James E. White
Chief of Police

D P D 568 (rev 06/21)

INTER-OFFICE MEMORANDUM
PROFESSIONAL DEVELOPMENT BUREAU

Date: February 27, 2024

To: Chief of Police James E. White (Through Channels)

Subject: **SUBMISSION OF SPECIFICATION REPORT – SURVEILLANCE VAN**

From: Deputy Chief Mark Bliss, Professional Development Bureau

Attached for your review and approval is the Specification Report for the Surveillance Van. This report is to comply with the Community Input Over Government Surveillance (CIOGS) Ordinance. The Specification Report has been reviewed and approved by Director Robert Millender, of the Department of Innovation and Technology (DoIT) and Director Stephen Lamoreaux of Informatics. This report needs approval from the Chief of Police and the Board of Police Commissioners before submission for a public hearing on the matter.

MARK BLISS
Deputy Chief
Professional Development Bureau

Attachments:

1. Specification Report – Surveillance Van
2. Manual Directive 102.2 – Bias-Based Policing
3. Manual Directive 101.11 – Record Retention Schedule
4. Manual Directive 101.12 – Data Sharing, Retention and Dissemination

APPROVED
FEB 29 2024
ASSISTANT CHIEF
OFFICE OF FIELD SUPPORT

APPROVED
MAR 04 2024
CHIEF OF POLICE
OFFICE OF THE CHIEF

#477
PDB
02/27/24

Specification Report – Surveillance Van

Sec. 17-5-453: Surveillance Technology Specification Reports.

(a) The Police Department certifies that the information contained in this document reflects the complete and accurate proposed use of the surveillance technology.

(b) This report has been approved by the Chief of Police and received the approval of the Board of Police Commissioners on _____.

(1) ***Description:*** Information describing the surveillance technology and its capabilities.

- The Detroit Police Department (DPD) seeks undercover van technology to assist in sensitive investigations. The Burke Services upgrade to the existing undercover van will replace existing technology and will replicate existing capabilities.
- The system consists of cameras monitoring all sides of the van and three pan tilt zoom (PTZ) cameras to monitor publicly visible areas from streets where the van will be parked. Internal network equipment connects the cameras to an onboard laptop computer with viewing and control software. Video will be recorded to an onboard external hard drive. Recorded video can be exported by connecting a USB drive. Two monitors will be mounted in the van for viewing cameras. A modem will be connected to the internal network for secure remote camera viewing and control. External microphones and connective components allow officers in the van the ability to monitor activity outside of the van. A printer will be installed in the van. All network and antennas will be installed. Illumination will be attached to the exterior of the van. Power will be supplied by a rechargeable battery system.

(2) ***Purpose:*** Any specific purpose the surveillance technology is intended to advance:

- The purpose of the surveillance van provides the ability of to conduct covert surveillance necessary for the investigation of various crimes. Surveillance vans are used in the investigation of crimes including, but not limited to, homicide, narcotics operations, human trafficking, and illegal dumping. The surveillance van may also be used for investigations originating out of Professional Standards.

(3) ***Deployment:*** If the surveillance technology will not be uniformly deployed or targeted throughout the City, what factors will be used to determine where the technology is deployed or targeted.

- The Detroit Police Department will deploy the surveillance van when there is a situation as described above, to keep the community, its residents, and first responders safe. Additionally, the surveillance van can be used to gain real time situational awareness by viewing and sending live video to remote locations for evaluation and tactical decision making.

(4) ***Fiscal Impact:*** The fiscal impact of the surveillance technology.

- The upgrade of the surveillance van will cost the Detroit Police Department $80,000.00 to complete. This is a one-time fixed cost for the upgrade and there are no additional costs.

(5) ***Civil Rights / Liberties Impacts:*** An assessment identifying with specificity;

(a) Any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and

- Video technology does not intrude upon any constitutionally protected areas.
- Misuse of video technology or any information collected is strictly prohibited.

(b) What specific, affirmative measures will be implemented to safeguard the public from the potential adverse impacts identified in this section.

- The Police Department will strictly enforce its policies pertaining to the use of this video technology and any information obtained from the technology.

(6) ***Authorized use:*** A complete description of the purpose and intended uses of the surveillance technology, including any uses that will be expressly prohibited.

The purpose and intended uses of the proposed technology includes:

- Apprehension of suspects and fugitives;
- Furthering criminal investigations; and
- Other legitimate law enforcement purposes.

The following uses of the technology are expressly prohibited:

- Traffic enforcement;
- Enforcement of civil laws, including immigration laws; or
- Use of the video technology for purposes other than legitimate law enforcement activities.

(7) ***Data Collection:***

(a) What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology;

- The surveillance van will provide visual, audio and video data on a location or individual.

(b) What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data; and

- After careful consideration, the DPD cannot determine any instance or situation where legally protected information may be collected from the proposed technology.
- Data from the surrounding areas may be collected during the use of the surveillance van.
- All inadvertently collected audio/video data will be deleted within thirty (30) days from the main hard drives with no copies being created.

(c) How inadvertently collected surveillance data will be expeditiously identified and deleted.

- After careful consideration, the DPD cannot determine any instance or situation where legally protected information may be collected from the proposed technology.
- In the event protected information is collected through the misuse of the technology, the Police Department will cause for its deletion as soon as feasible.
- Upon identifying that protected information has been collected through the misuse of technology, DPD will report the following to the Board of Police Commissioners within 15 days of its discovery:

  i. Type of information collected;

ii. Date range of the collection;
iii. Extent of impact (i.e., how many person's information was collected);
iv. DPD members who had access to the information; and
v. Date and method of destruction, once it has been destroyed.

(8) ***Data Protection:*** What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms.

- The Detroit Police Department will comply with the State of Michigan Criminal Justice Information System (CJIS) regulations and other applicable standards and policy to protect data. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related Department activity. Additionally, video transmitted from the van will use an encrypted IPSEC tunnel. This ensures that data cannot be intercepted or decrypted by unauthorized individuals.

(9) ***Data Retention:*** Insofar as the privacy of the public can be severely compromised by the long-term storage of mass surveillance data, what rules and procedures will govern the retention of surveillance data, including those governing:

(a) The limited time period, if any, surveillance data will be retained. Such information shall include a statement explaining why the designated retention period is no greater than that which is absolutely necessary to achieve the specific purpose(s) enumerated in the Surveillance Technology Specification Report;

- The DPD will adhere to its Data Retention Policy, which matches the requirements set forth in the corresponding state statute.

(b) The specific conditions that must be met to retain surveillance data beyond the retention period identified pursuant to Subsection (b)(9)(a) of this section; and

- Data will not be retained beyond the retention period except where such information constitutes evidence of a crime related to an open case,a closed case where prosecution and / or appeals remain pending, or a civil case where litigation/or appeals remain pending..

(c) The process utilized to regularly delete surveillance data after the retention period stated in Subsection (b)(9)(a) of this section has elapsed and the auditing procedures that will be implemented to ensure data is not improperly retained.

- The Police Departments policies and procedures allow for the retention of video recordings for up to 30 days. Recordings that contain evidence of incidents are retained until the case is solved, closed, and litigation ends.

(10) ***Surveillance Data Sharing:*** If a City department is seeking authorization to share access to surveillance technology or surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, or non-governmental persons or entities in the absence of a judicial warrant or other legal mandate, it shall detail:

(a) Which governmental agencies, departments, bureaus, divisions, or units, or non-governmental persons or entities will be approved for:

i. Surveillance technology sharing to the governmental agency, department, bureau, division, or unit, or non-governmental person or entity, and

ii. Surveillance technology sharing from the governmental agency, department, bureau, division, or unit, or non-governmental person or entity, and

iii. Surveillance data sharing to the governmental agency, department, bureau, division, or unit, or non-governmental person or entity;

(b) Where applicable, the type of information of surveillance data that may be disclosed to the governmental agency, department, bureau, division, or unit, or non-governmental person or entity; and

(c) Where applicable, any safeguards or restrictions that will be imposed on the surveillance technology or data receiving governmental agency, department, bureau, division, or unit, or non-governmental person or entity regarding the use or dissemination of the provided surveillance technology or data;

- DPD has a Data Sharing Policy (101.12) that sets forth the standard the Department must follow when sharing data.
- DPD will also comply with any constitutional applicable law and Criminal Justice Information System (CJIS) policies.

(11) Demands for Access to Surveillance Data: What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.

- The Police Department will only share information with government entities or third parties in accordance with a duly authorized data sharing agreement. Under no circumstances is a member of the Police Department authorized to share information for the purpose of assessing immigration status or enforcing immigrations laws.

(12) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Technology Specification Report is followed, including what independent persons or entities will be given oversight authority, if and how regular audits will be conducted, and in the case of the Police Department, also how the Board of Police Commissioners will be involved in the auditing and oversight process.

- The Detroit Police Department will include the surveillance van in the annual Surveillance Technology and Surveillance Use Reports. Additionally a weekly usage report will be sent to the Board of Police Commissioners.

(13) Training: Would specialized training be required in connection with the use of the surveillance technology.

- All members will be vetted, CJIS cleared, and trained in all the technology that they are assigned to use in the surveillance van. In addition, members are required to comply with Record Retention (101.11), Data Sharing (101.12), Bias-Based Policing (102.2) and all other policies as it relates to technology and standards of conduct.

(14) Complaints: What procedures will allow members of the public to register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and how the City department will ensure each question and complaint is responded to in a timely manner.

- The policies and procedures of the Detroit Police Department require that upon receiving notice of the desire to file a complaint, a member of the Department must involve a supervisor as soon as possible to receive the complaint. In addition, any citizen may lodge a complaint

directly with the Office of the Chief Investigator. Questions regarding the technology may be directed to the Office of the Chief of Police.

Series	Effective Date	Review Date	Directive Number
100 Administration	10/23/2021	Three Years	102.2
Chapter 102 – Standards of Conduct			
Reviewing Office *Office of the Chief of Police*			☐ New Directive ☒ Revised Revisions in *italics*
References			

BIAS-BASED POLICING

102.2 - 1 PURPOSE

The purpose of this directive is to unequivocally state that racial and ethnic profiling in law enforcement is totally unacceptable. This directive reaffirms the Detroit Police Department's commitment to unbiased policing in all its encounters between Department members and citizens, and reinforces procedures that serve to maintain public confidence and trust through the delivery of services in a fair and equitable fashion.

102.2 - 2 POLICY

The Detroit Police Department is committed to protecting the constitutional and civil rights of all citizens. Allegations of bias-based profiling or discriminatory practices, real or perceived, are detrimental to the relationship between the police and the communities the Detroit Police Department protects and serves, because they strike at the foundation of public trust. This trust is essential to effective community-based policing. Bias-based policing is an illegal and ineffective method of law enforcement. Bias-based policing results in increased safety risks to Department members and citizens and the misuse of valuable police resources. While recognizing that the majority of Detroit Police Department members perform their duties in a professional, ethical, and impartial manner, this Department is committed to identifying and eliminating any instances of bias-based policing.

102.2 - 3 Definition

102.2 - 3.1 Bias-Based Policing

The differential treatment of individuals in the context of rendering police service based on a suspect's classification or the member's perception of any such classification, such as appearance, race, ethnic background, gender *or gender-related identity*, sexual orientation, religion, economic status, age, cultural background, *immigration status, national origin,* or English language proficiency. Bias-based policing may also be defined as any police-initiated action that relies on any characteristic other than the behavior, conduct, unlawful act or omission of that individual, or information that leads the police to a particular individual.

102.2 - 3.2 English Language Proficiency

The ability of someone to speak, read, write or understand the English language at a level that allows such person to interact effectively.

102.2 - 3.3 Gender Identity or Expression

An actual or perceived gender-related identity, appearance, expression, or behavior of an individual, regardless of the designation of gender on one's birth certificate, driver's license, or state or municipal identification.

102.2 - 4 Procedure

102.2 - 4.1 Member Responsibility

1. All investigative detentions, traffic stops, arrests, searches, and seizures of property by Department members will be based upon a standard of reasonable suspicion or probable cause as required by the Fourth Amendment of the United States (U.S.) Constitution and statutory authority. Members must be able to articulate specific facts, circumstances, and conclusions, which support reasonable suspicion or probable cause for an arrest, traffic stop, or investigative detention.
2. Members must be able to articulate specific facts, circumstances, and conclusions that support reasonable suspicion or probable cause for any search or seizure, including but not limited to, traffic stops. All searches and seizures must be based on the standard of reasonable suspicion (investigatory detentions) or probable cause (searches) as required by the Fourth Amendment of the U. S. Constitution and statutory authority.
3. Members may consider the reported race, ethnicity, or national origin of a specific suspect or suspects in the same way they would use specific information regarding height, weight, hair color, etc., about specific suspects.
4. Police service will be provided to all persons without regard to race, ethnic background, gender, gender identity, sexual orientation, religion, economic status, age, English language proficiency, or cultural group.
5. During citizen contact, misunderstandings may occur from the member's failure to explain why contact was made. The member should inform individuals of their reason for contact.
6. Nothing in this section shall limit a member's ability to interview witnesses or discourage routine conversations with citizens not suspected of an offense.
7. Any member who has a reasonable opportunity must act to prevent or stop any member from violating this procedure and report it to their supervisor (refer to 102.11 Duty to Intervene).

102.2 - 4.2 Supervisory Responsibility

1. Supervisors should ensure that members assigned under their command are familiar with this policy and comply with its provisions.
2. Supervisors should monitor the activities of members under their command to ensure that bias-based policing is not practiced.

102.2 - 4.3 Complaint Process

Supervisors that receive a citizen complaint or allegation of bias-based policing on the part of members under their command, or any other member of this Department, shall forward such information in writing in accordance with this Department's directives regarding citizen complaints and internal investigations.

102.2 - 4.4 Training

All Department members receive initial cultural diversity and awareness training at the basic recruit-training academy. Additionally, training regarding interaction with citizens, policy, ethics, legal requirements, and related topics shall be integrated into the basic recruit-training program for all new members and as part of in-service training programs.

102.2 - 4.5 Compliance Reporting

Planning, Research, and Deployment shall conduct a quarterly audit of self-initiated traffic stops to determine if there are any racial disparities. Any potential racial disparity shall be determined by comparing the demographics of the community living in the precinct with the demographics of the individuals being stopped. A copy of this report shall be forwarded to each relevant Precinct Commander, Deputy Chief, and Assistant Chief. The Board of Police Commissioners shall receive an annual report of the bias-based policing audit.

Series	Effective Date	Review Date	Directive Number
100 Administration	08/16/2019	Annually	101.11
Chapter 101 - Organization and Management			
Reviewing Office *Planning, Research, and Deployment*			☐ New Directive ☒ Revised Revisions in *italics*
References			

RECORD RETENTION SCHEDULE

101.11 - 1 PURPOSE

The purpose of this policy is to provide procedures for the Detroit Police Department's (DPD) record retention system.

101.11 - 2 POLICY

Public records are the property of the people of the State of Michigan. As a result, government agencies are responsible for ensuring that the public records they create and receive while conducting public business are retained and destroyed in accordance with Michigan law. The Detroit Police Department has adopted the State of Michigan's General Schedule #11 Retention and Disposal schedule for local law enforcement agencies.

101.11 - 3 Definitions

Auditable Form or Log

The term "auditable form" or "auditable log" means a discrete record of the relevant information maintained separate and independent of blotters and other forms maintained by the Department.

Public Records

The Michigan Freedom of Information Act (FOIA) (Public Act 442 of 1976, as amended) defines public records as recorded information "prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function, from the time it is created."

101.11 - 4 Procedures

Abandoned Vehicle Notice - 2 years

These records document vehicles that are abandoned and/or impounded. They may include photographs, data describing the vehicle, TR-52 "Notice of Abandoned Vehicle" forms, and requests from wrecker companies.

101.11 Record Retention Schedule

Accident Reports - 3 years
These records document accidents reported to the Michigan State Police on the UD-10 "Uniform Traffic Crash Report" form. The retention is Pursuant to MCL 257.622.

Accounts Receivable Records – 6 years
These records document money received for restitution payments and may include transactions and daily balances.

Activity Logs - 3 years
These are daily activity logs of members deployed to the field or who are required to complete a DPD Activity Log.

Administrative Subject Files – 5 years after close of topic
These records document various topics, issues, projects or activities that an agency/member is involved in. They may include, but may not be limited to, topical reference files about issues, strategic planning files for the agency, or specific initiatives, and special projects files. Document types may include correspondence, memoranda, reports, research, articles, meeting notes, and related background materials. Subject files do NOT include case files, human resource files, accounting records and other specific function-based records.

Administrative Training Schedule - 5 years
This record documents in-house and external training. It lists the date, course title, and training hours received.

Alarm Billings - 2 years
These records document the billing for alarms and false alarms that *members* respond to. They may include billings, statements, and/or receipts.

American Disability Act (A.D.A.) Files – 3 years after employment ends
These records document compliance with the Americans with Disabilities Act. They may include, but may not be limited to, member's medical records, criminal history checks, background checks, driving record, workers compensation information, disability information, and credit report.

Animal Control - 7 years
These records document activity associated with animal control. They may include complaints and the Destruction of Animal *Report* (DOA) (DPD 669).

Animal Control – Citations - 3 years
These records document the issuance of animal control citations. If the citation is not paid, these records are passed onto the district court so a warrant or fine can be issued.

101.11 Record Retention Schedule

Annual Reports - PERMANENT
This is the agency's copy of the annual report, submitted each year to document what activities and events have taken place.

Arrest/*Detention Log Data* - *5* years
These records *identify people who were arrested. They may include, but may not be limited to, names, dates, charges, and disposition.*

Assigned Vehicle Maintenance (DPD251) - 1 year

Assumption of Risk (See Ride along Waiver)

Bank Statements - 6 years
These statements are used to document money that is received and then deposited for preliminary breath tests, vehicle fines, bonds, etc.

Blood Alcohol Content (BAC) Logs - 3 years
These records document the evidentiary breath test administered to a suspect, and includes the Evidential Breath Test Log (OD-33) and BAC Data master Simulator Logs.

Bicycle *Registrations* - 5 years
These records are used to recover stolen bicycles. They may include the owner's name, contact information, bicycle description, serial number, and license tag number.

Bond Receipts - 1 year
These receipts document the payment of bail bonds. The form is a three (3) part document. One (1) copy is issued to the bonder, one (1) copy is forwarded to the courts, and the agency retains one (1) copy. The form identifies the person's name, case number, charges, date, appearance information and the amount of bail.

Budget Information - 6 years
These records are used to develop annual budgets. They identify the amount that was requested and eventually approved. The documents may include proposals, salary information, projected overtime reports, *and* vehicle and equipment needs/assessments.

Building Plans - PERMANENT
These documents are used to construct and maintain buildings and other infrastructure. They may include building plans, blueprints, key charts, drawing plans and diagrams of the office/jail, *security system information, and emergency plans. Buildings include buildings owned by the law enforcement agency and buildings the law enforcement agency provides security for.*

101.11 Record Retention Schedule

Calendars – 2 years
These records document members' work schedules, activities, and tasks. The may include, but may not be limited to, automated or manual planners and calendars.

Committee Records - 2 years
These documents are from the various internal committees associated with the office, such as the Awards Committee. They may include membership lists, agendas, supporting documentation, minutes, reports, etc.

Complaints – Citizens - 2 years
These records document any complaints filed by citizens against a *member*. They document what action, if any, was taken.

Computer Aided Dispatch (CAD) Log - 2 years
These computer log reports are printed from the CAD system by Communications Operations. They document all calls that a *member* was dispatched *to*. The report summarizes the type of call, who responded, incident number generated, date, and time. They are used to support incident reports and various activities.

Contracts – EXP + 6 years (EXP = date contract expires)
These contracts document an agreement between the agency and anyone else. They may be used for services such as jail housing, medical examiners, jail doctors, medical personnel, police services, students, union labor, training and vendors.

Correspondence – Departmental - 2 years
This is general correspondence from various staff members within the Department. This correspondence is arranged chronologically or by correspondent name.

Correspondence - Various Groups/Organizations - 2 years
These records consist of various correspondence received from, and associated with, outside groups and/or organizations.

Court (Investigator) Case Files - 25 years
These records identify people who were arrested, and the charges that were filed against them. They may or may not contain copies of witness statements, subpoenas, photos, negatives, mug shots, incident reports, tickets, narratives, correspondence, statements, line up documentation, elimination prints, warrants, etc.

Daily Detail Sheet - 5 years
These records document who is on duty each day when roll call is taken.

Destruction of Records, Interoffice Memorandum (DPD568) – PERMANENT

Detainee Forms (See Holding Cell Forms or Logs)

Disciplinary Case Files – PERMANENT

Dispatch/911 Recordings – 90 days
Communications Operations shall be responsible for all recordings for the 90-day retention period. Any command that requests audio records shall be responsible for ensuring it is retained using the same retention policy as paper records and are part of the physical files.

Disposition of Department Property/Equipment – ACT + 5 years (ACT = until item is disposed)
These documents detail equipment/property donated or disposed of with a value over $500.00.

Discovery Orders - 1 year
These are copies of discovery orders submitted by attorneys for information related to cases.

Drug Forfeiture Records - 7 years
These records document the seizure of property related to drug traffic/offenses, pursuant to MCL 333.7524. The records may contain descriptions of what was seized (titles, deeds, etc.) and the disposition of the item(s).

Drug Screen Notification – 1 year

Equipment Maintenance Records – Until equipment is no longer in use
These records document the maintenance of equipment used by law enforcement agencies. They may include, but may not be limited to, manuals, calibration documentation, repair documentation, information about replacement parts and supplies, and supporting documentation.

Equitable Sharing Program Information – 5 years
These documents include, but are not limited to, receipts and procurement documentation for all expenditures of shared funds, bank statements, Forms DAAG-71, TD-F, ESACs, accounting and bookkeeping documents, logs and records, bank records and statements, and audit reports (Guide to Equitable Sharing for State, Local, and Tribal Law Enforcement, July 2018).

101.11 Record Retention Schedule

Evidence Property Records - *Retain until related incident report is destroyed*
These records document what property has been logged in and out of the evidence storage area. They may include, *but may not be limited to, the receipt number, case number, and complaint number.*

Expunged Records Information - 3 years
These records document what records have been expunged. They may contain the name, charge, date and related correspondence.

Event/Meeting Summary Form – 1 year

Facility Access Data – 2 years
These records document employees who used a badge or key card to access a building or other type of facility. Data may include, but may not be limited to, location that was accessed, employee information, and date/time of access.

Field Training Observations (FTO) – EVT + 2 years (EVT = when the probation period ends)
These records are completed during a new *member's* training period. They document their performance, and areas needing improvement during their probation period. They may include copies of daily observations, weekly summaries, activity logs, tickets, UD-10's, case reports, warrants, property receipts, etc.

Fingerprint Cards - *ACT + Five (5) Years (ACT = Can be disposed of when they are no longer needed for reference purposes)*
These records document fingerprints that are collected. They may include, but may not be limited to, Arrest/Fingerprint Cards (RI-07) that are used to submit fingerprints to the Michigan State Police pursuant to P.A. 289 of 1925, *and* other laws. *Note: Michigan State Police (MSP) is the official record keeper for fingerprints. The fingerprints retained by local law enforcement agencies (i.e. DPD) should be convenience copies, and they can be destroyed in compliance with General Schedule #1.*

Freedom of Information Act (FOIA) Requests - 1 year
This file will document any requests for information or public records. They may include requests for information, correspondence, a copy of the information released, and billing information.

Gem Dealer Information – 1 year (If there are no investigations)
P.A. 95 of 1981 requires dealers of precious metal or gems to register with local law enforcement and to supply transaction information regarding sales to police agencies. MCL 445.484 authorizes destruction of the transaction records after 1 year, if there is no investigation on the precious items involved in the transaction.

101.11 Record Retention Schedule

General Orders and Policies - PERMANENT
These records document internal policies, general orders, and Department orders issued by the Chief. They may contain official bulletins that are used to convey information to *Department members*.

Grant Records *Received* – ACT + 7 years (ACT = until grant is closed by the grantor)
These records may contain the application, financial reports, progress reports, and final reports for grants received. The grants may include, but are not limited to UHPCOPS, DARE Program, Training Grants, Equipment Grants, Federal Grants, Matching Grants, etc.

Grants Denied – 1 year
These records document grants the law enforcement agency applied for, but were denied. They may include, but may not be limited to, applications and supporting documentation.

Grievance Files - 7 years
These are copies of grievances filed against union contracts.

Holding Cell Forms or Logs - 7 years

Incident (Case) Reports - Non-Criminal - 3 years
These reports document non-criminal incidents. These records may include copies of UD-10's "Uniform Traffic Crash Report," computer printouts, written reports, statements, photos, negatives, crime lab reports, copies of warrants, affidavit of warrant, DI-177 "Breath, Blood, Urine Test Report," DI-93 "Refusal to be Tested," LEIN breath entry, Blood Alcohol Content report, Blood Alcohol Content Data Master, supplemental reports, court disposition, receipts, OWI cost recovery, case logs, discovery request, attorney request, affidavit for search warrants, homicide reports, liquor inspection reports, driver re-exam request, diagrams, *and interrogation video recordings. Classification is assigned according to what the person was charged with doing, not what they pled to.*

Incident (Case) Reports – Misdemeanor - 7 years
These reports document misdemeanor incidents. These records may include copies of UD-10's "Uniform Traffic Crash Report," computer printouts, written reports, statements, photos, negatives, crime lab reports, copies of warrants, affidavit of warrant, DI-177 "Breath, Blood, Urine Test Report," DI-93 "Refusal to be Tested," LEIN breath entry, Blood Alcohol Content report, Blood Alcohol Content Data Master, supplemental reports, court disposition, receipts, OWI cost recovery, case logs, discovery request, attorney request, affidavit for search warrants, homicide reports, liquor inspection reports, driver re-exam request, diagrams, *and interrogation video recordings.* All units must ensure when storing case records that all felonies and

misdemeanors are filed separately. *Classification is assigned according to what the person was charged with doing, not what they pled to.*

Incident (Case) Reports – Felony - 20 years
These reports document felony incidents. These records may include arrest records, copies of UD- 10's "Uniform Traffic Crash Report," computer printouts, written reports, statements, photos, negatives, crime lab reports, copies of warrants, affidavit of warrant, DI-177 "Breath, Blood, Urine Test Report," DI-93 "Refusal to be Tested," LEIN breath entry, Blood Alcohol Content report, Blood Alcohol Content Data Master, supplemental reports, court disposition, receipts, OWI cost recovery, case logs, discovery request, attorney request, affidavit for search warrants, liquor inspection reports, driver re-exam request, diagrams, *and interrogation video recordings.* All units must ensure when storing case records that all felonies and misdemeanors are filed separately. *Classification is assigned according to what the person was charged with doing, not what they pled to.*

Incident (Case) Reports – Homicide/*Felony CSC* - PERMANENT
These reports document homicide incidents *and criminal sexual conduct incidents. They may include, but may not be limited to, arrest records, copies of UD-10's "Uniform Traffic Crash Report," computer printouts, written reports, statements, photos, negatives, crime lab reports, copies of warrants, affidavit of warrant, DI-177 "Breath, Blood, Urine Test Report," DI-93 "Refusal to be Tested," LEIN breath entry, Blood Alcohol Content report, Blood Alcohol Content Data Master, supplemental reports, court disposition, receipts, OWI cost recovery, case logs, discovery request, attorney request, affidavit for search warrants, liquor inspection reports, driver re-exam request,* written reports, statements, photos, negatives, crime lab reports, copies of warrants, *diagrams, and interrogation video recordings. All units must ensure when storing case records that all felonies and misdemeanors are filed separately. Classification is assigned according to what the person was charged with doing, not what they pled to.* Specialized units who receive a special assignment regarding a homicide case *or criminal sexual conduct case shall* ensure all records are kept permanently.

Intake/Release Property Card/Form - 1 year
These records identify which personal property items were removed from an individual who is held by a city/township/village police agency prior to transfer to a county facility or release. They may include personal history information.

Internal Investigations - 5 years
Command internal administrative investigations (I&R's) not specifically listed in this directive.

101.11 Record Retention Schedule

Inventory (Current) - ACTIVE

Inventory Disposed - 3 years

Invoices – Original - 6 years
Invoices generated by the Department that document false alarms, police contract services, overtime, and licenses.

Job Applications-Not Interviewed/Not Hired - 1 year
These files, from individual applicants who were not interviewed, may include resumes, applications, and supporting documents.

Job Descriptions - SUP = until job description is superseded
These records document job classification systems and positions. They may include research, surveys, or reviews done to create job descriptions, as well as job classifications and selection criteria. Job descriptions may include a summary of responsibilities, functions, applicant requirements, and salary and benefit classifications.

Juvenile Arrest Records & Fingerprint Cards – ACT = until the juvenile's 17th birthday
These records are used to aid the tracking of juveniles. They may include a physical description of the youth, name, date of birth, date of emancipation, charge, disposition, photographs, fingerprints, court records, witness reports, incident reports, etc.

Letters of Clearance - 1 year
Letters are issued by an agency to a private citizen to show no criminal activity within the community.

License Plate Reader (LPR) Information – 1 year
These records document license plate information (images and metadata) that are collected by LPR devices to support investigations. They may include, but may not be limited to, plate information, location and GPS coordinates, time and date of image capture, and camera identification.

Litigation Files – ACT + 10 years (ACT = until case is closed)
These files document any litigation to which the Department or a *Department member* is a party. They may include depositions, transcripts, decisions, correspondence, data, exhibits, research materials, reports, press releases, media clippings, etc.

Liquor Inspection Records - 3 years
These records document establishments that sell or serve liquor. They contain quarterly inspection reports completed by *members* pertaining to the named

establishment (e.g. Daily Activity Report on Liquor, Vice and Gambling (D.P.D. 63), Monthly Summary of Liquor, Gambling and Vice Activity (DPD 419)).

Liquor License Establishment Records - ACT = While the establishment is in business
These files are used to monitor licenses issued to liquor establishments. They may include a copy of the actual liquor license that is issued by the Michigan Liquor Control Commission, drawings, background information, tax information, bank statements, birth certificates, LEIN printouts, etc.

LiveScan - Identification Database/Image System - *55 years*
This is an automated system used for capturing the fingerprints of individuals. Pictures may be produced from the system and affixed to folders or various paper work as needed. Retention reflects the need to migrate data from one system to the next.

MCOLES Certified Employee Separation Records – 50 years
These records document the reason for, and circumstances surrounding, a separation of service for members who are Michigan Commission on Law Enforcement Standards (MCOLES) certified. (MCL 28.563)

Meeting Records (Public Bodies) – PERMANENT
These records document the official activities of public bodies that are subject to the provisions of the Open Meetings Act, such as governing boards, community advisory bodies, etc. They include, but may not be limited to, meeting minutes, agendas, recordings, and documentation reviewed and considered for decision making during the meeting. Note: Recordings may be destroyed after the meeting minutes are approved.

Miscellaneous Business Licenses - ACT + *1 year* = While the establishment is in business
These records document businesses within a community that may be required by local ordinances to register with the agency. Examples include arcades, auction firms, massage facilities, spas, pawn shops, car shops, etc.

Monthly Assignment Sheet - 3 years

Monthly Equipment Inspection Sheet (DPD709) - 1 year

Monthly Worksheet - 2 years
This is a *monthly* summary of *patrol-related* activity completed by *each member individually* (e.g. Monthly Work Sheet - Patrol Officer (DPD194), Activity Summary - Patrol Vehicle (DPD279)).

101.11 Record Retention Schedule

Mutual Aid Agreements – ACT + 10 years (ACT = While the agreement is in place)
These are agreements executed between the Department and other agencies to provide mutual support as needed during a crisis or emergency.

Outside Employment (DPD525) - ACT = While employed by the Department
This form is completed by *members* who have a second job. It is authorized by the agency and used to identify any conflicts of interest.

Overtime Records - 2 years
These records document overtime used/submitted by *members* and are used to resolve any immediate issues with pay.

Pawn shop Slips - 3 years
These reports are completed by pawn shops and are submitted to the Department pursuant to P.A. 231 of 1945. They are used to aid in recovering stolen material.

Payroll Timesheets - 5 years
These are copies of timesheets that are completed and forwarded to the payroll office.

Personnel Information Records - ACT = While employed by the Department
These records are used as a reference tool for identifying *a member's* badge number, MITN number, phone number, address, seniority *date*, hire date, termination date, birthdays, etc.

Personnel Files – ACT + 7 years (ACT = While employed by the Department).
These files are maintained for each *member* and contain records that document all human resource related transactions that occurred during the *member's* period of active employment. They are used to record *member* performance (e.g. ratings, awards, training, outside employment application, personnel change forms, sick/vacation time, etc.).

Personal Protection Orders (PPO) - Until the expiration date on the PPO
These records are copies of personal protection orders issued by the court.

Photographs - Non-Criminal - 3 years
These are photographs of incidents, including crime scenes, accidents, evidence, mug shots, etc.

Photographs – Misdemeanor - 7 years
These are photographs of incidents, including crime scenes, accidents, evidence, mug shots, etc.

101.11 Record Retention Schedule

Photographs – Felony - 20 years
These are photographs of incidents, including crime scenes, accidents, evidence, mug shots, etc.

Pistol Purchase Permits/Registrations - 6 years
1. These records document individuals who apply for a Pistol Purchase Permit and individuals who have applied/passed and purchased a pistol. The records would include copies of the RI-10 "Purchase Permit" and the RI-11 "Safety Inspection Forms" that are forwarded to Michigan State Police (MSP) for registration and permanent retention. MCL 28.429 states that the RI-11 that is forwarded to the MSP is the permanent official record, and that the local agency shall retain a copy. MCL 28.422 requires that the RI-10 be kept for a period of 6 years by the local agency as the official record.
2. These records may also include the RI-9 "Dealer Application & License to Purchase." These are not CPL "Concealed Pistol License" records. CPL records are maintained by the County Clerk. The pistol test form should not be retained. Local agencies should never have any RI-60 "Pistol Sales Record" on file.

Position Interview Questions - SUP = Until questions are superseded
These documents contain a list of questions associated with the job descriptions. They are updated as the job descriptions are updated. The questions are used in the interview process to assure the same questions are asked to all candidates.

Prescription Drug Destruction Records – 3 years
These records document the weight of drugs received for destruction. They may include, but may not be limited to, the location, weight, activity dates, and people involved.

Promotional Results - ACT = While tests are active
These records contain information associated with test scores, test sheets, order of ranking, results of offsite testing, etc.

Radar Logs - 7 years

Receipt Books - 6 years
These books are used to document money received for preliminary breath tests, vehicle fines, bonds, etc.

Recordings *(Audio and Video)*
1. *Audio and/or video that is recorded using any type of device of routine surveillance/security, training, patrols, incidents, activities, red light violations, public space or crowd monitoring (i.e. individual holding cells, precinct video from parking lots/hallways/garage, etc.) shall be retained for thirty (30) days.*

Recordings that contain evidence of incidents are retained until the case is solved, closed, and litigation ends (MCL 780.316).

2. *In-car audio and video recordings, body-worn camera recordings, cellblock processing areas, hallways, and front lobbies shall be retained for ninety (90) days.*
3. *Body Worn Camera (Formal Complaints) shall be retained for three (3) years. If the body worn camera recording is relevant to a formal complaint against a law enforcement agency, the recording shall be kept for three (3) years (MCL 780.316). This retention period is in addition to the timeframe referenced in all other audio and video recordings (30 days).*
4. *If any of the above recordings are involved in litigations, retention shall be guided by the City of Detroit Law Department.*
5. *If any of the above recordings are involved in an internal investigation, retention shall be ten (10) years with Internal Affairs.*

Records Management Database System - 25 years
These systems are often used to track information associated with case processing, accident processing, dispatch case disposition, location, vehicle records, evidence logs, abandoned vehicles, administrative records, miscellaneous registrations, and permits. These systems may be linked to other systems, such as the Law Enforcement Information Network (L.E.I.N.) or M.I.C.R. systems. Retention reflects the need to migrate data from one system to the next.

Reprimand (DPD22 and DPD22b) – 2 years

Ride Along Waiver - 1 year
This is a waiver of liability signed by a citizen who rides with *Department members.* It is used to document the date and name of the person who participated.

Roll Call Training - 2 years
These documents contain miscellaneous information that is distributed to *members* at the beginning of each shift.

Salvaged Vehicle Report - 2 years
These records are generated by citizens who have applied for a Salvaged Vehicle Title.

Sex Offender Address Verification - SUP = Most recent Registration.
These are copies of the Michigan Sex Offender Registration form (DD-4) that is required by P.A. 295 of 1994 to register sex offenders. Information is entered into the Law Enforcement Information Network (L.E.I.N.) and used to track the location of these offenders.

101.11 Record Retention Schedule

Special Orders - 2 years
These are internal bulletins that are used to distribute information. Departments receiving the bulletins must sign to acknowledge receipt. These are reviewed annually to determine if they should become a Department Order or Policy.

Tamper Evident Envelope (TEE) - 1 year
These records document personal property removed from an individual being held in a holding facility or released, and may include personal history information.

Taxicab Permits – While Active
These are applications for taxicab driver permits. They identify the permits approved. Files may include the application, computer printouts, background checks, etc.

Temporary Details Report (DPD472) - 1 year

Tickets/Citations - *3* years
These are the *member's* copy of traffic citations that are issued. They are filed *by year* by the issuing *member*. They are used by the *members* when reporting to court and responding to the citation that was issued.

Ticket/Citation Book Receipts - 3 years
These records contain the ticket/citation numbers for the book, and the name of the officer that it was assigned to.

Ticket/Citation Logs - *3* years
These are registration logs of tickets issued. A copy is forwarded to the courts.

Traffic Crash Release Acknowledgement Forms – 2 years
These records document when someone obtains a traffic crash report within 30 days of a crash.

Training Bulletins - 2 years
These are internal bulletins that are used to notify a*n entity within the* Department or *individual members* that they are scheduled for upcoming training.

Training Files – ACT + 7 years (ACT = While employed by the Department)
These records are used to document any training *members* have received. They may contain training schedules, certificates, course descriptions, and receipts.

Training Fund - 5 years
These records document money available and spent from the training fund.

101.11 Record Retention Schedule

Unclaimed Monies - 6 years
These records document unclaimed money that is transferred to the treasury. It is deposited into the general fund.

Uniform Crime Reports - 6 years
These are reports generated from the Michigan State Police that contain crime statistics and other information.

Use of Force *Auditable Forms* and *Detainee Incidents within a Cellblock* – 10 years

- Review of Arrest Exception (UF-001);
- Use of Force (UF-002);
- SIR (UF-002a);
- Stop and Frisk (UF-003);
- Warrant Tracking (UF-004);
- Exceptions to Interview, Interrogations and Conveyances (UF-005);
- Detention of a Material Witness (UF-006);
- Holds Exceptions (UF-007); and
- Detainee Telephone and/or Visitor Exception Form (UF-008).

Vehicle Pursuit Forms (DPD665) – 7 years

Vehicle Tow by Private Tow (DPD73) or Impound or Release Form – 2 years
These forms are used to release vehicles that have been impounded. They document the complaint number, vehicle, wrecker agent, and release information.

Video Review Logs (DPD713 and713a) – 2 years.

Visitor Logs – 2 years
These records document individuals who visited the facility who are not employees. They may include, but may not be limited to, sign-in/out sheets or other records that contain the visitor's name and date/time of arrival and departure.

Warrants - ACT = While warrant is active and still in L.E.I.N.
Warrants are issued by the court/prosecutor and may include orders for release, protective conditions, case sheets, L.E.I.N. printouts, and Warrant/Vehicle Worksheets. Warrants are active until the suspect is arrested or the warrant is recalled by a court. Warrants are used to verify LEIN entries when audited. After the individual is arrested, they are turned over to the arresting authority or prosecutor.

Warrant Verification Log (DPD711) – 7 years

Witness Conveyance Form (DPD668) – 10 years

101.11 - 5 Retention and Destruction of Records

101.11 - 5.1 General

All commands shall be responsible for the accurate labeling and storage of its records during the retention period. The mass storage of records shall be by type and all information is to be clearly and legibly written on the file storage boxes. The following information shall be listed on the storage box:

- Contents;
- Start date of records;
- End date of records;
- Number of boxes (e.g., 1 of 3); and
- Destroy date.

101.11 - 5.2 Destruction of Records

The schedule for the destruction of Department records shall be instituted by the *Records Management* and implemented by Resource Management for a Department wide collection of expired records.

101.11 - 5.3 Command Responsibilities - Documentation of Records

Each command shall designate a member to assemble all available records from the command, which are eligible for destruction. The member shall prepare an Inter-Office Memorandum (DPD568) indicating each box with its contents and destruction date. The DPD568 shall be approved by the commanding officer before any records are removed for destruction. The command shall keep the original and forward a copy to the *Records Management*. The retention period for this memorandum shall be a permanent record at the command.

Series	Effective Date	Review Date	Directive Number
100 Administration	09/22/2016	Annually	101.12
Chapter 101 – Organization and Management			
Reviewing Office Planning and Deployment			☒ New Directive ☐ Reviewed
References			

DATA SHARING, RETENTION AND DISSEMINATION

101.12 PURPOSE

The purpose of this directive is to establish the guidelines and procedures for acquiring, accessing disseminating and retaining data stored in the Detroit Police Department's (DPD) computerized information systems, in addition to the following:

1. Delineates responsibilities for Department members when acquiring, entering, accessing disseminating and purging data;
2. Continues and expands established guidelines for the collection, storage, access dissemination and retention of computerized information;
3. Establishes policy and procedures for sharing computerized information with outside law enforcement and non-law enforcement agencies; and
4. Establishes mandates for compliance with title 28 Code of Federal regulations Part 23 (28 CFR Part 23) as it applies to Criminal Intelligence shared information by the Department with outside law enforcement agencies.

101.12-1 POLICY

The Detroit Police Department (DPD/Department) is committed to providing the public with professional and efficient service, in general – specifically, in addressing and investigating crime. To that end, the DPD employs various methods. Several of those methods result in capturing information and data deemed sensitive in nature and based on the content, is protected by established federal, state and local laws.

The DPD will also adhere to the following regarding its acquisition, retention and dissemination of ALL data:

- Entry of data into the Department's computerized systems will be restricted to authorized members;
- Department members will not purge any information stored in the Department's computerized information systems, unless explicitly authorized;

- Incidental sharing of data and information by an outside law enforcement agency will conform to the policies and procedures outlined in this Directive and will comply with 28 CFR 23.

101.12-2 COLLECTION AND ENTRY OF DATA AND INFORMATION

It is imperative that information and data gathered which is deemed as investigative and/or confidential in nature, and that is specifically intended to be entered into any Department computerized system by an authorized member, complies with the following criteria:

1. Department members will collect information in a lawful manner and in compliance with Department directives and applicable federal, state and local laws and policies.
2. Prior to submission for entry into the Department's computerized information systems, Department members making a submission will verify the information contained in the entry.
3. Members assigned to enter data will be responsible for accurately entering the data according to the prescribed guidelines.
4. Data entered into the Department's computer information systems is subject to the same level of supervisory review as is currently in place for reports submitted on formsets. Information will be attributed to the submitting officer(s).

   Department members will not retain information about any individual or organization gathered solely on the basis of religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation. Furthermore, under no circumstances is any member authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing Department owned resources.

101.12-2.1 Access to Computerized Information

A. Use by Department Members

- Access to information or files maintained in the Department's computerized information system is granted only when authorized; and
- Any member who accesses information through the Department's computerized information systems is accountable for the appropriate use and disposal of the information. Access to information is restricted to official police business.

- Additionally, the following system and network activities is strictly prohibited, with no exceptions:
    1. Unauthorized access, copying, or dissemination of classified or sensitive information (Criminal Justice Information, or CJI).
    2. Installation of any copyrighted software for which the Department or end user does not have an active license is strictly prohibited.
    3. Installation of any software, without preapproval and virus scan, is strictly prohibited.
    4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
    5. Revealing your account password to others or allowing use of your account by others.
    6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:
        a. accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

    7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to the Department.
    8. Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
    9. Circumventing user authentication or security of any host, network, or account.
    10. Interfering with or denying service to any user other than the employee's host.
    11. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
    12. Providing information about LEIN/NCIC or list of Department employees to parties outside the Department.

B. User Account – Access Validation

1. All user accounts shall be reviewed annually by the System Administrator or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information.
    a. The System Administrator or his/her designee may also conduct periodic reviews.

2. All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one (1) year or the work completion date, whichever occurs first.
    a. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.
3. The System Administrator or his/her designee should disable all new accounts that have not been accessed within 30 days of creation.
    a. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to information technology resources is required. In those instances, the individual going on extended leave should have a manager- approved request from the designated account administrator or assistant.)
4. The System Administrator or his/her designee must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.).
    a. If an individual is assigned to another office for an extended period (more than 90 days), the System Administrator or his/her designee will transfer the individual's account(s) to the new office (CJA).
    b. The System Administrator or his/her designee will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.
        i. Primary responsibility for account management belongs to the System Administrator or his/her designee.
5. The System Administrator or his/her designee shall:
    a. Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
    b. Periodically review existing accounts for validity, and Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

C. Remote Access by Outside Agency

The DPD may enter into agreements with outside agencies to provide limited remote access to its computerized information systems. Remote access to the Department's computerized information systems will only be permitted after compliance with the following:

- Must meet DoIT (Dept. of Innovation and Technology) requirements.

101.12-3 DISSEMINATION OF INFORMATION

Records, files or reports may be printed from computerized information systems and/or duplicated by Department personnel for Department use only, except as provided in this section.

A. The contents of any record, file or report will not be exhibited or divulged to any non-Departmental person or entity except in the performance of official duties and in accordance with Department policy, and applicable federal, state and local laws.

B. Public Release

1. Any information provided to the public will be released in accordance with Department directives and in compliance with federal, state and local laws.
2. Command staff members may release relevant information to community groups or private citizens, in compliance with Department directives and all federal, state and local laws (e.g. Clery Act, LEIN crash data, etc.)
3. For purposes of request(s) submitted under the Michigan Freedom of Information Act (the Act or FOIA), it should be noted that the data is "public record" within the meaning of the Act.
   a. Therefore, the data is public record and subject to disclosure, unless otherwise exempt from disclosure under the Act or other applicable statute.
   b. No data shall be disclosed or released to any third-party without the following:
      - A review by the DPD to verify that the data is the correct data requested; and
      - A review by the Law Department to make the necessary legal determination in cases where DPD requests data or attributes of data to be exempt from disclosure.

c. Labor Time and Costs under the Michigan Freedom of Information Act.
- Because locating and verifying the correct data can be time-consuming, and because the Act permits the City to request and to collect limited costs incurred by the City under certain circumstances, the DPD personnel who searches, retrieves, and review the data to verify the correctness shall keep track of his/her time spent in such actions and report the time spent to the Law Department when a copy of the recording is being delivered to the Law Department.
- The costs for the duplication of the data may only be charged by the Law Department in accordance with the Act.

NOTE: Department members may consult with the Office of Legal Affairs prior to dissemination of information to the public to determine if any prohibition on the release exists.

C. Incidental Sharing of Information with Outside Agencies

The Department recognizes that some criminal activity may affect multiple jurisdictions. Whenever possible, the Department will provide outside law enforcement agencies engaged in an active investigation access to information which is relevant to that investigation.

1. Department members receiving a request for information from an outside agency, whether in person, by phone or by fax, shall inform his/her immediate supervisor of the request.
2. Authorization shall be limited to the Chief of Police or a designee holding the rank of Captain or above.
3. The requesting agency and Chief of Police of the granting agency may enter into an interagency agreement, which will contain the following provisions:
   a. Execution of the agreement by the Chief of Police
   b. Complies with all applicable local, state and federal laws.
   c. These agreements shall expire on an annual basis.

101.12-4 SELF-CONTAINED INFORMATION SYSTEMS

Any unit that maintains investigative records or criminal intelligence information on a system that is self- contained is expressly prohibited from sharing any information contained on that system with any outside agency.

101.12-5 ACQUIRING AND RECEIVING INFORMATION

Information gathering and investigative techniques used by the DPD and information-originating agencies shall be in compliance and shall adhere to applicable regulations and guidelines, including, but not limited to:

- 28 CFR Part 23 regarding criminal intelligence information;
- Organization for Economic Co-operation and Development (OECD) Fair Information Practices;
- Applicable criminal intelligence information guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan; and
- Applicable constitutional provisions and the applicable administrative rules as well as any other regulations that apply to multi-jurisdictional criminal intelligence information databases.

1. External agencies that access and share data and information with DPD shall be governed by the laws and rules governing those individual agencies, as well as by applicable local, state and federal laws; and
2. DPD shall contract only with commercial database entities that provide an assurance that information gathering methods comply with applicable local, state and federal laws, as well as statutes and regulations.

101.12-6 RETENTION

Information in the Department's computerized information systems will adhere to the Department's Record Retention Schedule as delineated in the DPD manual, Directive 101.11, ***Record Retention,*** as well as all applicable federal, state and local laws.

101.12-6.1 Storage and Security

Members shall ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI. All necessary steps should be taken to prevent unauthorized access to this information.

101.12-6.2 Electronic Sanitization and Disposal

The Detroit Police Department (DPD) shall follow the following procedures when disposing of electronic data:

a. Sanitize, that is, overwrite at least (3) three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals;
b. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media; and
c. DPD shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures.

101.12-6.3 Breach Notification and Incident Reporting

DPD shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. 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.

101.12-6.4 Improperly Disclosed, Lost or Reported CJI Information

A. The following procedures must be followed:

1. The involved Department member shall notify his/her supervisor and an incident report must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)
2. The supervisor will communicate the situation to the Officer–in-Charge (OIC) of the Crime Intelligence Unit to notify of the loss or disclosure of CJI records.
3. The OIC will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
    a. 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.

b. 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.
c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

101.12-7 VIOLATIONS OF POLICY

Violations of this policy include, but are not limited to:

- Accessing data to which the individual has no legitimate right;
- Enabling unauthorized individuals to access data;
- Disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law;
- Inappropriately modifying or destroying data; and
- Inadequately protecting restricted data.

Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution or termination of employment.

101.12-8 LICENSE PLATE READERS

Automatic License Plate Recognition (ALPR) also refers to License Plate Reader (LPR) technology.

LPR provides automated detection of license plates. The LPR system consists of a high-speed camera, mounted either at a fixed location or on a mobile patrol vehicle, and a computer to convert data from electronic images of vehicle license plates into a readable format. The system then compares the information against specified databases of license plates. The system attaches camera identification, date, time, and location information, or GPS coordinates, to the digital image. The information is maintained electronically in a central location.

The digital image can include additional information such as:

- The vehicle's make and model;
- The vehicle's driver and passengers;
- Distinguishing features (e.g., bumper stickers, damage);
- State of registration

If a given plate is listed in the database, the system is capable of providing the vehicle's location, direction of travel, and the type of infraction related to the notification.

101.12 Data Sharing, Retention and Dissemination

101.12-8.1 USES OF LPR DATA

Identifying the intended uses of LPR data is critical in assessing any privacy and/or civil liberties implications due to the networking within LPR data collected by participating law enforcement agencies.

The Real Time Crime Center (RTCC) has, as one of its core missions, the sharing of information, thereby assisting law enforcement agencies in the fulfillment of their duties. LPR data may be used for, but is not limited to, the following purposes:

- Crime analysis;
- To alert law enforcement officials that a license plate number is on a list of targeted license plate numbers (Hot List) or is related to a criminal investigation and is found in the LPR database;
- To alert law enforcement officials that a license plate number on a hot list has been recorded by a fixed versus mobile camera, possibly requiring notification to law enforcement agencies in proximity or travel route of the identified vehicle; and
- To identify the movement of vehicles operated by individuals currently under an open criminal investigation.

101.12-8.2 PROCEDURES

LPR informational data files are periodically updated with different data sources being refreshed at different intervals. Therefore, it is important that LPR users take into account the potential for lag time between last update and an alert provided by the LPR system on a vehicle of interest or wanted vehicle. Any alert provided by an LPR system is to be considered informational and advisory in nature and requires further verification before action.

When alerted that a vehicle is wanted, stolen, or of interest to law enforcement, the mobile operator should, to the fullest extent possible, take the following steps:

1. Ensure the plate was read properly and that the state of origin is consistent with the alert.
2. Confirm the alert status by either manually entering the plate via the Mobile Data Computer (MDC) or requesting the check through dispatch.
3. Review the alert information to determine the nature of the advisory.

4. In the event that compelling circumstances are present or situational officer safety issues make it unsafe to confirm the status of the alert information prior to taking action, the operator must confirm the status of the alert information as soon as possible.
5. When action is taken on an alert vehicle, it is the responsibility of the person taking action to provide the appropriate disposition information so the system may be updated as necessary.
6. Only sworn law enforcement officers should engage in contacting occupants of stolen or wanted vehicles.