MERIDIAN TOWNSHIP POLICE DEPARTMENT
GENERAL ORDER

Subject: **LAW ENFORCEMENT INFORMATION NETWORK - ACCESS AND USE**	General Order: 310
Effective Date: February 6, 2019 Revision Date: March 3, 2022	Distribution: All Employees

I. PURPOSE

The Department is approved to have Law Enforcement Information Network (LEIN) access. This policy sets forth the requirements for employees accessing LEIN and requesting and/or receiving LEIN information. LEIN – An on-line system that provides authorized agencies with an integrated network for sharing information by interfacing with other criminal justice information sources, including the National Crime Information Center (NCIC).

II. POLICY

Employees of the Meridian Township Police Department shall utilize the LEIN/SOS System in accordance with the rules established by the Criminal Justice Information Systems (CJIS) Policy Council and within the parameters of this directive. Personal or other information obtained from the system shall not be released nor disseminated except as specifically allowed by CJIS Policy Council rules.

Department employees are bound by the rules of LEIN as set forth in the LEIN Operations Manual and administrative rules of LEIN promulgated pursuant to the Administrative Procedures Act (PA #306 of 1969, as amended).

III. PROCDEURES

A. LEIN Operators and Requestors

1. Only LEIN operators are authorized to directly access LEIN.

2. LEIN operators are required to be fingerprinted and cleared through a criminal history check prior to accessing LEIN. For newly sworn employees, the fingerprinting and criminal history check shall be completed as part of the employment screening requirements.

3. LEIN operators must successfully complete LEIN training and pass certification tests required by the CJIS Policy Council within six months after being designated as a LEIN operator. Once certified, LEIN operators must successfully pass recertification tests and

complete security awareness training as required by the CJIS Policy Council. Employees authorized to request LEIN information from LEIN operators, and employees authorized to receive LEIN information in conjunction with their job responsibilities, must successfully complete LEIN training related to the proper uses, distribution and disclosure of LEIN information before requesting or receiving LEIN information.

4. LEIN operators shall ensure the accuracy, timeliness and quality of information they enter in LEIN. All entries shall be made in accordance with regulations set forth in the LEIN Operations Manual and NCIC Operations Manual.

5. Employees violating these policies and procedures, including accessing LEIN or requesting and/or receiving LEIN information without authorization, may be subject to discipline and/or denied use of LEIN; subject to CJIS Policy Council Act criminal penalties; and Drivers' Privacy Protection Act criminal penalties.

6. LEIN users shall sign the Notice of Criminal Penalties and Civil Action for the Misuse of LEIN notification form which will be kept on file (Appendix A).

B. Terminal Agency Coordinators (TAC)/Trainers

1. There shall be a terminal agency coordinator designated and trained for the Department.

2. Terminal agency coordinators shall be responsible for the following:

a. Ensuring compliance with LEIN and NCIC policies and regulations.

b. Coordinating audits of LEIN operations conducted by the Department of State Police.

c. Providing LEIN training and testing required by the CJIS Policy Council.

d. Immediately reporting any known violation of this policy through the appropriate chain of command.

e. Providing technical support regarding LEIN use.

f. The TAC shall serve as the TAC trainer. TACs shall attend TAC training offered by the Michigan State Police.

C. Disclosure of LEIN Information/Documents

1. LEIN information shall be disclosed only as necessary to comply with Department policy (e.g., preparation of investigative reports for prosecution).

a. Under no circumstances shall the actual LEIN printout or a copy of a LEIN printout be given to or displayed in an area accessible to anyone not authorized to receive LEIN information.

b. LEIN information may only be transmitted via electronic mail if the message is sent encrypted. LEIN information may be transmitted via facsimile machine only after the intended recipient has been verified as being authorized and present to receive the information.

c. LEIN information accompanies reports taken to the Ingham County Prosecutor and Township Attorney. All reports taken to the Ingham County Prosecutor and Township Attorney are logged in the Warrant Log to track the dissemination of the LEIN information. The Warrant Log is maintained by the Records Unit and Court Services Officer.

d. Disclosure in violation of Department policy which also is a violation of state law shall be referred for criminal prosecution.

e. Employees violating these policies and procedures, including accessing LEIN or requesting and/or receiving LEIN information without authorization, may be subject to discipline and/or denied use of LEIN as well as prosecution under applicable statutes (See LEIN Manual).

f. Where follow-up actions against a person or agency after an information security incident involves legal action (civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence. Complaints alleging misuse of MTPD's computing and network resources and CJIS systems and/or data will be directed to the LASO.

D. Acceptable Use

1. LEIN operators shall access LEIN only as necessary in the course of their duty and investigations. Under no circumstances shall employees access LEIN or request and/or receive LEIN information for personal reasons.

2. Employees shall comply with the Meridian Charter Township Network Connection Use Policy as well as the policies set forth in this general order.

3. The Meridian Township EMS/Fire Department may request and receive LEIN information, through this Department for a pre-employment criminal convictions history check (purpose code "E" only) and a pre-employment driving record check.

   a. They may also receive LEIN information on a vehicle involved in a fire or a hazardous materials incident.

   b. A user agreement must be signed prior to access.

4. In the interest of school safety, school district administrators (superintendents, principals and assistant principals) may request and receive verbal information on a vehicle registration to identify the owner of a suspicious vehicle within 1,000 feet of school property.

   a. A user agreement must be signed prior to access.

5. Police officers will be informed as to who has been authorized access to LEIN information and the extent of information they are authorized to disclose.

New

6. Personnel working remotely must use Net Motion or another acceptable FIPS 140-2 encryption method when accessing any CJI such as SRMS, MICJIN, etc.

E. Examples of Misuse with Access to CJI

1. Using someone else's login.

2. Leaving a computer logged in with your login credentials unlocked allowing anyone access to MTPD's systems or CJIS systems and data in your name.

3. Allowing any unauthorized person to access CJI at any time for any reason.

   a. Unauthorized use of the CJIS system is prohibited and may be subject to criminal and/or civil penalties (See LEIN Manual).

4. Allowing remote access of MTPD's issued computer equipment to CJIS systems and/or data without prior authorization from the Chief of Police.

5. Obtaining a password for a computer account of another account owner.

6. Using MTPD's network to gain unauthorized access to CJI.

7. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, sending messages, or deleting messages without explicit agreement with the owner.

8. Maintaining CJI or duplicate copies of official MTPD files in either physical or electronic formats in a physically non-secure location without express permission.

9. Deliberately failing to promptly report any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this general order.

10. The above listing is not all-inclusive and any suspected misuse of any technology resource or CJIS system will be handled on a case-by-case basis. Activities will not be considered misuse when authorized by appropriate MTPD officials for security or performance testing.

F. LEIN Security

1. Access to all LEIN terminals and information systems containing CJI is governed by the anti-virus guidelines set up by the Meridian Township Information Technology Department.

2. Password Procedure:

   a. Eight characters minimum password length

   b. Must include two numbers

   c. Expires every 90 days

   d. New passwords cannot use any of the previous six passwords

   e. System lock-out after three failed login attempts

3. Unique Identifier Procedure

   a. The Department shall utilize the LEIN operator's full last name as a unique identifier.

b. In the case of operators with same last name, the name shall be followed by the first two letters of the operator's first name.

4. Network accounts are only created through standard human resources and police department requests.

G. Physical Security of Criminal Justice Information

1. All physical, logical, and electronic access must be properly documented, authorized, and controlled on devices that store, process, or transmit unencrypted CJI.

2. Visitors Access to Physically Secure Locations

a. A visitor is defined as a person who visits MTPD on a temporary basis and has no unescorted access to the physically secure location with MTPD where LEIN-based CJI and associated information systems are located.

b. All visitors must check in at the cadet desk and provide identification before being granted access to the facility.

c. All visitors will be accompanied by an authorized escort at all times while within any secure location to ensure the protection and security of any CJI therein.

d. Private contractors/vendors who require frequent unescorted access to restricted areas will be required to establish a CJIS Security Awareness Agreement between MTPD and each private contractor personnel.

e. 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 questioned and removed if necessary.

3. Authorized Physical Access

a. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical, and electronic breaches.

b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas are subject to a state and national fingerprint-

based record check unless these individuals are escorted by authorized personnel at all times.

c. Authorized personnel must protect all terminal monitors with viewable CJI displayed on the monitor and not allow viewing by the public or escorted visitors. Authorized personnel who leave their work station unattended must utilize a screen lock while they are absent. All workstations containing CJI must have a session lock after a maximum of 30 minutes of inactivity which stays in effect until the user reestablishes access.

d. Authorized personnel must properly protect and not share any account passwords which could lead to the dissemination of CJI.

e. Personnel shall not disseminate the door code to anyone without permission from the Chief of Police or his designee.

f. Authorized personnel shall take precautions to protect from viruses, worms, Trojan horses, and other malicious code.

g. In the event an authorize user ceases employment with MTPD, the individual must surrender all property and access managed by MTPD.

h. The Meridian Township IT Department will create and retain an email for one year regarding user accounts.

H. Security Incident Response

1. In the event of a security breach or a suspected security breach, the finder of the breach shall notify the on-duty supervisor immediately. The finder shall also complete a Security Incident Response Form (Appendix C) and forward it to the LASO.

2. The agency shall promptly report digital and physical incidents that significantly endanger the security or integrity of CJI to the Michigan State Police Information Security Officer in compliance with the FBJ CJIS Security Council using the CJIS-016 ISO Security Incident Report Form (Appendix D).

3. Examples of security breaches are as follows:

a. Trojan horse, worms, malware, spyware (other than cookies), or virus infection of any type on any network based workstation.

b. Phishing attempts on any network based workstation.

c. Unauthorized viewing or handling of CJI by anyone not authorized.

d. Loss of any information system related item (flash drives, hard drives, etc.) that have exited any physically secure location.

e. Improper or suspected improper use, access, or dissemination of CJI by others.

I. Media Protection

1. Digital and physical media shall be stored within physically secure locations or controlled areas with access restricted to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted to standards stated in FBI CJIS Security Policy Section 5.10.1.2.

2. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will be used to prevent data from being compromised and/or unauthorized access.

3. Digital Media Sanitization and Disposal

a. The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals.

b. Inoperable digital media shall be destroyed (cut up, shredded, etc.).

c. The agency shall maintain written documentation of the steps taken to sanitize or destroy digital media.

d. Sanitization and/or disposal of physical or digital media shall be witnessed and/or carried out by authorized personnel.

e. Physical media including LEIN print-outs requiring disposal shall be destroyed via cross-cut shredding and/or burning.

J. User Account Access Validation

1. The TAC shall be responsible for maintaining a list of active users for all CJI systems including LEIN, Talon, MICJIN, and SRMS. The TAC must be notified if a user's information system usage changes.

2. The TAC shall be responsible for completing monthly validations as required and described in the LEIN Operations Manual and the NCIC Operations Manual. If validation is not completed the list may be purged. (Appendix B)

Revised

3. The TAC or LASO shall be responsible for ensuring yearly validations as required and described in the LEIN Operations Manual and the NCIC Operations Manual are completed. This includes MICJIN, Talon, SRMS, LEIN, Windows, and CAD.

4. Meridian Township IT will remove or disable all access accounts for separated or terminate employees immediately following separation from the agency.

IV. CANCELLATIONS

None.

Authorized by:

Ken Plaga, Chief of Police

Index as:
LEIN
Mobile Data Computers
Standard 3.5

Application: This directive constitutes department policy, and is not intended to enlarge the employer's or employee's civil or criminal liability in any way. It shall not be construed as the creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims insofar as the employer's or employee's legal duty as imposed by law.

Appendix A

Misuse of the Michigan State Police Law Enforcement Information Network (LEIN) and its interfaced systems violates Michigan Compiled Law 28.214, Section 4 of the C.J.I.S. Policy Council Act:

(3) A person shall not access, use, or disclose nonpublic information governed under this act for personal use or gain.

(5) A person shall not disclose information governed under this act in a manner that is not authorized by law or rule.

(6) A person who intentionally violates subsection (3) or (5) is guilty of a crime as follows:

(a) For a first offense, the person is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $500.00, or both.

(b) For a second or subsequent offense, the person is guilty of a felony punishable by imprisonment for not more than 4 years or a fine of not more than $2,000.00, or both.

Misuse of the FBI National Crime Information Center (NCIC) is subject to additional federal criminal and/or civil penalties. The federal Privacy Act of 1974 states:

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000. [5 USC Sec.552a(i)]

Misuse of criminal history record information obtained through NCIC violates the Code of Federal Regulation, Title 28, Section 20.25:

Any agency or individual violating subpart B [State and Local Criminal History Record Information] of these regulations shall be subject to a civil penalty not to exceed $11,000 for a violation occurring on after September 29, 1999.

Misuse of Secretary of State (SOS) records violates State of Michigan driver and vehicle privacy protections laws. [MCL 28.295a, 257.902, 257.903, 324.80130d, 324.80319a, 324.81120, 324.82160, and other provisions of law.]

Under Michigan law, a person who makes a false representation or a false certification to obtain personal information or who uses personal information for a purpose other than a permissible purpose identified in the law is guilty of a felony, which may be punishable by imprisonment for up to 5 years and/or a fine of up to $5,000. Subsequent convictions may result in imprisonment for up to 15 years and/or a fine of up to $15,000.

Misuse of motor vehicle records is subject to additional federal criminal and/or civil penalties. The federal Driver's Privacy and Protection Act of 1994 states:

18 USC Sec. 2723:

(a) Criminal Fine. – A person who knowingly violates this chapter shall be fined under this title.

Notice of Criminal Penalties and Civil Action for the Misuse of LEIN

18 USC Sec. 2724:

(a) Cause of Action. – A person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court.

(b) Remedies. – The court may award –

(1) actual damages, but not less than liquidated damages in the amount of $2,500;

(2) punitive damages upon proof of willful or reckless disregard of the law;

I have read and understand the above Notice of Criminal Penalties and Civil Action and I agree to comply with its contents. Further, I understand that any violation of its contents may result in disciplinary action and/or referral for prosecution.

_____

Employee/User Signature Date

_____

Printed Name

APPENDIX B

LEIN SECURITY INCIDENT REPORT

Officer	Today's Date
Incident Date	Incident Time

Incident Type o Computer Security o Lost Information o Other
What computers were affected?
What system was affected?
Did access include any personally identifying information or CJI? If so, what?
What happened?
How did you find out?
What did you do?

Supervisor Notified	Date and Time of Notification

APPENDIX C

CJIS-016 (10/2016)
MICHIGAN STATE POLICE
Criminal Justice Information Center
Page 1 of 2

INFORMATION SECURITY OFFICER (ISO) SECURITY INCIDENT REPORT

AUTHORITY: MCL 28.215, MCL 28.162, and R 28.5201; **COMPLIANCE:** Mandatory; **PENALTY:** Loss of access to criminal justice information systems.

Agencies shall promptly report digital and physical incidents that significantly endanger the security or integrity of Criminal Justice Information (CJI) to the Michigan State Police Information Security Officer (ISO) in compliance with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy. If a question does NOT apply, enter "N/A" to signify not applicable.

Send Completed Hard Copy Form To:	**For Additional Information:**
Michigan State Police Criminal Justice Information Center Attn: Information Security Officer P.O. Box 30634 Lansing, MI 48909-0634	FBI CJIS SECURITY POLICY **Questions/Comments:** Phone: 517-284-3069

I. Agency Information

Point(s) of Contact (Full Name and Title)	Work Phone Number/Extension	Email Address	
Agency Name	Noncriminal Justice Agency ID	Criminal Justice Agency ORI	
Agency Address	City	State	ZIP Code
Date of Report	Date of Incident		

II. Incident Information

Incident Type
☐ Computer Security ☐ Digital Media ☐ Physical Media ☐ Mobile Device

Identify the time frame and the operational phase. (i.e., Was this a one-time occurrence or continuing? Could it occur anytime or do certain events trigger it?)

Location(s) of Incident

System(s) and/or Data Affected (e.g., Computer Aided Dispatch, Records Management System, File Server, Physical Media containing CJI)

Did access include any personally identifying information or CJI?	Is the hard drive encrypted?
☐ Yes ☐ No	☐ Yes ☐ No

Method of Detection/Discovery (e.g., via an audit trail, or accidental discovery)

Describe the incident. Why did this incident happen? What allowed this incident to occur? Were there policies in place which may be applicable to this incident? Should there be controls in place which may help to prevent this type of incident from reoccurring?

Actions Taken/Resolution

What are the vulnerabilities and impacts associated with this incident? Describe what you believe are the vulnerabilities and impacts to other information systems/criminal justice information as a result of this incident. Provide a description/list as to who you believe is affected or vulnerable to a similar incident.

CJIS-016 (10/2016)
MICHIGAN STATE POLICE
Criminal Justice Information Center
Page 2 of 2

III. Additional or Enhanced Incident Response for Mobile Device Operating Scenarios
Did the mobile device contain or access CJI? ☐ Yes ☐ No
Describe the loss of mobile device control. (i.e., was the mobile device known to be locked or unlocked and the duration of the loss)
Was there a total loss of the mobile device? (i.e., the mobile device has not been recovered)
Was criminal justice information stored on the mobile device? Was the mobile device used to access criminal justice information services or systems? Was the mobile device enrolled in Mobile Device Management? Was the mobile device remote locked or wiped? Was your agency able to determine the last known location of the mobile device? Was your agency able to recover the mobile device?
Did the mobile device loss of control, total loss, or compromise occur outside the United States?