Chapter 8 - Support Services

Crime Analysis

800.1 PURPOSE AND SCOPE

Crime analysis should provide currently useful information to aid operational personnel in meeting its tactical crime control and prevention objectives by identifying and analyzing methods of operation of individual criminals, providing crime pattern recognition and providing analysis of data from field interrogations and arrests. Crime analysis can be useful to the Department's long-range planning efforts by providing estimates of future crime trends and assisting in the identification of enforcement priorities.

800.2 DATA SOURCES

Crime analysis data is extracted from many sources including, but not limited to:

- Crime reports
- Field Interviews
- Parole and probation records
- Computer Aided Dispatch data
- Officer activity logs
- Department of Public Safety - Crime Records Service
- Partner agency crime data

800.3 CRIME ANALYSIS FACTORS

The following minimum criteria should be used in collecting data for crime analysis:

- Frequency by type of crime
- Geographic factors
- Temporal factors
- Victim and target descriptors
- Suspect descriptors
- Suspect vehicle descriptors
- Modus operandi factors
- Physical evidence information

800.4 CRIME ANALYSIS DISSEMINATION

For a crime analysis system to function effectively, information should be disseminated to the appropriate units or persons on a timely basis. Information that is relevant to the operational and tactical plans of specific line units should be sent directly to them. Information relevant to the development of the Department's strategic plans should be provided to the appropriate staff units. When information pertains to tactical and strategic plans, it should be provided to all affected units.

Transit Control Center

802.1 PURPOSE AND SCOPE

This policy establishes guidelines for the communications between the Metro Transit Police Department and the Transit Control Center. It addresses the immediate information needs of the Department in the course of its normal daily activities and during emergencies.

802.2 COMMUNICATION OPERATION

It is the policy of the Metro Transit Police Department to provide 24-hour telephone service to the public for information and for routine or emergency assistance. The Department provides two-way radio capability for continuous communication between Transit Control Center and department members in the field.

802.3 TRANSIT CONTROL CENTER SECURITY

The communications function is vital and central to all emergency service operations. The safety and security of Transit Control Center, its members and its equipment must be a high priority. Special security procedures should be established in a separate operations manual for Transit Control Center.

Access to Transit Control Center shall be limited to Transit Control Center members, the Shift Supervisor, command staff and department members with a specific business-related purpose.

802.4 RESPONSIBILITIES

802.4.1 COMMUNICATIONS SUPERVISOR

The Transit Control Center (TCC) is lead by a Communications Supervisor. The Communications Supervisor should work in conjunction with Police Administration or the authorized designee.

802.5 CALL HANDLING

Utilizing local agencies, the communications center provides members of the public with access to the 9-1-1 system for a single emergency telephone number.

When a call for services is received, the dispatcher will reasonably and quickly attempt to determine whether the call is an emergency or non-emergency, and shall quickly ascertain the call type, location and priority by asking four key questions:

- Where?
- What?
- When?
- Who?

The dispatcher will then relay information to the Metro Transit Police staff.

802.5.1 EMERGENCY CALLS

A call is considered an emergency when there is an immediate or potential threat to life or serious property damage, and the timely arrival of public safety assistance is of the utmost importance. A person reporting an emergency should not be placed on hold until the dispatcher has obtained all necessary information to ensure the safety of the responding department members and affected individuals.

Emergency calls should be dispatched immediately. The Shift Supervisor shall be notified of pending emergency calls for service when department members are unavailable for dispatch.

802.5.2 NON-EMERGENCY CALLS

A call is considered a non-emergency call when there is no immediate or potential threat to life or property. A person reporting a non-emergency may be placed on hold, if necessary, to allow the dispatcher to handle a higher priority or emergency call.

The reporting person should be advised if there will be a delay in the dispatcher returning to the telephone line or when there will be a delay in the response for service.

802.6 RADIO COMMUNICATIONS

The police radio system is for official use only, to be used by dispatchers to communicate with department members in the field. All transmissions shall be professional and made in a calm, businesslike manner, using proper language and correct procedures. Such transmissions shall include, but are not limited to:

(a) Members acknowledging the dispatcher with their radio identification call signs and current location.

(b) Dispatchers acknowledging and responding promptly to all radio transmissions.

(c) Members keeping the dispatcher advised of their status and location.

(d) Member and dispatcher acknowledgements shall be concise and without further comment unless additional information is needed.

Should radio procedure violations or other causes for complaint occur, all complaints and violations will be investigated and reported to the complainant’s supervisor and processed through the chain of command.

802.6.1 FEDERAL COMMUNICATIONS COMMISSION COMPLIANCE

Metro Transit Police Department radio operations shall be conducted in accordance with Federal Communications Commission (FCC) procedures and requirements.

802.6.2 RADIO IDENTIFICATION

Radio call signs are assigned to department members based on factors such as duty assignment, uniformed patrol assignment and/or member identification number. Dispatchers shall identify themselves on the radio with the appropriate station name or number, and identify the department member by his/her call sign. Members should use their call signs when initiating communication with the dispatcher. The use of the call sign allows for a brief pause so that the dispatcher

can acknowledge the appropriate department member. Members initiating communication with other law enforcement or support agencies shall use their entire radio call sign, which includes the department station name or number (e.g., "Transit 210").

802.7 DOCUMENTATION

It shall be the responsibility of Transit Control Center to document all relevant information on calls for service or self-initiated activity. Dispatchers shall attempt to elicit, document and relay as much information as possible to enhance the safety of the member and assist in anticipating conditions that may be encountered at the scene. Desirable information would include, at a minimum:

- Incident control number.
- Date and time of request.
- Name and address of the reporting person, if possible.
- Type of incident reported.
- Involvement of weapons, drugs and/or alcohol.
- Location of incident reported.
- Identification of members assigned as primary and backup.
- Time of dispatch.
- Time of the responding member’s arrival.
- Time of member’s return to service.
- Disposition or status of reported incident.

802.8 CONFIDENTIALITY

Information that becomes available through Transit Control Center may be confidential or sensitive in nature. All members of Transit Control Center and the Metro Transit Police Department shall treat information that becomes known to them as confidential and release that information in accordance with the Protected Information Policy.

Automated data, such as DVS records, warrants, criminal history information, records of internal police files or medical information, shall only be made available to authorized law enforcement personnel. Prior to transmitting confidential information via the radio, an admonishment shall be made that confidential information is about to be broadcast.

802.9 CPR TRAINING

Members authorized to answer calls for service shall be trained in providing CPR by telephone or transferring calls to the appropriate member or agency (Minn. Stat. § 403.03, Subd. 2).

Property and Evidence Office

804.1 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/procedures from the Metro Transit Police Department.

804.1.1 PROPERTY AND EVIDENCE SECURITY

The Property and Evidence Unit shall maintain secure storage and control of all property necessitating custody by the Department. The property and evidence technician(s) reports to the Administrative supervisor and is responsible for the security of the Property and Evidence. Property and Evidence keys/pass codes are maintained only by the property and evidence technician(s), Administrative supervisor, Investigative supervisor. An additional key is in a sealed and initialed envelope maintained in the safe in the office of the Chief of Police. The property and evidence technician(s) and others shall not loan Property and Evidence keys/pass codes to anyone and shall maintain them in a secure manner.

Any individual entering the Property and Evidence room other than the property and evidence technician(s) must be accompanied by the property and evidence technician (or authorized party).

804.2 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.

804.3 PROPERTY HANDLING

Any employee who first comes into possession of any property, shall retain such property in his/her possession until it is properly inventoried and placed in the designated property locker or storage room. 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).

An officer arresting a person for burglary, robbery or a 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 his/her 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. The property documentation must be completed to document the release of property not inventoried. The owner shall sign the documentation acknowledging receipt of the item(s) and officers should photograph the property if possible.

804.3.1 PROPERTY BOOKING PROCEDURE

All property must be inventoried prior to the employee going off-duty. Employees inventorying 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) Complete an evidence/property label and attach it to each package or envelope in which the property is stored.

(c) 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.

Officers shall pay particular attention to bags and/or backpacks entering the Property and Evidence Unit. Perishable items shall be discarded and items such as medication, currency/coin etc., shall be counted and inventoried separately. Officers shall make a notation in their report if they inventory medication, currency/coin or other noteworthy item(s). The Property and Evidence Technician receiving these items shall double check that the above procedure has occurred.

804.3.2 CONTROLLED SUBSTANCES

All controlled substances shall be inventoried separately from drug paraphernalia.

The officer seizing the narcotics and dangerous drugs shall place them in the designated property locker (typically the "drop" locker). All narcotics shall be inventoried at the Metro Transit Police Department.

804.3.3 EXPLOSIVES

Officers who encounter a suspected explosive device shall promptly notify the immediate supervisor or the Shift Supervisor. The local agency Bomb Squad, or contracted 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.

804.3.4 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 inventorying.

(b) License plates found not to be stolen or connected with a known crime, should be inventoried as found property. The Property and Evidence Office Unit may attempt to contact the registered owner or return the license plates to the Minnesota Department of Driver and Vehicle Services.

(c) All bicycles and bicycle frames require a property report. Property labels will be securely attached to each bicycle or bicycle frame. The property may be released directly to the property and evidence technician, or placed in the bicycle storage area until a property and evidence technician can log the property.

(d) All currency shall be counted in the presence of another officer and the money envelope initialed by both officers. A supervisor shall be contacted for cash in excess of $250. The supervisor shall also witness the count, and will initial and date the property documentation and specify any additional security procedures to be used.

1. All currency shall be counted by a minimum of two officers. The currency shall be placed into a money envelope which will then be secured with evidence tape and initialed by both officers.
2. Any currency over the amount of $250 must be verified by a Supervisor and the Supervisor must initial the money envelope.
3. Property and Evidence technicians receiving money envelopes shall place them into the safe.

(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 report.

Metropolitan Council / Metro Transit property, unless connected to a known criminal case, should be released directly to the appropriate Metropolitan Council / Metro Transit department. No labelal inventorying is required. In cases where no responsible person can be located, the property should be inventoried for safekeeping in the normal manner.

804.3.5 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).

(b) Members accepting surrendered firearms should complete a standardized Firearms Proof of Transfer form, if available. If a standard form is not available, use an Evidence/ Property form 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. MTPD 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 Property and Evidence Office 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 Property and Evidence Office 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.

804.4 PACKAGING OF PROPERTY

Packaging will conform to the Property and Evidence Office Packaging Manual maintained by the Property and Evidence Office Unit. Certain items require special consideration and shall be inventoried separately as follows:

(a) Controlled substances

(b) Firearms (ensure they are unloaded and inventoried separately from ammunition).

(c) Property with more than one known owner

(d) Drug paraphernalia

(e) Fireworks

(f) Contraband

804.4.1 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. If the proper property storage containers are not available, officers are asked to improvise a package keeping the safety of the officer as well as Property and Evidence Unit staff in mind.

A property report label shall be attached to the outside of all items or group of items packaged together.

804.4.2 PACKAGING CONTROLLED SUBSTANCES

The officer seizing controlled substances shall retain such property in his/her possession until it is properly weighed, packaged and placed in the designated storage locker (typically the "drop" locker). Prior to packaging and if the quantity allows, a presumptive test should be made on all suspected controlled substances. If conducted, the results of this test shall be included in the officer's report (e.g. positive or inconclusive).

Controlled substances shall be packaged in an envelope/evidence bag of appropriate size. The inventorying officer shall initial the sealed envelope and initial the evidence tape used to seal the package if applicable. Controlled substances shall not be packaged with other property.

The inventorying officer may weigh the suspected narcotics or dangerous drugs in the container in which it was seized. A full description of the item, along with packaging and total weight of the item as seized, will be placed in the case report.

804.4.3 RIGHT OF REFUSAL

The property and evidence technician has the right to refuse any piece of property that is not properly documented or packaged. Should the property and evidence technician refuse an item, he/she shall maintain secure custody of the item in a temporary property locker and inform the supervisor of the submitting officer.

804.5 RECORDING OF PROPERTY

The property and evidence technician receiving custody of evidence or property shall be responsible for tracking those items. The tracking of items is completed using the records management system (RMS).

Any changes in the location of property held by the Metro Transit Police Department shall be noted in the RMS.

804.6 PROPERTY CONTROL

Each time the property and evidence technician receives property or releases property to another person, he/she shall enter this information into the RMS. Officers desiring property for court shall, if possible, contact the property and evidence technician at least one week prior to the court day.

804.6.1 RESPONSIBILITIES OF OTHER PERSONNEL

Every time property is released or received, an appropriate entry shall be made within the RMS to maintain the chain of possession. No property or evidence is to be released without first receiving written authorization from a supervisor or investigator.

Officers requesting analysis for items other than controlled substances shall confer with an investigator regarding the details of the case.

804.6.2 TRANSFER OF EVIDENCE TO CRIME LABORATORY

The transporting employee will check the evidence out of property, indicating the date and time in the RMS and the request for laboratory analysis.

The property and evidence technician releasing the evidence must complete the required information in the RMS. 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 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 a copy of the receipt from the lab shall be returned to the Property and Evidence Unit for filing with the case.

804.6.3 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 in the RMS, stating the date, time and to whom it was released.

The property and evidence technician 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 RMS, indicating date, time and the person who returned the property.

804.6.4 AUTHORITY TO RELEASE PROPERTY

The property and evidence technician shall not release any evidence without approval from an authorized member of the Department. The Investigation Division shall authorize the disposition or release of all evidenccoming into the care and custody of the Department (unless the item is only being held for safekeeping).

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 and evidence technician 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.

804.6.5 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 all property shall be properly documented in RMS.

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 60 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) shall be properly disposed. The final disposition of all such property shall be fully documented in related reports.

A property and evidence technician 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 in the RMS.

Upon release or other form of disposal, the proper entry shall be recorded.

804.6.6 STOLEN OR EMBEZZLED PROPERTY

Stolen or embezzled property or property believed to be stolen or embezzled that is in the custody of this department shall 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 Property and Evidence Unit.

(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.

804.6.7 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.

804.6.8 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.

804.7 DISPOSITION OF PROPERTY

All property with an identified owner and/or an owner that has been notified, must be held for at least 60 days. If the owner is notified and fails to claim the property within the 60 days, it may be disposed of in compliance with existing laws and in accordance with Metro Transit's Property Retention Policy. The property and evidence technicians shall request a disposition or status on all property being held in conjunction with a pending criminal investigation or proceeding that has been held in excess of 60 days and for which no disposition has been received from a supervisor or investigator.

If the property owner is not located or is unknown, the property is deemed abandoned and may be disposed of after 30 days.

804.7.1 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)).

804.7.2 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 section 804.8, Minn. Stat. § 345.38 and Minn. Stat. § 345.75).

804.7.3 RETENTION OF BIOLOGICAL EVIDENCE
The Property and Evidence Office Unit Supervisor shall ensure that no biological evidence held by the Department is destroyed without adequate notification to the following persons, when applicable:

(a) The defendant

(b) The defendant's attorney

(c) The appropriate prosecutor

(d) Any sexual assault victim

(e) The Criminal Investigations Command Supervisor

Biological evidence shall be retained for a minimum period established by law, the Property and Evidence Office Unit 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 Criminal Investigations Command 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 Property and Evidence Office Unit Supervisor determines that such destruction is consistent with Minn. Stat. § 590.10 and the above notices have been made.

804.8 REPORT OF ABANDONED PROPERTY (MONEY)
The Property and Evidence Unit supervisor shall complete an annual report of presumed abandoned property as described in law to the Commissioner of Commerce. The report is to cover the 12-month period ending July 1 each year and is to be filed before October 31 each year (Minn. Stat. § 345.41).

804.9 INSPECTIONS OF THE PROPERTY AND EVIDENCE
On a routine basis, the Administrative Division supervisor shall inspect the evidence storage facilities and practices to ensure adherence to appropriate policies and procedures.

(a) Unannounced inspections of evidence storage areas shall be conducted annually as directed by the Chief of Police.

(b) An audit of evidence held by the Department may be conducted by a person(s) who is not routinely or directly connected with evidence control, as assigned by the Chief of Police.

(c) Whenever a change is made in personnel who have access to the Property and Evidence Unit, an inventory of all evidence/property shall be made by an individual(s) not associated with the Property and Evidence Unit or function to ensure that records are correct and all evidence property is accounted for.

(d) A quarterly audit of all property contained in the safe shall be conducted by a person who is not routinely or directly connected with evidence control. These audits shall be documented.

Records Section Procedures

806.1 PURPOSE AND SCOPE

The Records Supervisor shall maintain the Department Records Section Procedures Manual on a current basis to reflect the procedures being followed within the Records Section. Policies and procedures that apply to all employees of this department are contained in this chapter.

806.1.1 NUMERICAL FILING SYSTEM

Case reports are filed numerically within the Records Section by Records Section personnel.

Reports are numbered commencing with the last two digits of the current year followed by a sequential number beginning with 000001 starting at midnight on the first day of January of each year. As an example, case number 10-000001 would be the first new case beginning January 1, 2010.

806.2 FILE ACCESS AND SECURITY

All reports including, but not limited to, initial, supplemental, follow-up, evidence and all reports related to a case shall be maintained in a secure area within the Records Section, accessible only to authorized Records Section personnel. The Metro Transit Police Department currently utilizes an online based reporting system which is maintained by an outside vendor. Access to that system is granted by the Metro Transit Police Department and different levels of access are granted to authorized users.

806.2.1 REQUESTING ORIGINAL REPORTS

Should a copy of a report be needed for any reason (other than an officer's copy), the requesting party shall be referred to Records Section personnel. All released reports provided by the Metro Transit Police Department shall be recorded in the Dissemination tab of the online reporting system of the individual case. If an employee is not aware of when a report may be released, the individual requesting a copy of the report shall be directed to Records Section personnel.

806.3 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).

Records Maintenance and Release

810.1 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.

810.1.1 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).

810.2 POLICY

The Metro Transit 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).

810.3 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 command 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).

810.4 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.

810.4.1 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)).

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.

810.5 RELEASE RESTRICTIONS

Example 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.
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.

(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, 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.
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 Prosecuting 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).

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).

810.6 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 Prosecuting Attorney or the courts.

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.

810.7 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.

810.8 EXPUNGEMENT

A petition for expungement and expungement orders received by the Department shall be reviewed for appropriate action by the Custodian of Records.

810.8.1 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).

810.8.2 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.

810.9 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

812.1 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 Metro Transit 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.

812.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the Metro Transit 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.

812.2 POLICY

Members of the Metro Transit 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.

812.3 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.

(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.

(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 Metro Transit 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).

812.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Metro Transit 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 fingerprint 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.

812.5 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 Maintenance and Release 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.

812.5.1 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)).

812.5.2 REVIEW OF COMPREHENSIVE INCIDENT-BASED REPORTING SYSTEM (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.

812.6 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:

(a) Developing and maintaining security practices, procedures and training.

(b) Ensuring federal and state compliance with the Criminal Justice Information System (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.

812.6.1 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).

812.7 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 authorized access and use of protected information, as well as its proper handling and dissemination.

812.8 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 Metro Transit, 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 email.

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).

Criminal Justice Information Systems (CJIS)

813.1 PURPOSE AND SCOPE

The primary purpose of this policy is to educate and clarify Criminal Justice Information Systems (CJIS) policy and procedures for all MTPD employees, sworn and civilian.

It is our intent as an agency to follow the most current published CJIS security policy.

813.2 LOCAL SECURITY POLICY (REFERENCE CJIS POLICY 1.3)

The Police Department maintains a copy of the current version of the Criminal Justice Information System's Security Policy. The agency uses the policies in connection with both other Metro Transit Police Department policy and Metropolitan Council policies. In the case there are contradictory policies, the Police Department follows the CJIS Security Policy.

813.3 PERSONAL INFORMATION (REFERENCE CJIS POLICY 4.3)

For the purposes of this policy, 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 that 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. For example, a criminal history record 8/4/2014 CJISD-ITS-DOC-08140-5.3 13 inherently contains PII as would a Law Enforcement National Data Exchange (NDEx) case file. PII shall be extracted from CJI for the purpose of official business only.

The Police Department will continue to develop policies based on state and local privacy laws to ensure appropriate controls are applied when handling PII extracted from CJI.

813.4 INFORMATION MANAGEMENT (REFERENCE CJIS POLICY 5.1.1)

The Police Department's use of CJI is only for the purpose of the agency and its employees abilities to perform their job duties. Any disseminating or sharing of CJI with anyone that is not authorized to have access to the information is strictly prohibited.

813.5 INFORMATION HANDLING (REFERENCE CJIS POLICY 5.1.1.1)

The Police Department handles information according to local and state guidelines. The Police Department adheres to CJIS Policy section 5.8 relating to media protection.

813.6 INCIDENT RESPONSE (REFERENCE CJIS POLICY 5.3)

The agency will promptly report incident information to the appropriate party.

The agency will disconnect the infected workstation(s), server(s), and/or networking equipment.

The agency will maintain all records around information security events.

Other information collected for completing the Incident Response Form is below:

- Suspected cause for incident (name of the malware, virus, etc.)
- Was antivirus software running at the time of infection?
- HOw and when was the problem first identified?
- When was IT staff notified?
- How many workstations are infected?
- Is there any other equipment infected?
- What is the action plan for removal?
- Was any CJIS data or personal identification information compromised?

Once the system is free from infection, it can be reconnected.

813.7 ACCESS CONTROL (REFERENCE CJIS POLICY 5.5.2.21)

Each Police Department user shall be uniquely identified and shall not have shared credentialed access to information systems in order to provide non-repudiation for all logged or log-able activity. The Police Department shall not allow multiple concurrent active sessions for one user identification unless authorized in writing by the LASO on a case-by-case basis. These authorizations by the LASO can be by individual or role-based on specific operational needs.

813.8 REMOTE ACCESS (REFERENCE CJIS POLICY 5.5.6)

The Police Department shall authorize, monitor, and control all methods of remote access to the information system. The Police Department shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The Police Department shall control all remote accesses through managed access control points.

The Police Department may permit remote access for privileged functions only for compelling operational needs and shall document the rationale for such access.

The Police Department will comply with section 5.5.6 of the CJIS Security Policy.

813.9 PERSONALLY-OWNED INFORMATION SYSTEMS (REFERENCE CJIS POLICY 5.5.6.1)

The Police Department does not allow any personally-owned devices that can store agency information.

813.10 AUTHENTICATION STRATEGY (REFERENCE CJIS POLICY 5.6.2)

The Police Department adopts CJIS Security Policy 5.6.2.

813.11 AUTHENTICATOR MANAGEMENT (REFERENCE CJIS POLICY 5.6.3.22)

The agency requires that its users shall take responsible measures to safeguard authenticators issued to the, including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

813.12 MEDIA PROTECTION (REFERENCE CJIS POLICY 5.8)

The agency will do the following:

- Securely store electronic and physical media within a physically secure or controlled area.
- Restrict access to electronic and physical media to authorized individuals.
- Ensure that only authorized users remove printed for or digital media.
- Physically protect media at the end of life.
- Ensure end of life media is destroyed or sanitized.
- Not utilize public accessible computers to access, process, store, or transmit media.
- Store all hardcopy CJI printouts in a secure area accessible only to those employees who job function requires them to handle such documents.
- Safeguard all media against possible misuse.
- Take appropriate action when in possession of CJI when not in a secure area.

The agency will ensure that media at rest (i.e. store electronically) outside the boundary of the physically secure location shall be protected using encryption that is certified to meet FIPS 140-2 standards.

The agency will require users t lock or log off their computer when not in immediate vicinity of their work area to protect access.

813.13 ELECTRONIC MEDIA SANITIZATION AND DISPOSAL (REFERENCE CJIS POLICY 5.8.3)

The Police Department will ensure that the sanitization of electronic media or the destruction of inoperable media (via incineration, shredding, disintegrating, cutting, drilling, or grinding) is witnessed or carried out only by authorized personnel and that a chain of custody is maintain.

The Police Department will require for the sanitization of media that the data cleaning be done with an approved disk wiping utility using a minimum of three passes or a Security Service (NSA-CSS)-approved degausser.

813.14 DISPOSAL OF PHYSICAL MEDIA (REFERENCE CJIS POLICY 5.8.4)

The agency will ensure that the disposal of physical media is done through physical destruction via incineration, shredding, disintegrating, cutting, drilling, or grinding. The agency will ensure this is carried out by authorized personnel or a responsible contractor. A chain of custody will be kept for

all media disposed of. If any media is disposed of that isn't encrypted, only CJIS-vetted personnel will be allowed to maintain control of the media until disposal.

813.15 PHYSICAL PROTECTION (REFERENCE CJIS POLICY 5.9)

The Police Department will limit who has access to the physically secure location to only those personnel authorized by the agency. The agency will position information system devices and documents in such a way as to prevent unauthorized individuals from access and view.

813.16 ENCRYPTION (REFERENCE CJIS POLICY 5.10.2.3.35)

The Police Department will adhere to CJIS Security Policy 5.10.2.3. The agency utilizes an internal certificate authority that is configured and maintained by authorized employees of the Metropolitan Council to user certificates for smart card authentication. This system issues and revokes user certificates based on new user requests and user termination requests that are submitted by the agency. The certificate authority is owned and maintained by the agency.

813.17 VOICE OVER INTERNET PROTOCOL (REFERENCE CJIS POLICY 5.10.1.41)

The Police Department will maintain the VoIP phone system on a separate VLAN (Virtual Local Area Network) to segment phone traffic from all other network traffic. All VoIP phones will be on a separate network jack from all other network traffic and network computers will not be allowed to be connected to VoIP phones. All VoIP phones will have their administrative passwords changed from the factory default password. CJI will not be discussed over VoIP that is not encrypted with the FIPS 140-2 protocol.

813.18 PATCH MANAGEMENT (REFERENCE CJIS POLICY 5-10.1.41)

The Police Department will adhere to CJIS Policy 5.10.4.1.

813.19 SECURITY ALERTS AND ADVISORIES (REFERENCE CJIS POLICY 5.10.4.43)

The Police Department reviewed information system security alerts/advisories on a regular basis.

The Police Department issues alerts/advisories to the appropriate personnel.

The Police Department documents the types of actions to be taken in response to security alerts/ advisories.

The Police Department used automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

813.20 PERSONNEL SANCTIONS (REFERENCE CJIS POLICY 5.12.4)

If the Police Department becomes aware of an employee potentially using CJI in a manner that is not in accordance with the employee's job, the Police Department's Internal Affairs Unit will initiate

an investigation. The agency's TAC and LASO will be consulted during the process to assist with the determination of proper or improper use.

The Police Department will act on the findings of the Internal Affairs investigation in accordance to department policy and, if applicable, union contracts.

813.21 WIRELESS ACCESS RESTRICTIONS (REFERENCE CJIS POLICY 5.13)

The Police Department will deploy a VPN solution to all mobile devices that will ensure compliance with the FIPS 140-2 encryption standard when connection to systems containing Criminal Justice Information (CJI). The Police Department will not maintain a wireless system that allows a direct connection to systems containing CJI. Any wireless systems that the Police Department maintains will be controlled and all activity will be monitored.

813.22 REVIEW OF WI-FI LOGS (REFERENCE CJIS POLICY 5.13.1.113)

The LASO will review Wi-Fi logs on a recurring basis, not to exceed monthly. The agency shall not use (WEP and WPAx) to directly access criminal justice network environments without using a NIST-certified FTIPS 140-2 encryption tunnel. Any wireless networks connected or utilized will be segmented from the Police Department's criminal justice environment.

813.23 BLUETOOTH (REFERENCE CJIS POLICY 5.13.1.3)

The Police Department understands the risks of the use of Bluetooth devices. The Police Department will weigh the risk against operational objectives and employ the security measures possible to secure Bluetooth devices deemed to be necessary.

Any Bluetooth devices used to directly access CJI will be approved by the BCA prior to use. Any Bluetooth devices necessary to perform agency operations will be approved by the LASO prior to its use.

813.24 INCIDENT RESPONSE (REFERENCE CJIS POLICY 5.13.5)

The Police Department will react in a expedited manner when mobile devices are misplaced or stolen. The process will be:

1. The staff member must immediately notify the agency LASO and/or TAC if a device is misplaced or stolen, and an agency incident report will be completed.
2. If a device is stolen, immediately attempt to locate the device using available technology and determine the locked state of the device.
3. If a stolen device can be located using technology, a remote lock command will be immediately executed. If an investigation will not be commenced to locate the device and/or the suspects, a remote wipe command will be executed.
4. If a device is misplaced, determine if the device is in a locked state and locate it using available technology; immediately execute a lock command.
5. If the device is misplaced and we are unable to determine what state the device is in, a remote wipe command will be executed.

6. If a device is misplaced or stolen, the LASO will take the appropriate action up to and including notifying the BCA.

Computers and Digital Evidence

814.1 PURPOSE AND SCOPE

This policy establishes procedures for the seizure and storage of computers, personal communications devices (PCDs) digital cameras, digital recorders and other electronic devices that are capable of storing digital information; and for the preservation and storage of digital evidence. All evidence seized and/or processed pursuant to this policy shall be done so in compliance with clearly established Fourth Amendment and search and seizure provisions.

814.2 SEIZING COMPUTERS AND RELATED EVIDENCE

Computer equipment requires specialized training and handling to preserve its value as evidence. Officers should be aware of the potential to destroy information through careless or improper handling, and utilize the most knowledgeable available resources. When seizing a computer and accessories the following steps should be taken:

(a) Photograph each item, front, back and surrounding desktop or office setup, specifically including cable connections to other items. Look for a telephone line or cable to a modem for Internet access.

(b) Do not overlook the possibility of the presence of physical evidence on and around the hardware relevant to the particular investigation such as fingerprints, biological or trace evidence and/or documents.

(c) If the computer is off, do not turn it on.

(d) If the computer is on, do not shut it down normally and do not click on anything or examine any files.

1. Photograph the screen, if possible, and note any programs or windows that appear to be open and running.
2. Disconnect the power cable from the back of the computer box or if a portable notebook style, disconnect any power cable from the case and remove the battery.

(e) Label each item with case number, evidence sheet number and item number.

(f) Handle and transport the computer and storage media (e.g., tape, discs, memory cards, flash memory, external drives) with care so that potential evidence is not lost.

(g) Lodge all computer items into the Property and Evidence Office. Do not store computers where normal room temperature and humidity is not maintained.

(h) At minimum, officers should document the following in related reports:

1. Where the computer was located and whether it was in operation.
2. Who was using it at the time.

3. Who claimed ownership.

4. If it can be determined, how it was being used.

(i) In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all storage devices (e.g., printers, remote drives, hard drives, tape drives and disk drives) should be seized along with all media.

814.2.1 BUSINESS OR NETWORKED COMPUTERS

If the computer belongs to a business or is part of a network, it may not be feasible to seize the entire computer. Cases involving networks require specialized handling. Officers should contact a certified forensic computer examiner for instructions or a response to the scene. It may be possible to perform an on-site inspection, or to image the hard drive only of the involved computer. This should be done by someone specifically trained in processing computers for evidence.

814.2.2 FORENSIC EXAMINATION OF COMPUTERS

If an examination of the contents of the computer's hard drive, floppy disks, compact discs or any other storage media is required, forward the following items to a computer forensic examiner:

(a) Copy of report(s) involving the computer, including the Evidence/Property sheet.

(b) Copy of a consent to search form signed by the computer owner or the person in possession of the computer, or a copy of a search warrant authorizing the search of the computer hard drive for evidence relating to investigation or other legal authority for examination.

(c) A listing of the items to search for (e.g., photographs, financial records, E-mail, documents).

(d) A forensic copy of the media will be made, and subsequent forensic examination of the copy will be conducted by a trained digital forensic examiner.

814.3 SEIZING DIGITAL STORAGE MEDIA

Digital storage media including hard drives, floppy discs, CDs, DVDs, tapes, memory cards or flash memory devices should be seized and stored in a manner that will protect them from damage.

(a) If the media has a write-protection tab or switch, it should be activated.

(b) Do not review, access or open digital files prior to submission. If the information is needed for immediate investigation request the Property and Evidence Office to copy the contents to an appropriate form of storage media.

(c) Many kinds of storage media can be erased or damaged by magnetic fields. Keep all media away from magnetic devices, electric motors, radio transmitters or other sources of magnetic fields.

(d) Do not leave storage media where they would be subject to excessive heat such as in a parked vehicle on a hot day.

(e) Use plastic cases designed to protect the media, or other protective packaging, to prevent damage.

814.4 SEIZING PCDS

Personal communication devices such as cellular telephones, PDAs or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device including messages, stored data and/or images.

(a) Officers should not attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Unsent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages.

(b) Do not turn the device on or off. The device should be placed in a solid metal container such as a paint can or in a Faraday bag, to prevent the device from sending or receiving information from its host network.

(c) When seizing the devices, also seize the charging units and keep them plugged in to the chargers until they can be examined. If the batteries go dead all the data may be lost.

814.5 DIGITAL EVIDENCE RECORDED BY OFFICERS

Officers handling and submitting recorded and digitally stored evidence from digital cameras and audio or video recorders will comply with these procedures to ensure the integrity and admissibility of such evidence.

814.5.1 COLLECTION OF DIGITAL EVIDENCE

Once evidence is recorded it shall not be erased, deleted or altered in any way prior to submission. All photographs taken will be preserved regardless of quality, composition or relevance. Video and audio files will not be altered in any way.

814.5.2 SUBMISSION OF DIGITAL MEDIA

The following are required procedures for the submission of digital media used by cameras or other recorders:

(a) The recording media (e.g., smart card, compact flash card or any other media) shall be brought to the Property and Evidence Unit as soon as reasonably possible for submission into evidence.

(b) Officers are not authorized to review or copy memory cards. The evidence technicians are the only employees authorized to copy and/or distribute digital media made from the memory cards.

(c) As soon as reasonably possible following the collection of evidence, the camera operator is to remove the memory card from his/her digital camera and place the card into a plastic carrier (if available). The camera operator shall write their name, related

case number and any additional requested information on the Evidence Photo Log Form before placing the card into the drop locker along with the evidence form.

(d) Evidence technicians will make a copy of the memory card using appropriate storage media. Once they have verified that the images properly transferred to the storage media, the technicians will erase the memory card for reuse. The storage media will be marked as the original.

(e) Officers requiring a copy of the digital files must request a copy on the evidence form when submitted to evidence.

814.5.3 DOWNLOADING OF DIGITAL FILES

Digital information such as video or audio files recorded on devices using internal memory must be downloaded to storage media. The following procedures are to be followed:

(a) Files should not be opened or reviewed prior to downloading and storage.

(b) Where reasonably possible, the device should be connected to a computer and the files accessed directly from the computer directory or downloaded to a folder on the host computer for copying to the storage media.

814.5.4 PRESERVATION OF DIGITAL EVIDENCE

(a) Only evidence technicians are authorized to copy original digital media related to case documentation that is held as evidence. Only digital forensic examiners are authorized to copy original media seized as evidence. The original digital media shall remain in evidence and shall remain unaltered.

(b) Digital images that are enhanced to provide a better quality photograph for identification and investigative purposes must only be made from a copy of the original media.

(c) If any enhancement is done to the copy of the original, it shall be noted in the corresponding incident report.