# LEADS SECURITY POLICY


**Document Date: February 2021**

**LAW ENFORCEMENT AGENCIES DATA SYSTEM (LEADS)**
**SECURITY POLICY**
Version 2.2
Document Date: February 2017

# Table of Contents

# 1.0 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints. The sections in this document may enhance or clarify a policy statement from the CJIS Security Policy, or may add additional policy statements required by the CJIS Systems Agency. Should a section in this document enhance or clarify a section of the CJIS Security Policy, the section will reference the CJIS Security Policy statement at the end of the section and that reference will appear in parentheses with the letters CSP and the section number of the CJIS Security Policy being referenced.

## *1.1 Purpose*

The Illinois State Police (ISP) embraces the ***FBI CJIS Security Policy (CSP)*** as the base security policy for the State of Illinois. The CSP provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of requirements for the access to FBI CJIS Division's systems and information and to protect and safeguard Criminal Justice Information (CJI).

Consistent with, and in addition to the CSP, each Illinois CJA and NCJA shall adhere to the rules contained in this ***LEADS Security Policy***. These additional rules, more stringent than those imposed by the CSP, shall be followed by all agencies that access CJI in the State of Illinois. This document contains only those policy statements that clarify, provide additional detail, or impose more stringent requirements than what is contained in the CSP. ***(CSP 1.1)***

## *1.2 Scope*

CJIS and LEADS Security Policies provide minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, and/or destruction of CJI (See CJI Definition, Section 4.1). ***(CSP 1.2)***

## *1.3 Relationship to Local Security Policy*

A local agency may complement the CJIS and LEADS Security Policies with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS and LEADS Security Policies shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS and LEADS Security Policy standards. ***(CSP 1.3)***

## *1.4 Distribution of the LEADS Security Policy*

The LEADS Security Policy is a publically available document and may be posted and shared without restrictions. ***(CSP 1.5)***

# 2.0 LEADS SECURITY POLICY APPROACH

The LEADS Security Policy, as a companion to the CSP, represents the shared responsibility between the FBI CJIS Division, the ISP, and the criminal and noncriminal justice users of their information systems and data regarding the lawful use and appropriate protection of CJI. ***(CSP 2.0)***

# 3.0 ROLES AND RESPONSIBILITIES

It is the responsibility of all agencies covered under this policy to ensure the protection of Criminal Justice Information (CJI) between the FBI CJIS Division, the Illinois State Police, and their user communities.

## *3.1 Roles and Responsibilities for Agencies and Parties*

### 3.1.1 CJIS Systems Agency (CSA)

The FBI has designated the Illinois State Police (ISP) as the CSA[1] for the State of Illinois. ***(CSP 3.2.1)***

### 3.1.2 CJIS Systems Officer (CSO)

The ISP Director shall designate a statewide administrator from the CSA for the administration and management of the CJIS network and Illinois systems connecting to that network. The ISP Director has designated the LEADS Administrator as the CSO. ***(CSP 3.2.2)***

### 3.1.3 LEADS Terminal Agency Coordinator (LAC/TAC)

Every LEADS terminal agency shall appoint one employee as its LAC. ***(CSP 3.2.3)***

### 3.1.4 Local Agency Security Officer (LASO)

Criminal justice information security responsibilities at the LEADS agency shall be managed by the agency's Local Agency Security Officer (LASO). The LASO may be the LEADS Agency Coordinator (LAC), Chief, Sheriff or other management designated by the chief agency administrator. ***(CSP 3.2.9)***

# 4.0 CRIMINAL JUSTICE INFORMATION (CJI) AND PERSONALLY

1 CJIS Systems Agency (CSA) – A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory.

# IDENTIFIABLE INFORMATION (PII)

## *4.1 Criminal Justice Information (CJI)*

Criminal Justice Information is the term used to refer to all of the FBI CJIS and ISP provided data necessary for law enforcement and civil agencies to perform their missions, including but not limited to biometric, identity history, biographic, property, and case/incident history data. For purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked to a specific individual. ***(CSP 4.1)***

### 4.1.1 Criminal History Record Information (CHRI)

Due to its comparatively sensitive nature, controls required for the access, use, and dissemination of CHRI are defined in the Code of Federal Regulations, Title 28, Part 20. Regarding CHRI (both Illinois CHRI and III) **obtained through LEADS**, inquiries shall be made by a **criminal justice agency** for a **criminal justice purpose**. Both criteria must be met. (See Code of Federal Regulations, Title 28, Part 20.3 for definitions of *Administration of Criminal Justice* and *Criminal Justice Agency*). ***(CSP 4.1.1)***

## *4.2 Access to, Use, and Dissemination of LEADS/NCIC Data*

### 4.2.1 Proper Access and Dissemination of Data Obtained Through LEADS

Illinois Joint Committee on Administrative Rules, Title 20, Corrections, Criminal Justice, and law Enforcement, Chapter II: Department of State Police, Part 1240: Law Enforcement Agencies Data System – LEADS:

1. The LEADS network and LEADS data shall not be used for personal purposes.
2. Personal or unofficial messages shall not be transmitted.
3. LEADS data shall not be sold.
4. LEADS data shall not be disseminated to any individual or organization that is not legally authorized to have access to the information.

It is a violation of both state and federal law for information **obtained through LEADS** (CHF, NCIC, CHRI, III, SOS, etc.) to be used for licensing (such as day care centers, liquor license, taxi cab drivers, etc.) or noncriminal justice employment (such as fire departments, villages, towns, etc.). Criminal background checks of these types shall be performed by requesting a noncriminal

justice name and/or fingerprint-based check through the Illinois State Police, Bureau of Identification.

#### 4.2.2 Standards of Discipline

Participating criminal justice agencies shall have appropriate written standards for discipline of LEADS and CJIS Security Policy violations including, but not limited to unauthorized use, access, and/or dissemination. Existing agency discipline policies may be modified to include sanctions for LEADS and NCIC infractions. If misuse of LEADS/NCIC/CHRI is discovered, the chief agency administrator shall conduct an internal investigation and notify LEADS Administration in writing of the investigative findings and corrective action taken.

# 5.0 POLICY AND IMPLEMENTATION

## *5.1 Information Exchange Agreements*

#### 5.1.1 Criminal Justice Agency User Agreement

Any criminal justice agency that requests access to LEADS and NCIC data shall enter into a current, signed written agreement (LEADS Agreement) with the appropriate signatory authority of the ISP and the criminal justice chief agency administrator. ***(CSP 5.1.1.3)***

#### 5.1.2 Management Control Agreements

Any governmental Noncriminal Justice Agency (NCJA) that provides criminal justice services to a Criminal Justice Agency (CJA) shall be eligible for access to CJI through the execution of a Management Control Agreement.

The Management Control Agreement stipulates that management control of the criminal justice function remains solely with the CJA. An example of its use would be a City PD (CJA) that utilizes the IT services of the city (NCJA). The Management Control Agreement authorizes the NCJA employees to have access to the CJI, and allows the CJA to ensure that all services provided by the NCJA meet the requirements of the CJIS and LEADS Security Policies. The Management Control Agreement can be found in the CSP Appendix and the LEADS 2000 Security Web Site.

It is not necessary for private contractors to sign a Management Control Agreement. The contract signed by the CJA and the private contractor shall incorporate the necessary language to ensure the private contractor will follow the CJIS and LEADS Security Policies, including proper employee screening and the safeguarding of the CJI. ***(CSP 5.1.1.4)***

### 5.1.3 CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the CJA and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulation and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require. The CJIS Security Addendum can be found in the CSP Appendix and on the LEADS 2000 Security Web Site.

Each employee of a private contractor who will have access to CJI shall sign the signature page of the CJIS Security Addendum, and each CJA shall maintain the signed Security Addendum(s) for their records. ***(CSP 5.1.1.5)***

### 5.1.4 Secondary Dissemination

Each transaction that involves any extra-agency release (release to any authorized agency other than your own) of CHRI as supplied by LEADS/NCIC shall be logged in a Secondary Dissemination Log maintained by the servicing agency for a minimum of three years. ***(CSP 5.1.2)***

## *5.2 Security Awareness and Certification Training - Direct/Indirect Access*

Each LEADS agency shall ensure all authorized personnel with direct access[2] to data, indirect access[3] to data, and information technology roles are trained and/or certified at the appropriate level. Personnel with direct or indirect access to CJI, within six months of employment or assignment, shall successfully complete the appropriate training and/or certification required for their level of access. ***(CSP 5.2)***

## *5.3 Incident Response*

### 5.3.1 Reporting Information Security Events

The agency's LASO shall report system security incidents in the agency's area of responsibility to the CSA ISO. Notifications shall be made by completing the Computer Security Incident Reporting form located in Appendix A.1 at the end of this document or download the form from the LEADS 2000 Security Web Site.

2 Direct Access – Authorized users have the ability to conduct transactional activities themselves (the capability to query and/or update) on the local, state, or national systems.

3 Indirect Access - Authorized users do not conduct transactional activities on local, state, or national systems themselves, but can view and/or utilize the CJI in their work duties.

Submission instructions are located at the bottom of the Computer Security Incident Reporting form. ***(CSP 5.3.1)***

## *5.4 Access Control*

### 5.4.1 Wireless Access Restrictions

Agencies shall complete the LEADS Interface CDC Assignment form located on the LEADS 2000 Interface Agencies Web Site.

The ISP LEADS 2000 web-browser with receiver client is not authorized to be used for access to LEADS on a Mobile/Remote/Handheld device. ***(CSP 5.13.1)***

## *5.5 Identification and Authentication*

### 5.5.1 Authentication Policy and Procedures

Each person who is authorized to store, process and/or transmit CJI shall be uniquely identified when logging into systems containing CJI. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. This requirement applies regardless of the method used to access LEADS including interface agencies, wireless, LEADS 2000 web-browser client, etc. ***(CSP 5.6.1)***

#### 5.5.1.1 Standard Authentication (Password)

Agencies shall follow secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum of eight (8) characters on all systems.[4]
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Expire within a maximum of 90 calendar days.[5]
5. Not be identical to the previous ten (10) passwords.[6]
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered. ***(CSP 5.6.2.1.1)***

#### 5.5.1.2 Confidentiality

Passwords shall be kept confidential and not shared between users.
Exception: In an emergency, if it is required to divulge a password to

4 Exception: For LEADS2000 users only, ISP's current version of RACF requires the password contain at least one number.
5 Exception: For LEADS2000 users only, ISP's current version of RACF sets the password expiration at 35 days.
6 Exception: For LEADS2000 users only, ISP's current version of RACF sets password reuse at 32 generations.

another user, the password shall be changed immediately during next user log-on.

## *5.6 Configuration Management*

Each LEADS agency shall maintain a standard site configuration diagram showing all LEADS terminals, network connections and firewall placement. Additionally, an accurate listing of all LEADS terminals/workstations, including their CDC and/or logical identification number must be maintained. This information shall be provided to the LEADS Administrator upon request.

Each LEADS agency shall maintain procedures requiring the agency's LASO, LAC, Chief, Sheriff or other management signature approval of all network modifications (new terminal devices added and interfaces to other systems and networks). ***(CSP 5.7.1.2)***

## *5.7 Personnel Security*

### 5.7.1 Personnel Security Policy and Procedures

#### 5.7.1.1 Background Screening

To verify identification and authorization to access CJI, a state of residency and national fingerprint-based CHRI check using the Criminal Justice Applicant fingerprint card shall be conducted for personnel with direct access, indirect access, Information Technology Support, contractors, and other persons who have unescorted access to CJI, regardless of the frequency of access. Once the Criminal Justice Applicant card has been submitted to the ISP Bureau of Identification, the ISP will forward the background request to the FBI.

If results of the state of residency or FBI fingerprint-based background check confirms a felony conviction, the individual's access to LEADS and CJI will be prohibited. No person will be permitted LEADS access (including persons who provide maintenance or technical services), or unescorted access to CJI unless they are of good character and have not been convicted of a felony or a crime involving moral turpitude under the laws of this or any other jurisdiction. Any person may have their LEADS access denied if charged with a felony or crime of moral turpitude under the laws of this or any other jurisdiction. ***(CSP 5.12.1)***

#### 5.7.1.2 Personnel Termination

Upon termination, suspension, leave of absence or transfer of an employee, the User ID account for LEADS/NCIC shall be disabled, revoked or deleted as necessary to prevent unauthorized access. It is the responsibility of the agency's LAC to ensure this procedure is performed. ***(CSP 5.12.2)***

**Appendix A.1**

**LAW ENFORCMENT AGENCIES DATA SYSTEM**
**INFORMATION SECURITY OFFICER (ISO)**

# COMPUTER SECURITY INCIDENT REPORTING FORM

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT: _____ PHONE/EXT/E-MAIL: _____

LOCATION(S) OF INCIDENT: _____

SYSTEM(S) AFFECTED: _____

_____

METHOD OF DETECTION: _____

NATURE OF INCIDENT: _____

_____

INCIDENT DESCRIPTION: _____

_____

ACTIONS TAKEN/RESOLUTION: _____

_____

_____

**Submit To:** **CSA ISO/LEADS**
Illinois State Police
Attn: Bob Libman
260 N. Chicago St.
Joliet, IL 60586
(815) 740-3064
Fax: (815) 740-8799
LEADSISO@isp.state.il.us