
Protected Information

802.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the Alsip Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Department and not the public records information covered in the Records Maintenance and Release Policy.

802.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the Alsip Police Department and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

802.2 POLICY

Members of the Alsip Police Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

802.3 RESPONSIBILITIES

The Chief of Police shall select a member of the [Department/Office] to coordinate the use of protected information.

The responsibilities of this position include but are not limited to (20 Ill. Adm. Code 1240.90):

- (a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Illinois Secretary of State records, and the Illinois Law Enforcement Agencies Data Systems (LEADS).
- (b) Developing, disseminating, and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy. See the Alsip Police Department CJIS Access, Maintenance, and Security Policy for additional guidance.
- (c) Developing, disseminating, and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release, and security of protected information.
- (d) Developing procedures to ensure training and certification requirements are met.
- (e) Resolving specific questions that arise regarding authorized recipients of protected information.
- (f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

Protected Information

802.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Alsip Police Department policy, or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access (20 Ill. Adm. Code 1240.50).

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution (20 ILCS 2630/7; 20 Ill. Adm. Code 1240.50). See the CJIS Access, Maintenance, and Security Policy for additional guidance.

802.4.1 PENALTIES FOR NON-COMPLIANCE OR MISUSE OF RECORDS

The Department of State Police may suspend all or any portion of LEADS service without prior notification as the result of an agency's non-compliance with laws, rules, regulations, or procedures. The Director of State Police may suspend all or part of LEADS service for agency for violations of LEADS laws, rules regulations, or procedures (20 Ill. Adm. Code 1240.110).

It is a Class A misdemeanor to furnish, buy, receive, or possess LEADS information without authorization by a court, statute, or case law (20 ILCS 2630/7).

802.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know (20 Ill. Adm. Code 1240.50; 20 Ill. Adm. Code 1240.80).

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Clerk for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Unit to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of officers, other department members or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

Protected Information

802.6 SECURITY OF PROTECTED INFORMATION

The Chief of Police will select a member of the [Department/Office] to oversee the security of protected information.

The responsibilities of this position include but are not limited to (see the CJIS Access, Maintenance, and Security Policy for additional guidance):

- (a) Developing and maintaining security practices, procedures, and training.
- (b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems (20 Ill. Adm. Code 1240.50).
- (c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents, including computer attacks.
- (d) Tracking, documenting, and reporting all breach of security incidents to the Chief of Police and appropriate authorities.

802.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it (20 Ill. Adm. Code 1240.80). This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal) (20 Ill. Adm. Code 1240.50).

802.6.2 MAINTENANCE AND TECHNICAL SERVICES

The personnel security requirement for a LEADS agency requires conformance with 20 Ill. Adm. Code 1240.50. Generally, no person may provide maintenance or technical services at or near LEADS equipment 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 his/her authority to provide maintenance or technical services at or near LEADS equipment denied if he/she is charged with a felony or a crime involving moral turpitude under the laws of this or any other jurisdiction (20 Ill. Adm. Code 1240.50(3)).

802.6.3 PROTECTION OF LEADS DATA

LEADS data shall not be included on the violator's copy of any citation that is not delivered by hand to the violator. This specifically includes citation copies left on an unattended vehicle, a building or any other place where the violator is not present to receive the citation. LEADS data will continue to be included on other copies of the citation that are kept by the employee and/or the Department (18 USC § 2721 through 18 USC § 2725).

802.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies

Alsip Police Department

Policy Manual

Protected Information

authorized access and use of protected information, as well as its proper handling and dissemination.