GENERAL ORDERS MANUAL
WESTERN MICHIGAN UNIVERSITY
DEPARTMENT OF PUBLIC SAFETY

I. PURPOSE

The purpose of this general order is to establish policy and procedure guidelines for the use of MI/FBI Criminal Justice Information (CJI), including Law Enforcement Information Network (LEIN) and its interfaced computer systems. In addition, it defines the responsibilities of the Terminal Agency Coordinator (TAC), the Local Agency Security Officer (LASO), and authorized users of CJI at the WMU Department of Public Safety.

II. POLICY

All Western Michigan University Police Department personnel with access to MI/FBI CJI or any system with stored MI/FBI CJI have a duty to protect the systems from physical and environmental damage. Employees are also responsible for correct use, operation, care, and maintenance of the information including all hardware and software used in the collection, storage and transmission of CJI. To maintain the integrity and security of this department's and MI/FBI's CJI systems and data, each employee is required to adhere to this general order as well as laws and regulations set forth by the FBI and MSP in relation to the handling of CJI.

It is also the policy of the Western Michigan University Police Department to send, receive, and process administrative and query messages in accordance with the LEIN, NCIC, and CJIS rules as set forth in their respective policy documents and operating manuals. LEIN, NCIC, and CJIS manuals, policies and laws may be referenced at the following web address: http://www.michigan.gov/lein. It is departmental policy to treat all information received from the LEIN system, including its interfaced computer systems, as confidential according to the aforementioned rules, policies and procedures.

A. INTERFACED COMPUTER SYSTEMS

1. LEIN – Law Enforcement Information Network
2. NCIC – National Crime Information Center
3. NLETS – National Law Enforcement Telecommunications Systems
4. CMIS – Corrections Management Information System
5. SOS – Michigan Secretary of State
6. CPIC - Canadian Police Information Centre

B. CRIMINAL JUSTICE INFORMATION SYSTEMS (CJIS)

CJI is contained in, but not limited to, the following systems and programs:

1. CAD – Computer-Aided Dispatch
2. RMS – Reports Management Systems
3. Mobile CAD

4. eCitation and eCrash (LexisNexis)
5. Live Scan
6. Talon

III. EXAMPLES OF MISUSE OF LEIN/CJI

The list below is not all-inclusive and any suspected technology resource or MI/FBI CJIS system or MI/FBI CJI misuse will be handled on a case-by-case basis. Activities will not be considered misuse when authorized by the chief or deputy chief for security or performance testing. Unauthorized use of the MI/FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties, as well as departmental discipline.

A. Using someone else's login.
B. Leaving computer logged in with your login credentials unlocked, allowing anyone to access departmental systems and/or MI/FBI CJIS systems and data in your name.
C. Allowing unauthorized person to access MI/FBI CJI at any time for any reason.
D. Allowing remote access of department issued computer equipment to MI/FBI CJIS systems and/or data without prior authorization.
E. Obtaining a computer account that you are 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 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 his or her place of residence or in other physically non-secure locations 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 employee that may result in criminal prosecution or discipline under this policy.
Q. Using personally owned devices on the department's network (e.g., flash drives, CDs, DVDs, mobile devices, cameras, etc). Personally-owned devices should not store private department data or CJI.

IV. LEIN/CJI SYSTEM ACCESS

A. Authorized access to LEIN/CJI by employees of this agency is only permitted to those who have taken and passed the approved biennial LEIN test, read and signed the Notice of Criminal Penalties and Civil Action form, completed security awareness training, successfully passed a

fingerprint and background check, and otherwise met all minimum screening requirements set by the FBI CJIS Security Policy.

B. Members of this department are prohibited from accessing LEIN for personal reasons or any other reason outside the scope of criminal justice employment at this agency. Department personnel are prohibited from disseminating LEIN information to private citizens or non-criminal justice personnel who would not be authorized to receive it directly on their own authority.
C. Per the Secretary of State's Office, the only driver's records or vehicle records information that are to be obtained by LEIN are for court, criminal cases, traffic authorizations, traffic cases, or police applicants.

1. Any other request, such as other university department applicant's driving records, are to be handled by mail to the SOS Office, Commercial Look-Up Division, Third Floor, Mutual Building, 208 North Capitol Avenue, Lansing, MI. 48918
2. Employees of the Parking Services Division may access vehicle records information to accomplish their assigned job responsibilities.
3. Under no circumstance will SOS information be given to a private citizen or business to conduct their own investigation, i.e., accidents or suspicious incidents.

D. Secondary Dissemination: Department personnel may disseminate LEIN/CJI information to authorized persons or organizations outside of this agency when the information is being used for a legitimate criminal justice purposes and the following criteria are met:

1. For CJI not including CHRI (CCH information), the identity of the requester or organization is verified and confirmed to be an authorized LEIN recipient. Normally telephone requests to run a LEIN inquiry for another person should not be honored unless the person receiving the request definitively knows the requester. If there is any question as to a requester's LEIN access authorization, the requester's agency shall be contacted before conducting the request.
2. If CHRI (CCH) information is disseminated, the following information shall be documented in the Secondary Dissemination Log: Date, Name/Title of recipient, WMU Case Number, Name on CCH. The log is located on police share directory on department computers.

E. Due to the requirement of confidentiality of LEIN information, all LEIN printouts must either remain in the custody of personnel authorized to receive LEIN information, secured in a locked area only accessible to authorized personnel, or immediately be disposed of by cross-cut shredding them.

V. RELEASE OF LEIN INFORMATION TO THE PUBLIC

A. STOLEN PROPERTY: To run stolen property checks for private citizens, the officer shall obtain the caller's name, address, telephone number, description and location of property to be checked. An officer shall respond to the location of the property. If the property is located outside this department's jurisdiction, the caller should be advised to call department having jurisdiction. With the property in hand, the officer can then perform the LEIN/NCIC inquiry. If the property

has been reported stolen, the officer is to recover the property. If the inquiry is negative, the caller may be informed the property has not been reported stolen at this time.

B. WARRANTS: Persons calling to determine if an arrest warrant has been issued for them or another shall be advised their inquiry must be made in person at the police department or 8th District Court. The person may also advise their location so an officer can be dispatched to contact to person. A LEIN inquiry may be run after the person is positively identified by the officer.

C. VEHICLES: Callers may be informed that all vehicles reported stolen to this department are entered in LEIN/NCIC as stolen and that all impounded vehicles are entered into LEIN per General Order TLE-3. Callers wishing to determine if a suspicious vehicle has been stolen shall be advised that an officer will be dispatched to the location.

VI. TERMINAL AGENCY COORDINATOR & LOCAL AGENCY SECURITY OFFICER

A. The chief shall designate the Terminal Agency Coordinator (TAC) for LEIN for this department. The Terminal Agency Coordinator's responsibilities include:

1. Ensure the department's computer network prohibits unauthorized access to LEIN.
2. Serve as the primary liaison with the LEIN staff.
3. Coordinate LEIN operator training and ensure certification standards are maintained.
4. Distribute materials from LEIN and the interfaced computer systems.
5. Conduct the monthly LEIN/NCIC Record Validation process.
6. Report LEIN problems to the LEIN Field Services.
7. Perform regular checks of CCH inquiries ran by the department.
8. Monitor the process of warrant entry/cancellation with the courts.

B. The chief shall also designate the Local Agency Security Officer (LASO) for this department. The LASO may also serve as the TAC as many responsibilities overlap, however there is no requirement for such. The Local Agency Security Officer's responsibilities include:

1. Serving as the point of contact between MSP and this department on network and security issues, including security incident notification.
2. Monitor all security policies and provide guidance in implementing security measures and policies as they relate to CJIS.
3. Report violations of the security policy and guidelines. Establish and follow a security incident/violation response and reporting procedure to discover, investigate, document, and report on all security incidents/violations within the department.
4. Develop and conduct information security training programs. Provide resource information and other related publications to agency users. Ensure all personnel have been properly trained prior to granting access.
5. Maintain procedures regarding the changing of access levels, passwords, and accounts for users with changes in employment status.
6. Coordinate installation and upgrades to networks and applications that use CJI.

7. Maintain network topology documentation. Support security related configuration management for the department. Notify the state's CJIS Systems Agency Information Security Officer (CSA ISO) of any significant network changes.
8. Coordinate with MSP and FBI during periodic security audits, at the department or at device locations connected to the department, to ensure compliance with security policies and procedures.
9. Periodically review events logs and all personnel account access and privileges to department network, operating systems, software and systems associated with CJI.

C. LOCAL TAC AND LASO CONTACT INFORMATION:

Primary Local TAC: victoria.hastings@wmich.edu, 269-387-5607
Primary Local LASO: ryan.mcgregor@wmich.edu, 269-387-5420
Backup TAC & LASO: grant.allers@wmich.edu, 269-491-8972

VII. USER ACCOUNT ACCESS AND EVENT LOGS

A. The LASO is responsible for monitoring user access, user permissions, and event logs for software and systems that access, process, store, or transmit CJI.

B. User account lists and permissions for all systems containing CJI should be checked and documented annually, or more frequently. Event logs should be checked weekly.

C. User access shall be immediately revoked when employees are separated from the department (i.e., retire, resignation, termination, transfer, etc.)

D. Accounts should be disabled if a new account is not used in the first 30 days or if an individual is on leave for more than 30 consecutive days.

VIII. MONTHLY LEIN VALIDATIONS

A. The TAC is responsible for the monthly LEIN/NCIC record validation check.

B. The TAC will use the CJIC Reporter module within the MiCJIN Portal to obtain the monthly validation record list.

C. Validating the records includes:

1. Doing an inquiry of the record.
2. Checking with the court (i.e., injunctive orders, etc.) or contacting the complainant (i.e. stolen property/vehicles, etc.) to verify the record is still valid.
3. Compare the record with the case report, CCH (if applicable) and other documentation to ensure accuracy and completeness.
4. Following any additional instructions listed for each record type.
5. Immediately modify, cancel, or remove any record found to be inaccurate or invalid.

D. After all the records are validated, the TAC will mark the records as validated in the CJIC Reporter module.
E. The LEIN monthly validation list shall be kept on file for two years plus the current year.

F. LEIN entries are retained on file at the WMU police station. The investigating officer is responsible for providing the KCCDA as much information as possible to "pack the record" and be contained in the entry. All LEIN entries and cancellations are to be reflected in the police report to include the NCIC and LEIN entry reference numbers where applicable. The supervisor reviewing the initial incident report is responsible reviewing all LEIN entries associated with the case to ensure accuracy and completeness of the entry. Once the reviewing supervisor has completed the LEIN/NCIC entry "review check" they shall initial and date the LEIN entry packet and forward it to the LEIN TAC.

IX. LEIN ENTRIES

1. WARRANTS: The court of jurisdiction is responsible for entering warrants into LEIN/NCIC. When the court enters a warrant for this agency, a notification of entry is sent to the department's ORI (MI3988100). The shift supervisor shall run a LEIN/NCIC query and SOS record on the subject. The query results, original report and any other documentation should be used to check the court-entered information for accuracy and "pack the record" (add all additional personally identifying information to the entry). These forms are then forwarded to the LEIN TAC to review before being filed at the station.

   When a subject is arrested on a warrant from this agency, the arresting officer shall cancel the warrant in LEIN/NCIC and note if bonds were paid and if the subject was lodged or released. This shall also be documented in the officer's supplemental report with the cancellation attached.

   If the court cancels a warrant in LEIN (subject appears at the court, by prosecutor's request, etc.), the court will send a cancellation notification to the department's ORI. The shift supervisor shall check LEIN/TALON for these notifications each shift. For original misdemeanor and felony warrant cancellations, a supplemental report shall be completed documenting the reason for the court cancellation and any other action taken. Report supplements do not need to be completed for court-cancelled bench warrants. Warrant packet paperwork and corresponding LEIN documentation for all court-cancelled warrants shall be forwarded to the LEIN TAC by the shift supervisor and then forwarded to the Records Division.

2. INJUNCTIVE ORDERS: When an injunctive order is issued, a copy of the order is faxed to KCCDA to be entered into LEIN. KCCDA follows LEIN policies and "packs the record" for the injunctive order. KCCDA conducts a second party check of the entry. RUNS THE When the court enters an injunctive order related to a case submitted by this agency, a copy of the order is faxed to the KCCDA. LEIN TAC has the responsibility to complete monthly LEIN validations.

3. IMPOUNDED VEHICLES: Refer to General Order TLE-2.

4. MISSING AND UNIDENTIFIED PERSONS: Refer to General Order POL-17.
5. STOLEN PROPERTY: The investigating officer is responsible for ensuring stolen property is entered in LEIN and/or NCIC by KCCDA. The officer shall supply all known information ensuring the entry is fully "packed." For stolen vehicles, license plates, or guns, a copy of the incident report and the entry shall be filed at the station after being reviewed by the shift supervisor. For all other stolen property, the entry shall be forwarded to the records division after being reviewed by the shift supervisor. In all cases the police report shall reflect the stolen property was entered and include the LEIN/NCIC number assigned to the entry.

   When property or an article originally reported stolen to this department is recovered, an officer shall be assigned to write a supplemental report on the recovered stolen property. This officer is responsible for ensuring the stolen property/article is cancelled in LEIN and NCIC. With stolen vehicles, license plates, or guns, the officer shall pull the associated file from the dispatch room and forward it to the TAC with the LEIN cancellation documentation.

B. AUTOMATIC CANCELLATIONS OF ENTRIES BY LEIN AND NCIC

Most entries made to the LEIN/NCIC files have specific time limits for retaining an individual entry in a file. When any entry is cancelled by LEIN or NCIC a notice is sent via the LEIN terminal to the entering agency. Upon receipt of such a notice, the shift supervisor shall arrange for a supplemental report to be completed describing the cancellation and any other action taken. The supervisor shall then forward the documentation to the LEIN TAC. The LEIN TAC will review the documentation and submit it to the Records Division.

C. COMPUTERIZED CRIMINAL HISTORY (CCH) INQUIRIES

1. Each Person who operates the LEIN terminal to obtain a computerized criminal history shall comply with all the rules and regulations contained in the LEIN and NCIC manuals.
2. Criminal History information is for the exclusive use of criminal justice agencies. Under no circumstances is criminal history information to be used for personal reasons. Employees of the department shall only disseminate criminal history information to other LEIN authorized employees of this department, other sworn police officers, Prosecutor's Office, or courts of criminal record. Any other dissemination is strictly prohibited.
3. Patrol officers of this department shall only use the "C/" criminal investigation purpose code when running a criminal history. A specific purpose must be stated in the inquiry, such as: Larceny, OUIL, Arson, etc. Do not use generic terms such as: Arrest, Suspect, CCH, or Criminal. CCH inquiries are authorized on any suspect in a formal criminal investigation. CCH inquiries are authorized on people involved in suspicious activity as long as the suspicious activity is documented in a police report. CCH inquiries on traffic law violators are not authorized, unless they are arrested.
4. Command officers and sergeants are the only personnel authorized to request CCH inquiries for employment purposes. The purpose code for criminal justice employment is "J/" followed by the specific occupation of the person, such as: dispatcher, student, officer, intern, computer tech, network administrator, etc.
5. For background checks of individuals having access to the building, but who are not involved in the administration of criminal justice (vendors, volunteers, contractors, etc.), the purpose

code of "C/" shall be used followed by the description or occupation of the subject, such as: Custodian, Ride-Along, Plumber, etc.

6. CCH inquiries may only be made for the purposes stated above. No personnel of this department shall use any other purpose codes to run criminal histories without the express permission of the TAC.
7. In addition, all CCH Inquiries require completion of these fields OCA: case number, OPR: Terminal Operator, and FOR: Requester's name.
8. The names of all subjects having a CCH inquiry shall be documented in the incident report. For incidents with multiple checks of the same subject (i.e., due to a typographical error), then the number of inquiries, and reasons for such, shall also be documented in the report.

D. COMPUTERIZED CRIMINAL HISTORY SECURITY

1. The Terminal Agency Coordinator is responsible for maintaining the security of the CCH information for this department. On each Monday, the TAC will obtain list of all criminal histories run through our terminal over the previous seven days. This can be done by running a QLOG.

2. Most CCH inquiries will be immediately destroyed using a cross-cut shredder. CCH printouts not destroyed must have the final disposition documented in the police report (i.e., turned over to prosecutor, filed with original report, etc).

X. PERSONALLY-OWNED DEVICES

A. Personally-owned media and devices are not permitted to be connected (wired or wireless) to any department networks or computers with CJIS access. This includes but is not limited to phones, external hard drives, cameras, recording devices, USB flash drives, CDs, & DVDs.

B. In the event any personally owned devices are permitted in the future, written approval must be given by the department LASO. It shall be the responsibility of the LASO to promptly develop new department policies to regulate and permit the use of such devices, in accordance with CJIS policies.

XI. VISITOR ACCESS AND AUTHORIZED PHYSICAL ACCESS

A. A visitor is defined as a person who visits the department on a temporary basis who is not employed by the department and has no unescorted access to the physically secure location within the department where LEIN-based CJI and associated information systems are located. All locations beyond the lobby of the WMU Police Department are considered physically secure areas for purposes of this general order.

Visitors shall:

1. Check in before entering a physically secure area.
2. Provide an acceptable form of identification.
3. Allow themselves to be screened for weapons prior to access, if requested.

4. Be accompanied by an authorized departmental escort at all times, including delivery and service personnel. The visitor shall be physically escorted at all times. The use of cameras or other electronic means to monitor the visitor do not constitute an escort.
5. Not be allowed to view papers, computer screens or any other media containing CJI.
6. Not be allowed to sponsor or escort another visitor.
7. Not enter the server room or take pictures of any electronic devices unless approved by the department LASO.

B. Groups and Tours:
1. All requests by groups for tours of the WMU Police Department or designated secure areas must be approved by the Chief, Deputy Chief, TAC or LASO.
2. In most cases, these groups will submit a single form, to be signed by a designated group leader or representative.
3. The group leader will provide a list of names to department personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.
4. The visitor rules above shall apply for each visitor within the group (i.e. at least one escort is required for each group, provided the group stays together).

C. Strangers in physically secure areas without an escort should be challenged. Unauthorized individuals not having legitimate business in a restricted area shall be escorted to the lobby. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall appropriately remove the individual from the secure area.

D. Authorized Physical Access
Those permitted to enter physically secure areas without an escort are:
1. Individuals with authorized access to CJI.
2. Support personnel, private contractors/vendors, maintenance workers, and custodial workers are permitted after the following criteria are met:
   (a) Successfully complete state and national fingerprint-based record check.
   (b) Successfully complete a name-based CCH check (Note: A case number should be created and the CCH should be ran using the purpose code C/).
   (c) Complete security awareness training. Reading, signing and discussing the agency's Security Awareness Acknowledgment form is sufficient.

E. Any person with a conviction of a crime that was punishable by 1 year or more in jail are not permitted to access CJI nor are they permitted to have unescorted access to physically secure areas of the department.

XII. MEDIA PROTECTION

A. Controls shall be in place to protect media containing CJI while at rest, stored, or actively being accessed. This includes physical media (i.e., printed documents, imagery, etc) and electronic media (i.e., laptops, servers, flash drives, external hard drives, memory cards, etc).
B. All media containing CJI shall be secured in locked rooms or storage compartments when not under immediate control of the person authorized to view the CJI.

C. Printed or displayed CJI that is secure or under the control of an authorized person shall not be visible to the public or any unauthorized person. (i.e. LEIN being displayed on a monitor or paper printouts)
D. Media containing CJI which is transported outside of the departments assigned physically secure area must be monitored and controlled at all times by a designated person, authorized to access CJI.
E. When CJI is transmitted outside of the physically secure department area the data shall be encrypted.
    1. All department laptops and portable electronic devices with CJI access shall have encryption installed meeting FIPS 140-2 compliance standards.
    2. Patrol car MDTs with CJI access shall use encrypted VPN software (i.e., Absolute Secure Access). Patrol cars shall remain locked when unattended. CJI shall not be visible from outside the patrol car. Employees should regularly use the MDT screen blackout option to turn off the monitor when not in use. MDT screensavers should be set to activate after 30 minutes of inactivity.
F. LEIN/CJI data should not be electronically transmitted to other agencies or entities outside the department network unless the LASO has confirmed the software or services used are FIPS 140-2 compliant.

XIII. MEDIA SANITIZATION AND DESTRUCTION

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, and other similar items used to process, store and/or transmit CJI and classified and sensitive data shall be properly disposed.

A. Physical media (printouts and other physical media) shall be disposed of by one of the following methods:
    1. Shredded using department-issued cross-cut shredders.
    2. Secured until a private shredding company can come on-site and cross-cut shred the media while the entire process is witnessed by department personnel.
    3. Transported to an incinerator and destroyed while the entire process is witnessed by department personnel.

B. Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the following methods:
    1. Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the files to be sanitized are located.
    2. Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are weak and cannot effectively degauss magnetic media.
    3. Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

Physical and electronic media, including system hardware, that has been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from this department's control until the media or equipment has been sanitized and all stored information has been cleared using one of the above methods.

XIV. INCIDENT HANDLING, RESPONSE, AND MISUSE NOTIFICATION

A. ROLES:

1) CJIS Systems Officer (CSO): Role Definition: The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies.
WMU Public Safety: Chief Scott Merlo

2) Terminal Agency Coordinator (TAC): Role Definition: The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.
WMU Public Safety: Sgt Victoria Hastings and Ofc Grant Allers

3) CJIS Systems Agency Information Security Officer (CSA ISO): Role Definition:
   a) The CSA ISO shall: Serve as the security point of contact (POC) to the FBI CJIS Division ISO. 06/05/2017 CJISD-ITS-DOC-08140-5.6 8
   b) Document technical compliance with the CJIS Security Policy with the goal of assuring 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. 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.
   WMU Public Safety: Ryan McGregor or designee from OBFIT

4) FBI CJIS Division Information Security Officer (FBI CJIS ISO) Role Definition: The FBI CJIS ISO shall:
   a) Maintain the CJIS Security Policy
   b) Disseminate the FBI Director approved CJIS Security Policy.
   c) Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
   d) Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
   e) Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.

f) Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
g) Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

WMU Public Safety: Ryan McGregor

5) Local Agency Security Officer (LASO) Role Definition: Each LASO shall:
(a) Identify who is using the CSA 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.
(e) Support policy compliance and ensure the CSA ISO is promptly informed of security incidents

WMU Public Safety: Ryan McGregor and Grant Allers

B. Unauthorized access
If an employee has reason to believe a department computer or device with CJI access has been compromised by an unauthorized individual or computer virus, the following steps shall be taken:
1. DO NOT shut down, log off, power down, restart or unplug the computer or device.
2. Disconnect the computer from the network, internet and Absolute Secure Access (or any similar installed connection software). For wired computers, unplug the network cable from the computer. For devices or computers with wireless access, disconnect the computer from any wireless networks or WiFi hotspots. The department LASO or network administrator should be contacted if the employee requires assistance in these matters.
3. Immediately inform the LASO about all the events and circumstances regarding the unauthorized intrusion. Leave a note on the computer or device, forbidding use.

C. Misuse by authorized users
All department personnel shall report misuse of department technology resources or inappropriate use of CJI to the chief, deputy chief, TAC and LASO.

D. The LASO shall document each incident and notify state and national agencies when violations occur. Violation and compliance issues shall be reported to the state CSA ISO using the MSP ISO Security Incident Report form (CJIS-016) located on the www.michigan.gov/lein website. Additionally, computers or devices potentially compromised shall not be used again until the LASO has approved them for regular use.
E. Incident Response:
The security risk of both accidental and malicious attacks against government and private agencies remains persistent in both physical and logical environments. To ensure protection of CJI, Western Michigan University Public Safety shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and

user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

F. Reporting Security Events:
Western Michigan Public Safety shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Where feasible, Western Michigan University Public Safety shall employ automated mechanisms to help report security incidents. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

G. FBI CJIS Division Responsibilities
(1) The FBI CJIS Division shall:
(2) Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
(3) Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
(4) Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
(5) Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, including Product Security Bulletins, Virus Bulletins, and Security Clips.
(6) Track all reported incidents and/or trends.
(7) Monitor the resolution of all incidents

H. CSA ISO Responsibilities
(1) The CSA ISO shall:
(2) Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
(3) Identify individuals who are responsible for reporting incidents within their area of responsibility.
(4) Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
(5) Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
(6) 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.
(7) Act as a single POC for their jurisdictional area requesting incident response assistance.

I. Management of Security Incidents:

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

J. Incident Handling
Western Michigan Public Safety implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

K. Collection of Evidence
Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

L. Incident Response Training
Western Michigan University Public Safety shall ensure general incident response roles responsibilities are included as part of required security awareness training.

M. Incident Monitoring:
Western Michigan University Public Safety shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever timeframe is greater.

XV. PENALTIES

A. Some violations of CJIS and LEIN policies can result in criminal penalties and/or civil Actions.

B. Violations of this general order may result in network removal, access revocation, corrective or disciplinary action, and/or termination of employment.

Issued Date: 06/01/87
Revised Date: 05/18/94, 05/11/16, 02/22/17, 01/16/18, 01/18/18, 06/17/21, 01/04/22, 03/24/24, 05/13/24

Issued by

Scott Merlo
Director of Public Safety