| Series | Effective Date | Review Date | Directive Number |
|---|---|---|---|
| 100 Administration | 09/22/2016 | Annually | 101.12 |
| **Chapter**<br>101 – Organization and Management | | | |
| **Reviewing Office**<br>Planning and Deployment | | | ☒ New Directive<br>☐ 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.