

# LAW ENFORCEMENT INFORMATION NETWORK INFORMATION MANUAL



The Michigan Law Enforcement Information Network (LEIN) is a statewide computerized information system established in 1967 as a service to Michigan's criminal justice agencies. It is a repository of wanted person records, personal protection orders, missing persons, and vehicles that are abandoned, stolen, or impounded. Users of the LEIN system include local, state, and federal criminal justice agencies as well as other entities authorized by statute, policy, or rule.

This document provides a brief overview of the State of Michigan and the Federal Bureau of Investigation requirements and procedures for accessing the LEIN system and its associated databases. It is intended to provide helpful information for new and existing user agencies and is *not* all inclusive. Additional information may be obtained by visiting the LEIN Field Services (LFS) website at [www.michigan.gov/LEIN](http://www.michigan.gov/LEIN) or by contacting the LFS staff via the contact information provided within this document.

## WHAT IS LEIN?

The LEIN system is a communication network to supply information across Michigan to criminal justice agencies. It is the portal that links and provides access to various state and national databases including, but not limited to, the following.

- LEIN Hot Files
- Michigan Department of State Vehicle and Driver Record Information System
- Michigan Offender Management Information System
- National Crime Information Center (NCIC) Hot Files
- NCIC Interstate Identification Index
- National Instant Criminal Background Check System (NICS)
- Canadian Police Information Centre
- International Police
- International Justice and Public Safety Network

## LEIN ACCESS GUIDELINES

Access to the LEIN system is limited to the below listed agencies that have applied for and have been approved for access by the Criminal Justice Information Systems Officer (CSO).

### Who may be granted access to LEIN?

- Criminal Justice Agencies
- Correctional Agencies
- Courts (Criminal Divisions only)
- Governmental Law Enforcement Agencies
- Pre-trial Service Agencies
- Probation and Parole Agencies
- Prosecutors
- Non-governmental agencies statutorily vested with arrest powers and whose primary function is the administration of criminal justice
- Governmental agencies with the administration of criminal justice as its primary function and whose governing board has criminal justice agencies as the majority of its members
- Michigan Department of State
- Agencies authorized by statute
- Agencies, entities, or persons approved by the Criminal Justice Information System (CJIS) Agency (CSA) CSO for public safety purposes

### Misuse of LEIN

- Information obtained from the LEIN system must not be disseminated to any unauthorized person and/or entity.
- LEIN, or information obtained from the LEIN system, must not be used for personal reasons.
- Improper dissemination of LEIN information and/or the use of LEIN information for personal reasons may lead to criminal penalties and/or administrative sanctions for the violation of LEIN policy.
- Possible LEIN and/or NCIC violations shall be reported to LFS.
- MCL 28.214, Section 4, of the LEIN Policy Council Act provides for criminal penalties for misuse of LEIN.
- Michigan Commission on Law Enforcement Standards (MCOLES) certified officers found in violation of misuse of LEIN are referred to MCOLES.

## APPLYING FOR ACCESS TO LEIN

To request new or updated access to the LEIN system, contact the Application Analyst of LFS for instructions and for the necessary paperwork.

### New Agencies

The following information is required and must be submitted.

- LEIN User Agreement (CJIS-001) and relevant Addendums
- Management Control Agreement (when applicable)
- Local Area Security Officer (LASO) Appointment form (CJIS-007)
- Network Security Diagram
- Documentation verifying the agency's authority as a criminal justice agency
- Executive Level Training Supplement (*signed and required of all agencies during an audit*)

### Authorized Agencies Making Changes to Service or Adding Devices

Authorized user agencies must notify LFS in writing before changing Interface Providers, making changes to level or method of access, adding devices such as mobile computers or BlackBerries, and/or updating equipment such as firewalls, etc. The following information is required and must be submitted.

- LEIN User Agreement (CJIS-001) and relevant Addendums
- Management Control Agreement (when applicable)
- LASO Appointment form (CJIS-007)
- Network Security Diagram

### Network Security Diagram

All agencies must have a current Network Security Diagram approved by the Information Security Officer (ISO) on file. An updated diagram must be submitted for prior approval anytime a change is proposed, including making changes to level or method of access, change of Interface Provider, adding devices such as mobile computers or BlackBerries, updating equipment such as firewalls, changing connectivity methods, etc. Network Security Diagrams must, at a minimum, include and/or document the following:

- Agency Name
- Statement, "For Official Use Only" (or similar)
- Servers
- Workstations (when applicable)
- Routers
- Firewalls - Including make and model, must be International Computer Security Association certified; verify at [www.icsalabs.com](http://www.icsalabs.com).
- Internet
- If user devices are establishing a Virtual Private Network over the Internet, include the Internet as part of the connection.
- Connection to county (or other agency) and/or connectivity to the State of Michigan
- Other external connections (to the city, clerk, etc.)
- Wireless Access Points – At a minimum, the following information must be provided:
  - Who connects to it;
  - How they are authenticated;
  - How it is secured; and
  - If the Service Set Identifier is broadcasted.
- Mobile Computers (mobile data terminals or mobile computer devices)
  - Provide an explanation of how the mobiles are connecting;
  - How they are authenticating;
  - What type of encryption is used; and
  - If the mobiles can be removed from the vehicle and still access LEIN.
- All CJIS traffic must be encrypted a minimum of 128 bits.

## LEIN ACCESS

Direct Access and Indirect Access are the two types of LEIN access.

### **Direct Access**

Having an electronic device used to perform, or cause to be performed, transactions in LEIN. Types of devices (sometimes referred to as “terminals”) include a desktop computer, access through court management software, in car mobile computer, BlackBerry, etc.

Direct Access agencies must have an approved LEIN User Agreement on file with LFS; must follow all the physical and personnel security requirements; are required to name a LASO and a Terminal Agency Coordinator (TAC); will be audited; must maintain a Network Security Diagram, and submit a Network Security Diagram to LFS for review and approval prior to any changes being made to the network.

### **Indirect Access**

Having no electronic devices used to perform, or cause to be performed, transactions in LEIN. This type of access authorizes an agency to access and use the information obtained from LEIN. An Indirect Access agency must be serviced by another authorized user agency with Direct Access.

Indirect Access agencies must have an approved LEIN User Agreement on file with LFS. All the physical and personnel security requirements must be followed, but the Indirect Access agency is not required to be audited or to name a TAC. Since Indirect Access agencies do not have a device that accesses LEIN, it is not necessary to maintain a Network Security Diagram. Indirect Access agencies are required to assign a LASO.

## METHODS OF ACCESS

Agencies will want to discuss these options with their information technology experts and their city or county partners to find the best option. It is common for agencies to have more than one type of connectivity. For example, an agency may have Direct Access via the Michigan Criminal Justice Information Network (MiCJIN) Portal for desktop access. They may subscribe through another agency to run mobile computers, and SecurID tokens may be used by off site investigators. Please contact the MiCJIN Agency Access Coordinator to discuss connectivity options and to initiate any moves, additions, or changes to your connection.

### **Indirect Access Agency**

The agency contacts an established authorized user agency to have queries run on their behalf. The agency has no Direct Access.

### **Direct Access via the MiCJIN Portal**

This option allows access to the LEIN system, Department of State Driver License Images, Sex Offender Registry, mug shots, etc., with a single sign on. Local Government Extranet (data transmission network) or other connectivity charges may apply, as a direct connection to the state network is required. A station/mnemonic is required. Details can be found at the MiCJIN website at:

[http://www.michigan.gov/msp/0,1607,7-123-1593\\_24055-66415--,00.html](http://www.michigan.gov/msp/0,1607,7-123-1593_24055-66415--,00.html). Access to other applications may also require approval through the MiCJIN Unit.

### **Interface (Provider) Agency**

The agency purchases software from a vendor that provides Direct Access to the LEIN system. Vendor fees, software costs, and connectivity fees may apply. This may be a good option for agencies with many users or who have partner agencies to share costs. Service can be provided to other authorized criminal justice agencies (subscribers). A station/mnemonic is required.

### **Interface Subscriber Agency**

The agency subscribes through another criminal justice agency that has an established network (Interface Agency), such as a county sheriff, court, or dispatch center. The Provider agency may require subscriber to share costs. There are also vendors who can act as Interface Providers. In addition to the cost of the software, vendors may also charge license fees.

### **Token Agency**

Agency uses individual SecurID Tokens (Token) for two factor authentication to connect to the MiCJIN Portal over the Internet to access LEIN. The cost is currently \$132 a year for each Token. Each user requires a Token. Users cannot share Tokens. Agencies cannot send or receive administrative messages when using Tokens.

If accessing LEIN through the MiCJIN Portal, a MiCJIN User Agreement (RI-93) and MiCJIN Service Application (RI-92) are required.

## **AGENCY REQUIREMENTS**

An authorized user agency must agree to and abide by the following requirements.

- A signed agreement must be entered into by completing a LEIN User Agreement (CJIS-001). By signing the LEIN User Agreement, the agency administrator (sheriff, chief of police, dispatch director, court administrator, etc.) enters the agency into the agreement that outlines the responsibilities of all parties and specifies the state and federal requirements to ensure data integrity and privacy of information in LEIN and interfaced systems.
- Prior to testing or implementing connections to the LEIN system, the agency must submit a request with LFS and receive approval. The agency must maintain a detailed Network Security Diagram depicting the connection(s) to LEIN. The Network Security Diagram must be updated and resubmitted to LFS for approval anytime a change is made to the network or devices are added including adding mobile computers, updating firewalls, changing vendors, upgrading connectivity lines, etc.
- The agency must notify LFS in writing and receive prior approval to making any changes to the network or adding devices.
- The agency must comply with federal and state audits by both the Michigan State Police (MSP) LEIN Audit & Training Unit and the Federal Bureau of Investigation (FBI) CJIS Audit Unit.
- Once approved for any type of Direct Access an individual(s) must be designated to serve as a TAC.
- Once approved for any type of Direct Access an individual must be designated to serve as a LASO.
- The agency must complete a Management Control Agreement, when applicable.
- The awareness of and compliance with state and federal statutes, the LEIN Administrative Rules, the Michigan and Federal CJIS security policies, the procedures outlined in the LEIN Operations Manual, and in the NCIC Operating Manual.
- When records have been entered into LEIN, the agency must complete monthly validations to ensure accuracy and completeness of the records and ensure the validity of their supporting documents (warrants, missing person reports, etc.).
- All records entered into LEIN must be able to be confirmed as valid 24 hours a day, seven days a week. Agencies who enter records, but are not open 24 hours a day and seven days a week, must seek an alternate method for achieving this standard.

- The following local policies must be in place and must also have a system solution in place to satisfy all policy requirements.
  - Procedures for completing monthly validations.
  - Acceptable Use Policy (including standards of discipline and criminal penalties).
  - Anti-virus guidelines.
  - Penalties for misuse of LEIN.
  - Media and hard copy handling procedures (disposal, secondary dissemination, etc.).
  - Password policy and procedures.
  - Passwords shall be a minimum length of eight (8) characters.
  - Passwords shall not be a dictionary word or proper name.
  - Passwords and the User ID shall not be the same.
  - Passwords shall expire within a maximum of 90 calendar days.
  - All systems shall prevent password reuse of the last ten passwords.
  - Passwords shall not be transmitted in the clear outside the secure domain.
  - Passwords shall not be displayed when entered.
- Unique Identifier Policy and procedures.
- Access to LEIN, or information obtained from LEIN, is permitted only under the management control of criminal justice agencies in the discharge of their official mandated responsibilities.

### **Physical Security**

All devices that provide Direct Access to LEIN (desktops, mobile computers, servers, etc.), as well as the data obtained from LEIN, must be located or stored in secured environments, under the management control of an approved criminal justice agency. Devices must not be accessible to the public or to persons not authorized to operate, view, or possess data transmitted or received by LEIN.

### **Personnel Security**

Proper background checks and fingerprinting must be completed on all LEIN operators, those who manage or administer the information technology infrastructure, unescorted agency or nonagency personnel, and anyone else with access to information obtained from the LEIN system.

- Proper and complete background investigations should include the following LEIN queries.
  - State of Michigan and FBI fingerprint search
  - LEIN and NCIC Wanted Files
  - Criminal History Records - PURPOSE (52): (?)/ (POSITION)
  - Department of State Driver Records
  - Corrections Management Information System

### **TAC**

The TAC shall be a person versed and knowledgeable in rules, regulations, applications, and operation of LEIN and NCIC and the interfaced computer systems. The TAC shall have the authority to act on behalf of the departmental agency administrator for liaison with LFS.

The TAC serves as the agency's main point of contact for LEIN related issues. The TAC maintains, updates, distributes, and provides LEIN associated information to users within their agency. The TAC ensures system integrity with regard to security, access, and dissemination of LEIN information. The TAC coordinates training and certification of agency users, and ensures all LEIN and NCIC policies, rules, and statutes, as well as proper local agency policies and procedures are enacted and followed.

### **Testing and Training**

- All TACs must attend a LEIN Basic TAC School and all subsequent LEIN TAC Update Schools. New agency TACs are expected to attend the first available LEIN Basic TAC School.

- TACs are responsible for providing training and the operator test to users.
- LEIN operators must be certified (trained and tested) in order to operate LEIN without direct supervision.

### **Operator Certification**

All operators must be certified (trained and tested) within six months of employment or assignment.

### **Operator Recertification**

All certified operators must be tested and recertified biennially (every two years). Failure to pass the operator certification test within six months of hire, or failure to recertify biennially, will render an employee ineligible to operate LEIN.

### **Security Training**

All LEIN operators, as well as those managing the information technology infrastructure, are required to attend security awareness training every two years, in accordance with the FBI CJIS Security Policy. Testing is not required, but documentation must be maintained.

### **LASO**

All agencies with access to LEIN information must designate an individual to serve as a LASO.

The LASO serves as the local agency's point of contact for security related issues. The LASO is responsible for ensuring only authorized users have access to LEIN and related systems; reporting any security incidents to the MSP ISO; identifying and documenting how equipment is connected to the state system, and maintaining an up to date Network Security (topological) Diagram at all times (when applicable); ensuring that personnel security screening procedures are being followed; ensuring that appropriate hardware security measures are in place; assisting with security awareness training; and establishing and maintaining management control agreements with noncriminal justice agencies, including CJIS Security Addendums where applicable.

## **INFORMATION SOURCES**

The LEIN and CJIS systems operate under strict guidelines including both state and federal rules and policies. Sources of detailed information regarding use, dissemination, security, and other requirements may be obtained from the following sources.

- Michigan CJIS Security Policy
- LEIN Operations Manual
- NCIC Operating Manual
- PA 163 of 1974, as amended, MCL 28.214
- FBI CJIS Security Policy
- LEIN TAC Manual
- Michigan CJIS Administrative Rules

Authorized users may download copies of the above sources online at [www.michigan.gov/lein](http://www.michigan.gov/lein). Many of the information sources on this website are encrypted, as required by the FBI CJIS Security Policy, and require a password for access. Authorized users receive this password monthly through a LEIN all-terminal message with the monthly validation notices. The password changes every 90 days.

The Criminal Justice Information Center distributes a quarterly publication, *The RAP Sheet*, which contains information and updates related to LEIN and CJIS systems. Additionally, LFS distributes information related to LEIN and CJIS systems through a Listserv. Criminal justice personnel wishing to be placed on *The RAP Sheet* distribution list or the Listserv may send an e-mail request containing name, agency name, mailing address, telephone number, and e-mail address to [mspleinfss@michigan.gov](mailto:mspleinfss@michigan.gov).

## FREQUENTLY ASKED QUESTIONS

**1. May information obtained through LEIN be disclosed under the Freedom of Information Act (FOIA)?**

Information obtained from LEIN is not subject to disclosure under FOIA, and must be redacted prior to fulfilling FOIA requests. For MSP work sites, when a subpoena is presented for LEIN and/or NCIC information, it should be immediately forwarded to the FOIA Unit of the MSP. Other law enforcement should follow their department protocol.

**2. How often will agencies be audited?**

At a minimum, all agencies with Direct Access to LEIN must submit to a triennial audit by the MSP and may also be subject to a triennial audit by the FBI CJIS Division. Follow up audits may take place when necessary.

**3. Why must we complete a LEIN application when requesting Sex Offender Registry (SOR) and/or Automated Pistol Registration System (APRS)?**

Enhancements to the SOR and APRS applications allow users to access criminal history information and Hot File information via LEIN directly from within the application. The SOR and/or APRS terminal must be treated as a LEIN terminal for security purposes. Therefore, it is necessary for your agency to be approved for Direct Access to the LEIN system.

**4. What is a Security Addendum, and when does an agency need to complete it?**

A Security Addendum is an agreement between the government agency and a private contractor, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Criminal justice agencies are required to complete a Security Addendum with every employee of any contractor with approved access to CJIS systems or CJIS information. Agencies may obtain a copy of the Security Addendum at [www.michigan.gov/lein](http://www.michigan.gov/lein).

**5. What is considered improper LEIN use?**

Improper use of LEIN occurs when LEIN is utilized for an unauthorized noncriminal justice purpose. Specific examples include, but are not limited to, running LEIN on yourself, friends, or family members for noncriminal justice purposes; running yourself as a test record; running a license plate to get information on a driver for personal interests; running yourself or a family member to get driving record information for insurance purposes; running a family member to determine if a Personal Protection Order or other court order has been issued, and running a citizen for a military recruiter.

**6. How do you report a possible LEIN violation?**

Complaints regarding the potential misuse of LEIN should be directed to the LFS Policy Analyst at (517) 241-0639 or to [mspleincomplaints@michigan.gov](mailto:mspleincomplaints@michigan.gov).

**7. Can I cut and paste data from LEIN into a report?**

Previous policies that restricted the cutting and pasting of data from LEIN into a report were rescinded. Agencies must continue to adhere to dissemination and FOIA rules and policies.

**8. How long should an agency retain monthly validation reports?**

Agencies must retain the most current copy of each validation listing for one year plus the current year.

## CONTACT INFORMATION

<b>Criminal Justice Information Center</b>			
Name	Title	Telephone	E-mail
Dawn Brinningstaull	CJIC Director	(517) 241-0604	<a href="mailto:brinnid@michigan.gov">brinnid@michigan.gov</a>
Terri Smith	ISO	(517) 241-0607	<a href="mailto:smithta@michigan.gov">smithta@michigan.gov</a>
<b>LEIN Field Services</b>			
Peggy Hines	Section Manager	(517) 241-0702	<a href="mailto:hinesp@michigan.gov">hinesp@michigan.gov</a>
Diane Doubrava	Section Secretary	(517) 241-0667	<a href="mailto:doubravad@michigan.gov">doubravad@michigan.gov</a>
Pam Cruz	Application Analyst (Billing; Paperless Warrants; Service Requests)	(517) 241-0658	<a href="mailto:cruzpj@michigan.gov">cruzpj@michigan.gov</a>
Vacant	Operations Analyst (Technical Assistance)	(517) 241-0703	
Liz Canfield	Policy Analyst (LEIN Use Complaints; Policy Assistance)	(517) 241-0639	<a href="mailto:Canfielde@michigan.gov">Canfielde@michigan.gov</a>
Jerry Scott	Data Integrity Technician (LEIN Validations; Record Integrity Assistance)	(517) 241-0787	<a href="mailto:scottjl@michigan.gov">scottjl@michigan.gov</a>
<b>LEIN Audit &amp; Training Unit</b>			
Kevin Collins	Audit & Training Unit Manager	(517) 241-0641	<a href="mailto:collinsk@michigan.gov">collinsk@michigan.gov</a>
Ryan Mainz	Detroit Region Auditor	(734) 525-4483	<a href="mailto:mainzr@michigan.gov">mainzr@michigan.gov</a>
Ann Vogel	Gaylord Region Auditor	(989) 732-9836	<a href="mailto:vogelann@michigan.gov">vogelann@michigan.gov</a>
Suzan Clark	Saginaw Region Auditor	(989) 758-1581	<a href="mailto:clarks10@michigan.gov">clarks10@michigan.gov</a>
Vacant	Grand Rapids Region Auditor		
<b>MiCJIN Service Center</b>			
Mitzi Goldstein	Unit Manager	(517) 241-0693	<a href="mailto:goldstem@michigan.gov">goldstem@michigan.gov</a>
Dave Bennett	Agency Access Coordinator (Connectivity to MSP Applications)	(517) 241-0615	<a href="mailto:bennett5@michigan.gov">bennett5@michigan.gov</a>
Therese Hudak	Portal Technician (Connectivity Troubleshooting)	(517) 241-0798	<a href="mailto:hudakt@michigan.gov">hudakt@michigan.gov</a>
Bradley Rahn	Portal Technician (SecurID Tokens; User Account Assistance)	(517) 241-0764	<a href="mailto:rahnb@michigan.gov">rahnb@michigan.gov</a>

