ILLINOIS STATE POLICE DIRECTIVE
SRV-223, ACCESS TO CRIMINAL JUSTICE INFORMATION

RESCINDS:	**REVISED:**
NEW	05-01-2023 **2023-155**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):** 11.4.1, 11.4.4, 11.4.5, 40.1.1, 40.2.1, 42.1.3, 82.1.1, 82.1.6, 82.2.4, 82.3.6

I. POLICY

The Illinois State Police (ISP) will provide access to criminal justice information for ISP users for the purpose of conducting authorized ISP and/or State of Illinois business. ISP will ensure that all employees who have access to criminal justice information are trained and/or certified on proper handling of access, use, dissemination, and destruction of criminal justice information.

II. AUTHORITY

II.A. FBI CJIS Security Policy, Version 5.9.2 12/07/2022, or most current version

II.B. Illinois Administrative Code Title 20, Part 1240 – Law Enforcement Agencies Data System (LEADS)

II.C. LEADS Security Policy, Version 2.2 02/01/2017, or most current version

II.D. All relevant federal and state rules, regulations, laws, and policies that govern the access and use of criminal justice information maintained by the ISP, or accessible to the ISP, despite the method of interface system.

III. DEFINITIONS

III.A. Criminal Justice Information (CJI) – information collected by criminal justice agencies that is needed for the fulfillment of their mission including, but not limited to biometric data, identity history data, biographic data, property data, and case/incident history in all systems housed by ISP and/or accessible to ISP employees.

III.B. Law Enforcement Agencies Data System (LEADS) – a statewide, computerized telecommunications information system designed to provide services, information, and capabilities to the law enforcement and criminal justice community in the state of Illinois. LEADS allows access to criminal justice information including, but not limited to, Hot Files (HF), Criminal History Record Information (CHRI), Firearm Owner's Identification (FOID), Concealed Carry License (CCL), Motor Vehicle Registration and Driver's Information and Imaging (SOS), the FBI's National Crime Information Center (NCIC/III), and the International Justice and Public Safety Network (NLETS).

III.C. Least Privilege – applied to employees, the principle of least privilege translates to authorizing information system access at the lowest level of rights a user can have and still do their job.

IV. PROCEDURES

IV.A. CJI Training and/or Certification

IV.A.1. Supervisors of ISP or contractual employees, who as part of their job duties have physical and/or logical; direct and/or indirect access to CJI, will ensure employee(s) complete training and certification as required by all federal and state rules, regulations, laws, and policies that govern access to CJI.

IV.A.2. Supervisors of contractual employees with access to CJI will ensure contractual employee(s):

IV.A.2.a. Read and sign a Federal Bureau of Investigation Criminal Justice Information Services Security Addendum, form ISP 2-683, and maintain a copy of the signed form ISP 2-683 on behalf of the Department.

IV.A.2.b. Certify at the appropriate level of FBI CJIS Security Awareness Training.

IV.B. Authorizing Access/Least Privilege

IV.B.1. Supervisors will only authorize access to systems containing CJI if it is required for the completion of job duties.

IV.B.2. Security Administration for systems containing CJI is not centralized. Supervisors shall contact the appropriate authorizing entity responsible for granting, modifying, or removing access to systems containing CJI.

IV.B.3. Security Administrators for systems containing CJI shall grant access consistent with the concept of least privilege.

IV.C. Personally-Owned Devices

Access to systems containing CJI by users from personally-owned devices/information systems will be evaluated on a case-by-case basis based upon operational need, security, and access requirements. This assessment will be consistent with the FBI CJIS Security Policy controls outlined in Section 5.5.6.1 – Personally Owned Information Systems.

-End of Directive-