PLANNING AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

FOR SIGNATURE OF: James E. Craig, Chief of Police

TYPE OF DIRECTIVE: Manual Directive 307.4

SUBJECT: CRIMINAL JUSTICE INFORMATION SYSTEMS (CJIS)

ORIGINATED OR REQUESTED BY: Planning and Deployment

APPROVALS OR COMMENTS:
The above referenced directive is a new directive that is a Michigan State Police (MSP) mandated requirement for the Department in reference to the protection of Department criminal justice information (CJI). The information in this directive was provided to Planning and Deployment by the Department's Technical Support Division and the U.S. Department of Justice (Federal Bureau of Investigation) CJIS Policy.

APPROVED
JUL 10 2018
ASSISTANT CHIEF
ADMINISTRATIVE OPERATIONS

APPROVED
SEP 18 2018
SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

APPROVED
1ST ASSISTANT CHIEF
OFFICE OF THE CHIEF

RECEIVED
OCT 15 2018
BOARD OF POLICE COMMISSIONERS

AFTER THE DIRECTIVE IS APPROVED AND SIGNED, PLEASE RETURN TO PLANNING AND DEPLOYMENT.
1301 Third Street, 7th Floor, Detroit MI 48226

Series	Effective Date	Review Date	Directive Number
300 Support Services		Annually	307.4
Chapter 307 – Information System			
Reviewing Office Technical Support			☒ New Directive ☐ Revised
References: U.S. Department of Justice (Federal Bureau of Investigation) CJIS Policy			

CRIMINAL JUSTICE INFORMATION SYSTEMS (CJIS)

307.4 - 1 PURPOSE

The purpose of this directive is to provide information security requirements and guidelines for the Detroit Police Department for the creation, viewing, modification, transmission, dissemination, storage, and destruction of Criminal Justice Information (CJI).

307.4 - 2 POLICY

It is the policy of the Detroit Police Department that all Department members adhere to the security criteria set forth in this directive.

307.4 - 3 Acceptable Use

1. The Detroit Police Department (DPD) is committed to protecting its members from illegal or damaging actions that may occur knowingly or unknowingly by Department members when involved in CJI. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, File Transfer Protocol, and National Crime Information Center (NCIC) access are the property of the DPD. These systems are to be used for law enforcement purposes in serving the interests of the Department during normal operations.
2. It is the responsibility of every member to know these guidelines and to conduct their activities accordingly. Inappropriate or noncompliant use exposes the Department to risks including but not limited to virus attacks, compromises within the network systems and services, and could cause legal issues.
3. This policy applies to all Department members and any device used to access the Department's network.

307.4 - 3.1 General Use and Ownership

1. While Technical Support desires to provide a reasonable level of privacy, Department members should be aware that any data created on Department systems remains the property of the Detroit Police Department. Because of the need to protect the network,

Technical Support cannot guarantee the confidentiality of information stored on any network device belonging to the Detroit Police Department.

2. Any information that a member considers sensitive or vulnerable (i.e. residual LEIN, NCIC information on a computer terminal that has access to the internet, and CJIS information) *shall* be encrypted.
3. For security and network maintenance purposes, authorized members within the Department may monitor equipment, systems, and network traffic at any time.
4. The DPD reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

307.4 - 3.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Extranet-related systems shall be classified as either confidential (i.e. Criminal Justice Information (CJI), Department member's personal data) or non-confidential. Members shall take all necessary steps to prevent unauthorized access to confidential information.
2. Keep passwords secure and do not share accounts. Each Department member is responsible for the security of their passwords and accounts.
3. In accordance with the FBI CJIS Security Policy, all personal and Department computers, laptops, and workstations shall prevent further access to the Department's system by initiating a session lock after a maximum of 30 minutes of inactivity. Members shall directly initiate a session lock to prevent inadvertent viewing when a device is unattended.
4. All devices used by members that are connected to the DPD Internet/Intranet/Extranet, whether privately owned or property of the Department, shall be continually executing approved virus-scanning software with a current database.
5. Members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse codes.

307.4 - 3.3 Unacceptable

1. Under no circumstances is a Department member authorized to engage in any activity that is illegal under local, state, federal, or international law using Department resources. The following activities are strictly prohibited, with no exceptions:

    a. Unauthorized access, copying, or dissemination of classified or sensitive information (CJI);
    b. Installation of any copyrighted software for which the Department does not have an active license;
    c. Installation of any software without prior approval from a member's commanding officer;
    d. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, logic bombs, etc.);
    e. Revealing an account password to other Department members or sharing an account with another member;

f. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which a member is not an intended recipient, or logging into a server that a member is not expressly authorized to access, unless doing so within the scope of their regular duties (i.e. System Administrator, Technical Support). For the purpose of this policy, the following are examples of "disruption":

- Network sniffing
- Pinged floods
- Packet spoofing
- Denial of service
- Forged routing information for malicious purposes

g. Port scanning or security scanning unless prior notification has been given to the Department;
h. Executing any form of network monitoring that would intercept data not intended for the member's host, unless this activity is a part of the member's regular duties;
i. Circumventing user authentication or security of any host, network, or account;
j. Interfering with or denying service to another Department member;
k. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a member's terminal session, via any means, locally or via the Internet/Intranet/Extranet; and
l. Providing information about LEIN/NCIC or a list of Department members to parties outside the DPD.

2. The following activities are included as violations of acceptable use:

a. Accessing data to which a member has no legitimate right;
b. Enabling unauthorized members or other individuals to access data;
c. Disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law;
d. Inappropriately modifying or destroying data; and
e. Inadequately protecting restricted data.

3. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination from the Department.

307.4 - 4 Department Member Security (Access Control)

1. Access control for Department members, outside agency personnel, and private contractors/vendors for the purpose of gaining access to the physical, logical, and electronic LEIN-based Criminal Justice Information (CJI) of the Detroit Police Department is essential in the security of the Department.

2. The Terminal Agency Coordinator (TAC), who is assigned through Technical Services of the DPD, is responsible for identity verification. The TAC will ensure a Michigan and FBI fingerprint-based record check is conducted of all Department members, outside agency personnel, and private contractors/vendors with direct access to LEIN-based CJI and all Department members, outside agency personnel, and private contractors/vendors with direct responsibility to configure and maintain systems, networks, and databases with direct access to CJI within 30 days of assignment.
3. The TAC will conduct a name-based check to receive criminal history record information (CHRI) for all Department members, outside agency personnel, and private contractors/vendors with direct access to LEIN-based CJI and all Department members, outside agency personnel, and private contractors/vendors with direct responsibility to configure and maintain systems, networks, and databases with direct access to CJI.
4. All requests for access shall be made as specified below by the Michigan State Police (MSP) Chief Security Officer (CSO):

    a. If a felony conviction of any kind exists, access to LEIN-based CJI shall be denied;
    b. The Department may ask for a review by the MSP CSO in extenuating circumstances where the severity of the offense and the time that has passed may support a possible exception by the MSP CSO;
    c. If a record of any kind exists or the individual requesting access appears to be a fugitive or has an arrest history without conviction, LEIN-based CJI access shall not be granted until the MSP CSO has reviewed the record to determine if CJI access is appropriate;
    d. If the individual requesting access is employed by a Non-Criminal Justice Agency (NCJA), the MSP CSO and the Department's Terminal Agency Coordinator (TAC), shall review the record to determine if LEIN-based CJI access is appropriate;
    e. If a Department member who currently has access to LEIN-based CJI is arrested and/or convicted, continued access to CJI shall be determined by the MSP CSO. If the MSP CSO determines that access to LEIN-based CJI would not be in the best interest of the public, access shall be denied and the Department shall receive written notice of the access denial;
    f. Outside agency personnel and private contractors/vendors with access to physically secure locations or controlled areas during CJI processing shall be subject to MI and FBI fingerprint-based record checks unless escorted by an authorized Department member; and
    g. As a best practice, individual CHRI background checks will be conducted by the Department TAC every five (5) years.

5. Prior to granting access to LEIN-based CJI to all retained contractors and vendors, the Department TAC shall verify identification with MI and FBI fingerprint-based record checks.
6. Access by outside agencies/entities requires prior approval by the Department TAC, MSP CSO, and the Legal Advisor.
7. The TAC will conduct a name-based records check CHRI for all individuals stipulated in this section.
8. If a record of any kind is located, there will be a delay in system access pending review of criminal history record information.
9. When identification of the applicant with a criminal history has been established by fingerprint comparison, the TAC shall review the matter.
10. A contractor found to have a criminal record consisting of felony conviction(s) shall be disqualified from LEIN-based CJI access.
11. Applicants confirmed to have outstanding arrest warrants shall also be disqualified.
12. The Department must have a memorandum of understanding (MOU) and a law enforcement data sharing agreement regarding gaining access to the physical, logical, and electronic LEIN-based Criminal Justice Information (CJI) of the Detroit Police Department.

307.4 - 4.1 Access List of Personnel

The Department TAC shall maintain a current list of personnel with authorization to access LEIN-based CJI and shall, upon request, provide a copy of the access list to the MSP CSO.

307.4 - 4.2 Misdemeanor Offense(s)

Applicants with a record of misdemeanor offense(s) may be granted LEIN-based CJI access if the MSP CSO determines the nature and severity (not punishable by more than one (1) year) of the offense(s) does not warrant disqualification.

307.4 - 4.3 Reassigned/Transferred/Retired/Terminated/Resigned Members

The Department TAC shall review LEIN-based CJI access authorizations when members are reassigned or transferred to other entities within the Department and initiate appropriate actions such as closing/establishing accounts and changing system access. The same is true for terminated/retired/resigned members.

307.4 - 5 Physical Protection

307.4 - 5.1 Physically Secure Location

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the LEIN-based CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-

public areas of the Detroit Police Department shall be identified with a sign at the entrances.

307.4 - 5.2 Visitors Access

1. A visitor is defined as a person who visits a Department facility on a temporary basis who has no unescorted access to the physically secure location within the Department facility where LEIN-based CJI and associated information systems are located. All visitors of Department facilities shall abide by the following directions:

    a. Provide a valid form of identification used to authenticate the visitor;
    b. Visitor information shall be entered on the visitor log along with the authorized member responsible for escorting the visitor;
    c. A visitor badge shall be worn on the approved visitor's outer clothing and collected at the end of the visit;
    d. Visitor badges and/or lanyards shall be marked "Escort Required;"
    e. The visitor badge shall not be electronic or allow an unescorted guest access without a physical escort;
    f. The visitor shall not be allowed to enter a secured area without an escort present; and
    g. Visitor badges shall be logged and the log shall contain the name of the visitor, the department they are visiting, and the name of their escort during the visit.

2. The visitor must be accompanied by an authorized escort at all times to include delivery or service personnel. An escort is defined as authorized person who accompanies a visitor at all times within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
3. The following are examples of individuals that may be authorized unescorted access to Department facilities:

    a. Noncriminal Justice Agency (NJCA) personnel such as city or county IT members who require frequent unescorted access to restricted areas will be required to establish a Management Control Agreement between the Detroit Police Department and the NJCA. Each NJCA employee with CJI access will appropriately have a state and national fingerprint-based record background check prior to this restricted area access being granted; and
    b. Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to establish a CJIS Security Addendum between the Detroit Police Department and each private contractor. Each private contractor will appropriately have a state and national fingerprint-based record background check prior to any restricted area access being granted.

4. Visitors shall not be allowed to view screen information (shoulder surfing).
5. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn members shall be notified or, if there are no sworn members available, non-sworn members shall call 911.
6. A visitor who has no unescorted access to the physically secure location within a Department facility shall not be allowed to sponsor another visitor.
7. A visitor shall not enter into a secure area with electronic devices unless approved by the Department's Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without written permission from an authorized supervisor.
8. All requests by groups for tours of a Department facility will be referred to the Department's LASO for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on Department premises.

307.4 - 5.3 Authorized Physical Access

1. Only authorized personnel will have access to physically secure non-public locations. The Department will maintain and keep a current list of authorized personnel. All physical access points into the Department's secure areas will be authorized before granting access. The Department will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the Department from physical, logical, and electronic breaches.
2. All Department members with CJI physical and logical access must adhere to the following requirements:

    a. To verify identification, a state of residency and national fingerprint-based record check shall be conducted within 30 days of assignment for all members who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI;
    b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times;
    c. Prior to granting access to CJI to support personnel, private contractors/vendors, the Detroit Police Department shall verify identification via a state of residency and national fingerprint-based record check; and
    d. Refer to the CJIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.

3. Any individual with CJI physical and logical access shall complete the following security awareness training:

   a. All authorized Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six (6) months of being granted duties that require CJI access and every two (2) years thereafter; and
   b. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum.

4. All Department members with CJI physical and logical access must be aware of who is in their secure area before accessing confidential data by taking appropriate action to protect all confidential data and protect all terminal monitors with viewable CJI displayed on the monitor, not allowing public or escorted visitors view of them.

5. All Department members with CJI physical and logical access must properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc. The following are examples of protecting individual security:

   a. Report the loss of issued keys, proximity cards, etc. to their immediate supervisor;
   b. If the loss occurs after normal business hours, or on weekends or holidays, members are to call the Department's TAC to have authorized credentials like a proximity card deactivated and/or door locks possibly rekeyed; and
   c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures.

6. Members must properly protect CJI from viruses, worms, Trojan horses, and other malicious code.
7. The Department TAC shall establish proper Web usage – allowed versus prohibited.
8. Members shall not use personally owned devices on Department computers with CJI access.
9. The use of electronic media is only allowed by authorized Department members. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.
10. Members shall encrypt emails when electronic email is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements. If CJI is transmitted by email, the email must be encrypted end-to-end and the email recipient must be authorized to receive and view CJI.

11. Members shall report any physical incidents to the Department's LASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs, and printouts containing CJI.
12. Members shall only release hard copy printouts of CJI to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a "need to know" basis.
13. Members shall ensure data centers with CJI are physically and logically secure.
14. Members shall keep appropriate Department security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the Department, state and/or federal agencies.
15. Members shall not use food or drink around information technology equipment.
16. Members shall know which door to use for proper entry and exit of any Department facility and only use marked alarmed fire exits in emergency situations.
17. Members shall ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

307.4 - 6 Roles and Responsibilities

307.4 - 6.1 Terminal Agency Coordinator (TAC)

The Terminal Agency Coordinator (TAC) serves as the point-of-contact at the Department for matters relating to CJIS access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and MI CJIS systems policies/addenda.

307.4 - 6.2 Local Agency Security Officer (LASO)

The Local Agency Security Officer (LASO) has the following responsibilities:

a. Identify who is using the CSA (MI) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same;
b. Identify and document how the equipment is connected to the state system;
c. Ensure that personnel security screening procedures are being followed as stated in this policy;
d. Ensure the approved and appropriate security measures are in place and working as expected; and
e. Support policy compliance and ensure the CJIS System Agency Information Security Officer (CSA ISO) is promptly informed of security incidents.

307.4 - 6.3 Agency Coordinator (AC)

An Agency Coordinator (AC) is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractors/vendors and the Detroit Police Department. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor

subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by LEIN/NCIC.

307.4 - 6.4 CJIS System Agency Information Security Officer (CSA ISO)

The CJIS System Agency Information Security Officer (CSA ISO) is responsible for the following:

a. Serves as the security point of contact (POC) to the FBI CJIS Division ISO;
b. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level;
c. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users; and
d. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. They shall 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.

307.4 - 6.5 Information Technology Support

In coordination with the above roles, all vetted IT support staff will protect CJI from compromise at the Detroit Police Department by performing the following:

a. Protect information subject to confidentiality concerns – in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and the planned end of life. CJI is stored on computers, laptops, in-car computers, servers, tape backups, CDs, DVDs, thumb drives, and internet connections as authorized by the Department;
b. Be knowledgeable of required Department technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit, and at the end of life;
c. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores using Department-approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.;
d. Properly protect Department CJIS systems from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions):

    - Install and update antivirus on computers, laptops, in-car computers, servers, etc.

- Scan any outside non-agency owned CDs, DVDs, thumb drives, etc. for viruses

e. Data backup and storage – centralized or decentralized approach:

- Perform data backups and take appropriate measures to protect all stored CJI
- Ensure only authorized vetted personnel transport off-site tape backups or any other media that stores CJI is removed from any physically secured location
- Ensure any media released from the Department is properly sanitized/destroyed

f. Timely application of system patches – part of configuration management. The Department shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws;

g. Access control measures – address least privilege and separation of duties. The IT staff shall enable event logging of the following:

- Successful and unsuccessful system log-on attempts
- Successful and unsuccessful attempts to access, create, write, delete, or change permission on a user account, file, directory, or other system resource
- Successful and unsuccessful attempts to change account passwords
- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for user to access, modify, or destroy the audit log file

h. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to the following:

- Hotel business center computers
- Convention center computers
- Public library computers
- Public kiosk computers

i. Ensure account management in coordination with the Terminal Agency Coordinator (TAC):

- Ensure that all user IDs belong to currently authorized users
- Keep login access current, updated, and monitored
- Remove or disable terminated, transferred, or associated accounts
- Authenticate verified users as uniquely identified

- Prevent multiple concurrent active sessions for one user identification for those applications accessing CJI
- Not use shared generic or default administrative user accounts or passwords for any device used with CJI

j. Ensure the following network infrastructure protection measures are in place:

- Take action to protect CJI-related data from unauthorized public access
- Control access and monitor the enabling and updating configurations of boundary protection firewalls
- Enable and update personal firewall on mobile devices as needed
- Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear context. *Note: a police vehicle shall be considered a physically secure location
- Ensure any electronic media that is removed from a physically secured location in encrypted in transit by a person or network
- Not use default accounts on network equipment that passes CJI (e.g. switches, routers, or firewalls)
- Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by Department authorized personnel. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using the same wide area network; and

k. Communicate and keep the Department informed of all scheduled and unscheduled network and computer downtimes, security incidents, and misuse.

307.4 - 6.6 Visitor Access/Security

1. Administration of the Visitor Check-in/Check-out procedure is the responsibility of identified individuals in each Department facility.
2. Prior to gaining access to a physically secure area, a visitor must go through the following process:

a. The visitor will be screened by Department personnel for weapons. No weapons are allowed in any Department facility except when carried by personnel authorized by the Department;
b. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any Department facility except when carried by personnel deemed authorized by the Department;

c. Escort personnel will acknowledge being responsible for properly evacuating visitors in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures; and
d. Escort personnel will validate that a visitor is not leaving the Department facility with any Department owned equipment or sensitive data.

3. All Department personnel and supporting entities are responsible for reporting any unauthorized physical, logical, and electronic access to the Local Agency Security Officer (LASO). Below are the Department point of contacts for reporting any non-secure access:

LASO Name: Manager Michael Saraino	LASO Phone: 313 596-1860	LASO email: Sarainom572@detroitmi.gov
TAC Name: PO Jonathan Yakimovich	TAC Phone: 313 596-1860	AC email: LEINAdmin@detroitmi.gov

307.4 - 6.7 Penalties

1. Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including access privileges, civil and criminal prosecution, and/or termination.
2. Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring member, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

307.4 - 7 User Account – Access Validation

1. The purpose of user account – access validation is to establish requirements for user accounts and access validation for all criminal justice networks to ensure the security of system access and accountability.
2. All accounts shall be reviewed annually by the Department's Local Agency Security Officer (LASO) to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain CJI. The LASO may also conduct periodic reviews.
3. All Department guest accounts with access to the criminal justice network shall contain an expiration date of one (1) year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.
4. The LASO should disable all new accounts that have not been accessed within 30 days of creation. Accounts of members on extended leave (more than 30 days) should be disabled. Exceptions can be made in cases where uninterrupted access

to IT resources is required. In those instances, the member going on extended leave should have a Department-approved request from the designated account administrator.

5. The LASO must be notified if a user's information system usage or need-to-know changes (i.e. the member is terminated, transferred, etc.). If a member is assigned to another entity for an extended period (more than 90 days), the LASO will transfer the member's account(s) to the new entity.
6. The LASO will remove or disable all access accounts for separated or terminated members immediately following separation from the Department.
7. The primary responsibility for account management belongs to the LASO.
8. The LASO 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
   c. Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

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

307.4 - 8 Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of the Department's entire network. As such, all Department members (including contractors and vendors with access to Department systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

307.4 - 8.1 General

1. All systems-level passwords (e.g. root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
2. All production system-level passwords must be part of the Information Security administrated global password management database.
3. All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed every 90 days and the past 10 passwords cannot be reused.
4. User accounts with access to LEIN/NCIC privileges must have a unique password from all other accounts held by that user.
5. Passwords must not be inserted into email messages or other forms of electronic communication.
6. All user-level, system-level, and LEIN/NCIC access level passwords must conform to the guidelines described below.

307.4 - 8.2 Guidelines

Members shall comply with the below password construction requirements:

a. Be a minimum length of eight (8) characters on all systems;
b. Not be a dictionary word or proper name;
c. Not be the same as the User ID;
d. Expire within a maximum of 90 calendar days;
e. Not be identical to the previous ten (10) passwords;
f. Not be transmitted in the clear or plaintext outside the secure location;
g. Not be displayed when entered; and
h. Ensure passwords are only reset for authorized users.

307.4 - 8.3 Password Protection Standards

1. Members shall not use their User ID as their password or share their passwords with anyone. All passwords are to be treated as sensitive, confidential Department information.
2. The following are prohibited as it pertains to password protection standards:

   a. Do not reveal a password to the supervisor;
   b. Do not talk about a password in front of others;
   c. Do not hint at the format of a password (e.g. "my family name");
   d. Do not reveal a password on questionnaires or security forms;
   e. Do not share a password with family members;
   f. Do not reveal a password to a co-worker while on furlough;
   g. Do not use the "Remember Password" feature of applications;
   h. Members shall not write passwords down and store them anywhere in their workplace; and
   i. Do not store passwords in a file on any computer system unencrypted.

3. If someone demands a password, refer them to this directive or have them contact Technical Support for assistance.
4. If an account or password is suspected to have been compromised, report the incident to the Local Agency Security Officer (LASO) and change all passwords.
5. Password cracking or guessing may be performed on a periodic or random basis by the MSP/FBI or Technical Support members. If a password is guessed or cracked during one of these scans, the user will be required to change it.

307.4 - 8.4 Application Development Standards

Application developers must ensure their programs contain the following security precautions:

a. Should support authentication of individual users, not groups;
b. Should not store passwords in clear text or in any easily reversible form;

c. Should provide some sort of role management, such that one user can take over the function of another without having to know the other's password; and
d. Should support Terminal Access Controller Access Control System + (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

307.4 - 8.5 Remote Access Users

Access to Department networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user ID are required) or a form of advanced authentication (i.e. Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.)

307.4 - 9 Unique Identifier (User Name Policy)

307.4 - 9.1 General

The Detroit Police Department requires that each Department member with access to Department networks, applications, and/or LEIN/NCIC for the purpose of storing, processing, and/or transmitting CJI shall be uniquely identified by use of a unique identifier. A unique identifier shall also be required for all persons who administer and maintain the systems that access Department and LEIN-based CJI and/or networks. The Department requires users to identify themselves uniquely before they are allowed to perform any action on the network and/or applications. All user IDs shall belong to currently authorized users. Members shall not share their IDs with other Department members or family members at any time.

307.4 - 9.2 Guidelines

The unique identification can take the form of the following examples:

a. User's full name (JohnWDoe);
b. Form of full name (SASmith);
c. Badge number (WV724966);
d. Combination of name and badge number (jhardWV966);
e. Pension number (123456789); or
f. Other unique alphanumeric identifier.

307.4 - 10 Malicious Code, Spam, and Spyware Protection

1. Requirements must be met by all computers connected to Department networks to ensure effective malicious code, spam, and spyware protection. This protection shall apply to all Department systems with or without Internet access throughout the network and on all workstations, servers, and mobile computing devices on the network.
2. The Detroit Police Department shall employ virus protection mechanisms to detect and eradicate malicious code (e.g. viruses, worms, Trojan horses) at critical points

throughout the network and on all workstations, servers, and mobile computing devices on the network.

3. The Department shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.
4. The Department shall implement spam and spyware protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers). Spyware protection will be employed at workstations, servers, and/or mobile computing devices on the network.
5. The Department will use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet access, and removable media.

307.4 - 10.1 Prevention of Malicious Code Problems

Below are examples of ways to prevent malicious code problems:

a. Always run the corporate standard;
b. Run the current version and install anti-virus software updates as they become available;
c. Anti-virus software is to be enabled on all workstations and servers at start-up and employ resident scanning;
d. Detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways;
e. On servers, update virus signature files immediately, or as soon as possible, with each new release;
f. Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying the "Trash";
g. Delete spam, chain, and other junk email without forwarding;
h. Never download files from unknown or suspicious sources;
i. Avoid direct disk-sharing with read/write access unless there is absolutely an Department requirement to do so;
j. Always scan a floppy diskette from an unknown source for viruses before using it; and
k. Always scan any media that is brought into the Department before introducing it to the network.

307.4 - 10.2 Detection

Any activities with the intention to create and/or distribute malicious programs into the Department's networks (e.g. viruses, worms, Trojan horses, logic bombs, etc.) are prohibited. Virus-infected computers must be removed from the network until they are verified as virus-free. If a virus is detected on a workstation and the anti-virus software

cannot eliminate the virus, contact the Department LASO. Do not turn off the computer as it will be quarantined and taken off the network until it can be scanned and re-imaged with the operating system image.

307.4 - 11 Media Protection

1. The intent of media protection is to 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.
2. The scope of media protection applies to any electronic or physical media containing MI/FBI Criminal Justice Information (CJI) while being stored, accessed, or physically moved from a secure location from the Department. Media protection applies to any authorized member who accesses, stores, and/or transports electronic or physical media. Transporting CJI outside the Department's assigned physically secure area must be monitored and controlled.
3. Authorized Department members shall protect and control electronic and physical CJI while at rest and in transit. The Department will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the Department Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting, and storing media.

307.4 - 11.1 Media Storage and Access

1. 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.
2. To protect CJI, Department members shall:

    a. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room;
    b. Restrict access to electronic and physical media to authorized members;
    c. Ensure that only authorized users remove printed or digital media from the CJI;
    d. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques, and procedures;
    e. Not use personally owned information systems to access, process, store, or transmit CJI unless the Department has established and documented the specific terms and conditions for personally owned information system usage;
    f. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to the following:

- Hotel business center computers
- Convention center computers
- Public library computers
- Public kiosk computers

g. Store all hardcopy CJI printouts maintained by the Department in a secure area accessible to only those employees whose job function requires them to handle such documents;
h. Safeguard all CJI by the Department against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy; and
i. Take the following appropriate action when in possession of CJI while not in a secure area:

- CJI must not leave the member's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place
- Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption:

  - When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers, and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
  - When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards

j. Members shall lock or log off their computer when not in immediate vicinity of their work to protect CJI. Not all members have the same CJI access permissions and need to keep CJI protected on a need-to-know basis; and
k. Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI.

307.4 - 11.2 Media Transport

1. Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable,

transportable digital memory media (i.e. magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card).

2. Dissemination to another agency is authorized if:

   a. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency; or
   b. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

3. Department members shall:

   a. Protect and control electronic and physical media during transport outside of controlled areas; and
   b. Restrict the pickup, receipt, transfer, and delivery of such media to authorized members.

4. Department members will control, protect, and secure electronic and physical media during transport from public disclosure by:

   a. Use of privacy statements in electronic and paper documents;
   b. Limiting the collection, disclosure, sharing, and use of CJI;
   c. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those individuals or roles that require access;
   d. Securing hand carried confidential electronic and paper documents by:

      - Storing CJI in a locked briefcase or lockbox
      - Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized members
      - For hard copy printouts or CJI documents:

        ➢ Package hard copy printouts in such a way as to not have any CJI viewable
        ➢ Printout or CJI documents that are mailed or shipped must have documented procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by methods that provide for complete shipment tracking and history, and signature confirmation of delivery

   e. Not taking CJI home or when traveling unless authorized by the Department LASO. When disposing confidential documents, use a cross-cut shredder.

307.4 - 11.3 Electronic Media Sanitization and Disposal

The Department shall sanitize, that is, overwrite at least three (3) times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals.

Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The Department shall maintain written documentation of the steps taken to sanitize or destroy electronic media. The Department 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. For end of life media policy, refer to "Media Sanitization Destruction Policy."

307.4 - 11.4 Breach Notification and Incident Reporting

The Department 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. The CSA ISO Computer Security Incident Response Capability Reporting Form (CJIS.061) can be accessed and completed at www.michigan.gov/lein under the "Sample Documentation" button. The completed form can be submitted via email directly from the form.

307.4 - 11.5 Roles and Responsibilities

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

a. Department members shall notify their supervisor or the Department LASO, and an incident-report form 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, steps taken/to be taken in response to the incident;
b. The supervisor will notify the LASO of the loss or disclosure of CJI records;
c. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents;
d. The CSA ISO will:

- 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 of major incidents that significantly endanger the security or integrity of CJI
- 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
- Act as a single POC for their jurisdictional area for requesting incident response assistance

307.4 - 12 Discipline

1. In support of the Department's mission of public service to the City of Detroit citizens, the Department provides the technological resources needed to members to access MI/FBI CJIS systems and information.
2. All Department members with access to MI/FBI Criminal Justice Information (CJI) or any system with stored MI/FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care, and maintenance of the information. All technology equipment, such as computers, laptops, software, copiers, printers, terminals, in-car computers, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit MI/FBI CJIS is a privilege allowed by the Department, MI CSO, and the FBI. To maintain integrity and security of the Department's and MI/FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state, and local laws, regulations, and contractual obligations. All existing laws and Department regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.
3. Misuse of computing, networking, or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against an individual or the Department after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules of evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of the Department's computing and network resources and MI/FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

307.4 - 12.1 Examples of Misuse with Access to MI/FBI CJI

1. The following are examples of misuse with access to MI/FBI CJI:

    a. Using someone else's login;
    b. Leaving a computer logged in with the member's login credentials unlocked, allowing anyone to access Department systems and/or MI/FBI CJIS systems and data containing the member's name;
    c. Allowing an unauthorized individual to access MI/FBI CJI at any time for any reason. Note: Unauthorized use of the MI/FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties;
    d. Allowing remote access of Department issued computer equipment to MI/FBI CJIS systems and/or data without prior authorization by the Department;
    e. Obtaining a computer account that the member is not authorized to use;
    f. Obtaining a password for a computer account of another account owner;

g. Using the Department's network to gain unauthorized access to CJI;
h. Knowingly performing an act which will interfere with the normal operation of MI/FBI CJIS systems;
i. Knowingly propagating a computer virus, Trojan horse, worm, and/or malware to circumvent data protection or compromising existing security holes to MI/FBI CJIS systems;
j. Masking the identity of an account or machine;
k. Posting materials publicly that violate existing laws;
l. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner;
m. Unauthorized possession of, loss of, or damage to the Department's technology equipment with access to CJI through unreasonable carelessness or maliciousness;
n. Maintaining CJI or duplicate copies of official Department files in either manual or electronic formats at the member's place of residence or in other physically non-secure location without express permission;
o. Using the Department's technology resources and/or CJIS systems for personal or financial gain;
p. Deliberately failing to report promptly any known technology-related misuse by another member that may result in criminal prosecution or discipline under this policy; and
q. Using personally owned devices on the Department's network to include personally-owned thumb drives, CDs, mobile devices, tablets on Wi-Fi, etc. Personally owned devices should not store Department data or CJI.

2. The above listing is not all-inclusive and any suspected technology resource or MI/FBI CJIS system or MI/FBI CJI misuse will be handled by the Department on a case by case basis. Activities will not be considered misuse when authorized by appropriate Department officials for security or performance testing.

307.4 - 12.2 Private Policy

All Department members utilizing Department-issued technology resources funded by the Department expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of Department systems indicates consent to monitoring and recording. The Department reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit, and at end of life. Department members shall not store personal information with an expectation of personal privacy that are under the control and management of the Department.

307.4 - 12.3 Personal Use of Agency Technology

The computers, electronic media and services provided by the Department are primarily for business use to assist members in the performance of their jobs. Limited, occasional,

or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the system's use for their business purposes. However, members are expected to demonstrate a sense of responsibility and not abuse this privilege.

307.4 - 12.4 Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, the Department shall:

a. Establish an operational incident handling capability for all information systems with access to MI/FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and
b. Track, document, and report incidents to appropriate Department officials and authorities.