious injury without posing significant potential of causing death.

- K. **Media:** Media means any person who is an employee, agent, or independent contractor of any newspaper, magazine or other periodical, book publisher, news agency, wire service, radio or television station or network, cable or satellite station or network, or audio or audiovisual production company, or any entity that is in the regular business of news gathering and disseminating news or information to the public by any means, including, but not limited to, print, broadcast, photographic, mechanical, internet, or electronic distribution. For purposes of this policy, the following are indicia of being a member of the media: visual identification as a member of the press, such as by displaying a professional or authorized press pass or wearing a professional or authorized press badge or some distinctive clothing that identifies the wearer as a member of the press.

4) Law Enforcement Procedures

- A. **Uniform:** All officers responding to public assemblies must at all times, including when wearing protective gear, display their agency name and a unique personal identifier in compliance with this department's uniform policy. The chief law enforcement officer must maintain a record of any officer(s) at the scene who is not in compliance with this requirement due to exigent circumstances.
- B. **Officer conduct:**
1. Officers shall avoid negative verbal engagement with members of the crowd. Verbal abuse against officers does not constitute a reason for an arrest or for any use of force against such individuals.
 2. Officers must maintain professional demeanor and remain neutral in word and deed despite unlawful or anti-social behavior on the part of crowd members.
 3. Officers must not take action or fail to take action based on the opinions being expressed.
 4. Officers must not interfere with the rights of members of the public to observe and document police conduct via video, photographs, or other methods unless doing so interferes with on-going police activity.
 5. Officers must not use a weapon or munition unless the officer has been trained in the use and qualified in deployment of the weapon/munition.
 6. This policy does not preclude officers from taking appropriate action to direct crowd and vehicular movement; enforce ordinances and statutes; and to maintain the safety of the crowd, the general public, law enforcement personnel, and emergency personnel.

5. Responses to Crowd Situations

- A. **Lawful assembly.** Individuals or groups present on the public way, such as public facilities, streets or walkways, generally have the right to assemble, rally, demonstrate, protest, or otherwise express their views and opinions through varying forms of communication including the distribution of printed matter. These rights may be limited by laws or ordinances regulating such matters as the obstruction of individual or vehicle access or egress, trespass, noise, picketing, distribution of handbills, leafleting and

loitering.

B. Unlawful assembly

1. The definition of an unlawful assembly has been set forth in Minnesota Statute [§609.705](#).
2. The mere failure to obtain a permit, such as a parade permit or sound permit, is not a sufficient basis to declare an unlawful assembly
3. The fact that some of the demonstrators or organizing groups have engaged in violent or unlawful acts on prior occasions or demonstrations is not grounds for declaring an assembly unlawful.
4. Whenever possible, the unlawful behavior of a few participants must not result in the majority of peaceful protestors being deprived of their First Amendment rights, unless other participants or officers are threatened with dangerous circumstances.
5. Unless emergency or dangerous circumstances prevent negotiation, crowd dispersal techniques must not be initiated until after attempts have been made through contacts with the police liaisons and demonstration or crowd event leaders to negotiate a resolution of the situation so that the unlawful activity will cease, and the First Amendment activity can continue.

C. Declaration of Unlawful Assembly

1. If the on-scene supervisor/incident commander has declared an unlawful assembly, the reasons for the declaration and the names of the decision maker(s) must be recorded. The declaration and dispersal order must be announced to the assembly. The name(s) of the officers announcing the declaration should be recorded, with the time(s) and date(s) documented.
2. The dispersal order must include:
 - a) Name, rank of person, and agency giving the order
 - b) Declaration of Unlawful Assembly and reason(s) for declaration
 - c) Egress or escape routes that may be used
 - d) Specific consequences of failure to comply with dispersal order
 - e) How long the group has to comply
3. Whenever possible, dispersal orders should also be given in other languages that are appropriate for the audience. Officers must recognize that not all crowd members may be fluent in the language(s) used in the dispersal order.
4. Dispersal announcements must be made in a manner that will ensure that they are audible over a sufficient area. Dispersal announcements-must be made from different locations when the demonstration is large and noisy. The dispersal announcements should be repeated after commencement of the dispersal operation so that persons not present at the original broadcast will understand that they must leave the area. The announcements must also specify adequate egress or escape routes. Whenever possible, a minimum of two escape/egress routes shall be identified and announced.

D. Crowd Dispersal

1. Crowd dispersal techniques should not be initiated until officers have made repeated announcements to the crowd, or are aware that repeated announcements

- have been made, asking members of the crowd to voluntarily disperse, and informing them that, if they do not disperse, they will be subject to arrest.
2. Unless an immediate risk to public safety exists or significant property damage is occurring, sufficient time will be allowed for a crowd to comply with officer commands before action is taken.
 3. If negotiations and verbal announcements to disperse do not result in voluntary movement of the crowd, officers may employ additional crowd dispersal tactics, but only after orders from the on-scene supervisor/incident commander. The use of these crowd dispersal tactics shall be consistent with the department policy of using the minimal officer intervention needed to address a crowd management or control issue.
 4. If, after a crowd disperses pursuant to a declaration of unlawful assembly and subsequently participants assemble at a different geographic location where the participants are engaged in non-violent and lawful First Amendment activity, such an assembly cannot be dispersed unless it has been determined that it is an unlawful assembly, and a new declaration of unlawful assembly has been made.

6. Tactics and Weapons to Disperse or Control a Non-Compliant Crowd

Nothing in this policy prohibits officers' abilities to use appropriate force options to defend themselves or others as defined in the (law enforcement agency's) Use of Force policy.

A. Use of Batons

1. Batons must not be used for crowd control, crowd containment, or crowd dispersal except as specified below.
2. Batons may be visibly displayed and held in a ready position during squad or platoon formations.
3. When reasonably necessary for protection of the officers or to disperse individuals in the crowd pursuant to the procedures of this policy, batons may be used in a pushing, pulling, or jabbing motion. Baton jabs must not be used indiscriminately against a crowd or group of persons but only against individuals who are physically aggressive or actively resisting arrest. Baton jabs should not be used in a crowd control situation against an individual who is attempting to comply but is physically unable to disperse or move because of the press of the crowd or some other fixed obstacle.
4. Officers must not strike a person with any baton to the head, neck, throat, kidneys, spine, or groin, or jab with force to the armpit unless the person has created an imminent threat of great bodily harm to another.
5. Batons shall not be used against a person who is handcuffed except when permissible under this department's Use of Force policy and state law.

B. Restrictions on Crowd Control and Crowd Dispersal

1. Canines. Canines must not be used for crowd control, crowd containment, or crowd dispersal.
2. Fire Hoses. Fire hoses must not be used for crowd control, crowd containment, or crowd dispersal.
3. Electronic Control Weapons (ECWs) must not be used for crowd control, crowd

containment, or crowd dispersal.

4. Motorcycles and police vehicles must not be used for crowd dispersal, but may be used for purposes of observation, visible deterrence, traffic control, transportation, and area control during a crowd event.
5. Skip Fired Specialty Impact Less-Lethal Munitions (Wooden Dowels and Stinger Grenades) may be used as a last resort if other crowd dispersal techniques have failed or have been deemed ineffective.
6. Direct Fired munitions may never be used indiscriminately against a crowd or group of persons even if some members of the crowd or group are violent or disruptive.
 - a) Except for exigent circumstances, the on-scene supervisor/incident commander must authorize the deployment of Direct Fired munitions. Direct Fired munitions must be used only against a specific individual who is engaging in conduct that poses an immediate threat of loss of life or serious bodily injury to them self, officers, or the general public; or is creating an imminent risk to the lives or safety of other persons through the substantial destruction of property.
 - b) Officers shall not discharge a Direct Fired munitions at a person's head, neck, throat, face, left armpit, spine, kidneys, or groin unless deadly force would be justified.
 - c) When circumstances permit, the on-scene supervisor/incident commander must make an attempt to accomplish the policing goal without the use of Direct Fired munitions as described above, and, if practical, an audible warning shall be given to the subject before deployment of the weapon.
7. Aerosol Hand-held Chemical Agents must not be used in a demonstration or crowd situation or other civil disorders without the approval of the on-scene supervisor/incident commander.
 - a) Aerosol, hand-held, pressurized, containerized chemical agents that emit a stream shall not be used for crowd management, crowd control, or crowd dispersal during demonstrations or crowd events. Aerosol hand-held chemical agents may not be used indiscriminately against a crowd or group of persons, but only against specific individuals who are engaged in specific acts of serious unlawful conduct or who are actively resisting arrest.
 - b) Officers shall use the minimum amount of the chemical agent necessary to overcome the subject's resistance.
 - c) When possible, persons should be removed quickly from any area where hand held chemical agents have been used. Officers must monitor the subject and pay particular attention to the subject's ability to breathe following the application of a chemical agent.
 - d) A subject who has been sprayed with a hand-held chemical agent shall not be left lying on their stomach once handcuffed or restrained with any device.
9. Chemical munitions use in a crowd situation is subject to the following:
 - a) Chemical munitions must be used only when:
 - 1) a threat of imminent harm or serious property damage is present, or

other crowd dispersal techniques have failed or did not accomplish the policing goal as determined by the incident commander,

- 2) sufficient egress to safely allow the crowd to disperse exists, and
 - 3) The use of chemical munitions is approved by the on-scene supervisor/incident commander, and
- b) When feasible, additional announcements should be made prior to the use of chemical munitions in a crowd situation warning of the imminent use of chemical munitions.
 - c) Deployment of chemical munitions into a crowd must be avoided to prevent unnecessary injuries.
 - d) CN chemical munitions are prohibited.
 - e) The use of each chemical munition must be recorded (time, location), and the following information must be made available by the department on request :
 - 1) the name of each chemical munition used in an incident,
 - 2) the location and time of use for each munition deployment,
 - 3) access to the safety data sheet (SDS) for chemical munition
 - f) Where extensive use of chemical munitions would reasonably be anticipated to impact nearby residents or businesses, agencies should consider proactively notifying impacted individuals of safety information related to the munitions use as soon as possible, even if after the event.
 - g) When chemical munitions are used, an emergency responder will be on standby at a safe distance near the target area when feasible.
 - h) Chemical munitions are subject to the same procedural requirements as outlined in the (law enforcement department)'s UOF policy.

C. Arrests

1. If the crowd has failed to disperse after the required announcements and sufficient time to disperse, officers may encircle the crowd or a portion of the crowd for purposes of making multiple simultaneous arrests.
2. Persons who make it clear (e.g., by non-violent civil disobedience) that they seek to be arrested may be arrested and must not be subjected to other dispersal techniques, such as the use of batons or chemical agents. Persons refusing to comply with arrest procedures may be subject to the reasonable use of force.
3. Arrests of non-violent persons shall be accomplished by verbal commands and persuasion, handcuffing, lifting, carrying, the use of dollies and/or stretchers, and/or the use of soft empty hand control holds.
4. Officers must document any injuries reported by an arrestee, and as soon as practical, officers must obtain professional medical treatment for the arrestee.
5. Juveniles arrested in demonstrations shall be handled consistent with department policy on arrest, transportation, and detention of juveniles.
6. Officers arresting a person with a disability affecting mobility or communication must follow the department policy on arrest, transportation, and detention of persons with disabilities.

6. Handcuffs

- A. All persons subject to arrest during a demonstration or crowd event shall be handcuffed in accordance with department policy, orders, and training bulletins.
- B. Officers should be cognizant that flex-cuffs may tighten when arrestees hands swell or move, sometimes simply in response to pain from the cuffs themselves. When arrestees complain of pain from overly tight flex cuffs, officers must examine the cuffs and ensure proper fit.
- C. Arrestees in flex-cuffs must be monitored to prevent injury.
- D. Each unit involved in detention and/or transportation of arrestees with flex-cuffs should have a flex-cuff cutter and adequate supplies of extra flex-cuffs readily available.

7. Media.

- A. The media have a First Amendment right to cover public activity, including the right to record video or film, livestream, photograph, or use other mediums.
- B. The media must not be restricted to an identified area, and must be permitted to observe and must be permitted close enough access to view the crowd event and any arrests. An onsite supervisor/incident commander may identify an area where media may choose to assemble.
- C. Officers will not arrest members of the media unless they are physically obstructing lawful efforts to disperse the crowd, or efforts to arrest participants, or engaged in criminal activity.
- D. The media must not be targeted for dispersal or enforcement action because of their media status.
- E. Even after a dispersal order has been given, clearly identified media must be permitted to carry out their professional duties unless their presence would unduly interfere with the enforcement action.

8. Legal Observers

- A. Legal observers, including unaffiliated self-identified legal observers and crowd monitors, do not have the same legal status as the media, and are subject to laws and orders similar to any other person or citizen.
- B. Legal observers and monitors must comply with all dispersal orders unless the on-site supervisor/incident commander chooses to allow such an individual legal observers and monitors to remain in an area after a dispersal order.
- C. Legal observers and crowd monitors must not be targeted for dispersal or enforcement action because of their status.

9. Documentation of Public Assembly and First Amendment Activity

- A. The purpose of any visual documentation by (law enforcement agency) of a public assembly or first amendment activity must be related only to:
 - 1) Documentation of the event for the purposes of debriefing,
 - 2) Documentation to establish a visual record for the purposes of responding to citizen complaints or legal challenges, or
 - 3) Creating visual records for training purposes.

- B. If it is the policy of (law enforcement agency) to videotape and photograph, it must be done in a manner that minimizes interference with people lawfully participating in First Amendment activities. Videotaping and photographing of First Amendment activities must take place only when authorized by the on-site supervisor/incident commander.
 - C. Individuals should not be singled out for photographing or recording simply because they appear to be leaders, organizers, or speakers.
 - D. Unless evidence of criminal activity is provided, videos or photographs of demonstrations shall not be disseminated to other government agencies, including federal, state, and local law enforcement agencies. If videos or photographs are disseminated or shared with another law enforcement agency, a record should be created and maintained noting the date and recipient of the information.
 - E. If there are no pending criminal prosecutions arising from the demonstration or if the video recording or photographing is not relevant to an Internal Affairs or citizen complaint investigation or proceedings or to civil litigation arising from police conduct at the demonstration, the video recording and/or photographs shall be destroyed in accordance with department policies.
 - F. This directive shall not prohibit department members from using these videos or footage from such videos as part of training materials for officers in crowd control and crowd dispersal techniques and procedures.
-

South Saint Paul Police Department Policy Manual

S Saint Paul PD Policy Manual

INDEX / TOPICS

A

ABUSE OF AUTHORITY.	9
ACCOUNTABILITY TO SUPERVISOR.	17
ADMINISTRATIVE INVESTIGATIONS	
Criminal parallel.	494
OIS.	56
Vehicle damage.	400
ADMINISTRATIVE LEAVE.	494
AGENCYHEAD.	60
AIRCRAFT	
Accidents.	273
ALCOHOL	
Firearms.	63
Intoxicants.	151
Vehicle use.	397
AMMUNITION.	61
ANIMAL CONTROL.	439
ANIMALS	
Euthanize.	65
Injured.	65
Line-of-duty deaths.	557
ANTI-RETALIATION.	479
APPOINTMENTS	
Exposure control officer.	484
ARRESTS	
Consular notifications.	451
Control devices.	42
First amendment assemblies.	317
Towed vehicles.	354
ASSET FORFEITURE.	365
AUDIO/VIDEO RECORDING	
Holding cells.	456
AUDITS	
Informant files.	374
Informant funds.	377
Personnel complaints.	490
AUTHORITY	
Law enforcement.	8
AUTHORIZED WEAPONS.	60
AUTOMATED LICENSE PLATE READER (ALPR).	302

B

BADGE.	537
BADGES, PATCHES AND IDENTIFICATION	
Administrative leave.	494
BARRICADED SUSPECT.	247
BARRICADED SUSPECTS.	246
BIAS-BASED POLICING.	236
BIOLOGICAL SAMPLES	
Hazards.	274
BODY ARMOR.	500
BODY ARMOR	
Suspects.	61
BOMBS	
Aircraft accidents.	274
Chaplains.	202
MDT/MDC.	289
C	
CANINES	
Foot pursuits.	297
CASH	
Audit.	377
Custody.	455
CERTIFICATE MAINTENANCE.	541
CHAPLAINS.	198
CHIEF EXECUTIVE.	10
CHILD ABUSE.	120
CHILD ABUSE	
Mandatory notifications.	120
CHILDREN	
Firearms.	64
Safety.	453
CHILD SAFETY SEAT.	498
CITATION RELEASES.	259
CIVIL	
Liability response.	57
Subpoenas.	168
CIVIL DISPUTES.	325
CIVILIAN/NON-SWORN	
Crisis intervention incidents.	324
COMMAND STAFF	
Line-of-duty deaths.	547
Work-related injuries.	523
COMMUNICABLE DISEASES	
Custody.	449
COMMUNICATION CENTER	
Mandatory sharing.	170
CONDUCT.	145
Personnel complaints.	488
Standards of conduct.	150
CONFIDENTIALITY	
Communicable disease information.	487

South Saint Paul Police Department

S Saint Paul PD Policy Manual

South Saint Paul Police Department Policy Manual

Custodial telephone calls.	453
Informants.	372
Personnel complaints.	497
CONTACTS AND TEMPORARY DETENTIONS	
Bias-based policing.	237
CONTROL DEVICES.	42
Custody.	454
Decontamination.	485
Training.	266
COURT APPEARANCES.	167
COURT ORDERED FIREARMS SURRENDER	
Domestic Violence.	98
COURT ORDERED FIREARM SURRENDERS	
Child Abuse.	127
COURT ORDERS	
Civil disputes.	325
Source testing.	487
Subpoenas.	167
CRIME AND DISASTER SCENE	
INTEGRITY.	239
CRIMINAL ACTIVITY REPORTING.	159
CRISIS INTERVENTION INCIDENTS.	320
CRISIS RESPONSE UNIT.	249
CUSTODIAL SEARCHES.	458

D

DAMAGE BY PERSONNEL.	161
DEATH	
Traffic related.	350
DEATH NOTIFICATION.	181
DEFECTIVE VEHICLES.	393
DEFINITIONS	
Policy Manual.	12
DEPARTMENT/OFFICE-OWNED	
PROPERTY.	387
Loss or damage.	388
DEPARTMENTAL DIRECTIVES.	18
DEPENDENT ADULTS	
Safety.	453
DISCIPLINE	
Personnel complaints.	496
DISCLAIMERS	
Policy Manual.	12
DISCRIMINATION	
Personnel complaints.	490
DISPUTED CLAIMS.	414
DNA SAMPLES.	196
DRIVING	
MDT/MDC.	287
Safety.	151
DUTY FIREARMS.	60

E

ELECTRONIC MAIL.	20
Personnel complaints.	489
EMPLOYEE COMMENDATIONS.	506
EMPLOYEE CONVICTIONS.	482
EVIDENCE	
Bombs.	255
Personnel complaints.	489
Seizing recordings.	308
EXAMINATIONS	
Mental, Physical.	510
EXPLOSIONS.	254
EXPOSURE(S).	245
EXPOSURE CONTROL.	484
Officer.	484

F

FIELD TRAINING OFFICER.	277
FIREARMS	
Proficiency.	62
FIREARMS	
Conduct.	151
Custody.	454
Destruction of animals.	440
Retiree carry.	22
Vehicle Use.	398
FIRST AMENDMENT ASSEMBLIES.	313
FITNESS FOR DUTY.	509
FOREIGN	
Nationals.	451
FOREIGN DIPLOMATIC AND CONSULAR	
REPRESENTATIVES.	261
FORMS	
Complaint.	489
Unauthorized possession of medical	
cannabis.	329

H

HANDCUFFING AND RESTRAINTS	
Custody.	455
HANDCUFFS.	39
HATE CRIMES.	152
HAZARDOUS MATERIAL.	244
HAZARDOUS MATERIAL (HAZMAT)	
RESPONSE	
Aircraft accidents.	274
Precautions.	485

South Saint Paul Police Department

S Saint Paul PD Policy Manual

South Saint Paul Police Department Policy Manual

Traffic.	349
HIGH-VISIBILITY VESTS.	348
HOSTAGE AND BARRICADE INCIDENTS	
Rapid response and deployment.	266
HOSTAGES.	246
HOSTAGE SITUATION.	248

I

IDENTITY THEFT.	183
IMMUNIZATIONS.	486
INFORMANTS.	372
INFORMATION TECHNOLOGY USE.	155
INSPECTIONS	
Control devices.	42
Exposure control.	484
Firearms.	64
Holding cells.	456
INTERNAL AFFAIRS	
Personnel records.	503
INTERROGATIONS, RECORDING.	360
INVESTIGATION AND PROSECUTION.	360

J

JURISDICTION	
Aircraft accidents.	274
Consular notification.	451
JURISDICTION	
Traffic collisions.	349

K

KEYS	
Vehicle.	396
KINETIC ENERGY PROJECTILE.	44

L

LAW ENFORCEMENT AUTHORITY.	8
LEG RESTRAINTS.	40
LIMITED ENGLISH PROFICIENCY.	187
LIMITED ENGLISH PROFICIENCY	
Eyewitness identification.	379

M

MANUALS.	19
MEDIA	

Aircraft accidents.	275
First amendment assemblies.	318
OIS.	59
MEDIA REQUEST.	163
MEDICAL	
Aircraft accidents.	273
Personnel records.	503
Screening - custody adults.	453
Treatment for OC spray.	43
Treatment for work-related injury and illness.	522
MINIMUM STAFFING.	21
MOBILE DIGITAL TERMINAL USE.	287
MUTUAL AID.	169
First amendment assemblies.	316

N

NEWS MEDIA RELATIONS.	163
NONSWORN	
Vehicles.	397
NOTIFICATION	
Consular.	451
NOTIFICATIONS.	53
Pregnancy.	541
NOTIFICATIONS	
Aircraft accidents.	274
Exposure control.	484
Traffic death.	350
Vehicle towing.	354

O

OATH OF OFFICE.	11
OCCUPATIONAL DISEASE, PERSONAL	
INJURY AND DEATH REPORTING.	522
OC SPRAY.	43
OFFICER/DEPUTY RESPONSE TO CALLS.	81
OFFICER SAFETY	
Crime and disaster scene integrity.	239
Firearm confiscation.	52
Foot pursuits.	297
Informants.	374
LEOSA.	22
Seat belts.	498
Vehicle towing.	355
OLEORESIN CAPSICUM.	43
OPERATIONS LIEUTENANT.	65
ORGANIZATIONAL STRUCTURE.	16
OUTSIDE AGENCY ASSISTANCE.	169
OUTSIDE EMPLOYMENT.	518

South Saint Paul Police Department

S Saint Paul PD Policy Manual

South Saint Paul Police Department Policy Manual

Change in Status.	520
Obtaining Approval.	518
Prohibited Outside Employment.	519
OVERTIME	
Court.	168

P

PARKING.	397
PATROL FUNCTION.	234
PEPPER SPRAY.	43
PERSONAL APPEARANCE.	525
PERSONAL PROPERTY.	387
Loss or damage.	388
PERSONNEL COMPLAINTS	
Bias-based policing.	237
PERSONNEL RECORDS.	502
PHOTOGRAPHS	
Aircraft accidents.	275
First amendment assemblies.	314
PLASTIC CUFFS.	39
POLICY MANUAL.	12
POLICY REVISIONS.	14
PREGNANCY.	541
PREGNANCY	
Custody.	449, 455
PRIVACY EXPECTATION	
MDT/MDC.	287
PRIVACY EXPECTATIONS	
Administrative searches.	494
PRIVATE PERSONS ARRESTS.	185
PROBATIONARY EMPLOYEES	
Personnel complaints.	497
PROPERTY PROCEDURES.	408
Controlled Substances.	409
Disputed Claims.	414
Packaging Of Property.	411
Property Booking.	409
Property Release.	413
PROTECTED INFORMATION.	427
PROTECTED INFORMATION.	427
PROTECTIVE CUSTODY.	122
PUBLIC RECORDING OF LAW	
ENFORCEMENT ACTIVITY.	307
PURSUIT INTERVENTION.	77
PURSUIT POLICY.	68
PURSUIITS	
Foot.	297

R

RANGEMASTER	
Control devices.	42
RAPID RESPONSE AND DEPLOYMENT.	265
RECORDS BUREAU	
Suspicious activity reporting.	331
RECORDS REQUESTS	
Personnel records.	504
RECORDS RETENTION	
Personnel complaints.	497
REFLECTORIZED VESTS.	348
RELIGIOUS	
Accommodations in custody.	454
REPORT CORRECTIONS.	161
REPORTING CONVICTIONS.	482
Family Violence.	482
REPORT PREPARATION.	159
RESTRAINTS.	38
RESTRICTED INFORMATION.	165
REVIEWS	
Crisis intervention incidents.	324
Exposure control plan.	484
Mobile audio/video.	237
RIDE-ALONG.	241
Eligibility.	241

S

SAFE HAVEN.	124
SAFE PLACE.	124
SAFETY	
Canine.	396
Conduct.	151
Firearms.	63
First responder.	239
SAFETY EQUIPMENT	
Chaplains.	199
Seat belts.	498
SCRAP METAL THEFT INVESTIGATION.	362
SEARCH AND SEIZURE.	99
SEARCHES.	458
SEARCHES	
Administrative.	494
Crime scene.	239
SEARCHING	
Dead Bodies.	180
SECURITY	
Personnel records.	504
SOCIAL MEDIA.	217
SPIT HOODS.	39
STANDARDS OF CONDUCT.	145
SUBPOENAS.	167
SUPERVISION DEPLOYMENTS.	21

South Saint Paul Police Department

S Saint Paul PD Policy Manual

South Saint Paul Police Department Policy Manual

SUPERVISION STAFFING LEVELS.	21
SUSPICIOUS ACTIVITY REPORTING.	330

WATCH COMMANDERS.	280

T

TAKE HOME VEHICLES.	398
TATTOOS.	526
TECHNOLOGY USE.	155
TEMPORARY MODIFIED-DUTY ASSIGNMENTS.	539
TRAFFIC Enforcement.	347
TRAFFIC CITATIONS.	347
TRAFFIC FUNCTION.	347
TRAINING.	429
Anti-Retaliation.	481
TRAINING Canine.	89
Communicable disease.	487
Control devices.	45
Custody.	457
Firearms.	64
First amendment assemblies.	319
Personnel records.	503
Rapid response and deployment.	266
TRAINING, Searches.	462

U

UNIFORM REGULATIONS.	527
UNIFORMS Chaplains.	199
UNITY OF COMMAND.	17
USE OF SOCIAL MEDIA.	217

V

VEHICLE MAINTENANCE.	393
VEHICLES Inventory.	354
Towing.	353
VIDEO RECORDINGS First amendment assemblies.	314

W

WASHING OF VEHICLES.	394