
Protected Information

812.1 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 Elk Grove 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.

812.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the Elk Grove 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.

812.2 POLICY

Members of the Elk Grove 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.

812.3 RESPONSIBILITIES

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

The responsibilities of this position include, but are not limited to:

- (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), Department of Motor Vehicle (DMV) records and California Law Enforcement Telecommunications System (CLETS).
- (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.
- (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.

Elk Grove Police Department

Elk Grove PD Policy Manual

Protected Information

- (f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

812.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Elk Grove 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.

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.

812.4.1 PENALTIES FOR MISUSE OF RECORDS

It is a misdemeanor to furnish, buy, receive or possess Department of Justice criminal history information without authorization by law (Penal Code § 11143).

Authorized persons or agencies violating state regulations regarding the security of Criminal Offender Record Information (CORI) maintained by the California Department of Justice may lose direct access to CORI (11 CCR 702).

812.4.2 RELEASE OF CORI

Only the persons listed below are authorized to release CORI. Each authorized person releasing CORI is responsible to ensure that each request granted appears legitimate and that the requester is an authorized recipient with a right and need to know.

- (a) Criminal Records Security Officer
- (b) Records Manager
- (c) Full-time employees of the Records Bureau
- (d) Personnel specifically designated in writing by Division Commanders with the concurrence of the Criminal Records Security Officer

812.4.3 RELEASE OF CORI TO FIELD PERSONNEL

Personnel shall not have access to CORI until a background investigation has been completed and approved.

CORI shall not be transmitted by radio broadcast or through computer terminals to field personnel or vehicles. Nothing in this procedure is intended to prohibit broadcasting warrant information concerning wanted persons or limited release of offense information for officer safety.

812.5 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.

Elk Grove Police Department

Elk Grove PD Policy Manual

Protected Information

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 Manager 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 Bureau 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.

812.5.1 REVIEW OF CRIMINAL OFFENDER RECORD

Individuals requesting to review their own California criminal history information shall be referred to the Department of Justice (Penal Code § 11121).

Individuals shall be allowed to review their arrest or conviction record on file with the Department after complying with all legal requirements regarding authority and procedures in Penal Code § 11120 through Penal Code § 11127 (Penal Code § 13321).

812.6 SECURITY OF PROTECTED INFORMATION

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

The responsibilities of this position include, but are not limited to:

- (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.
- (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.

812.6.1 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. This includes leaving protected information, such as documents or computer databases, accessible to others

Elk Grove Police Department

Elk Grove PD Policy Manual

Protected Information

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).

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

812.7.1 COMPUTER TERMINAL SECURITY

Computer terminal equipment capable of providing access to automated criminal offender record information is located in the Records Bureau, the Dispatch Center and in the Detective Division to preclude access by unauthorized persons.

No employee shall be authorized to operate computer terminal equipment with access to CORI until the operator has completed the appropriate training.

812.7.2 DESTRUCTION OF CORI

When any document providing CORI has served the purpose for which it was obtained, it shall be destroyed by shredding.

Each employee shall be responsible for destroying the CORI documents they receive.

812.7.3 CUSTODIAN OF CRIMINAL RECORDS

The Records Manager, unless otherwise directed by the Support Services Division Manager, shall be the Department's official Custodian of Criminal Records. The Custodian of Criminal Records shall be responsible for the security, storage, dissemination and destruction of criminal records, and will serve as a primary contact for the California Department of Justice for any related issues. The Records Manager may appoint other department employees to the role of Custodian of Criminal Records, who will share the same responsibilities regarding criminal records.

The Administration will ensure that he/she makes the appropriate applications and notifications to the California Department of Justice regarding the Department's Custodian of Criminal Record appointments, per the requirements of Penal Code § 11102.2.

This subsection is not intended to interfere with any other employee acting as a custodian of records for other statutory purposes but is narrowly tailored to address issues of criminal history records.

812.8 TRAINING PROGRAM

All personnel authorized to process or release CORI shall be required to complete a training program prescribed by the Criminal Record Security Officer. The Training Bureau shall coordinate the course to provide training in the proper use, control, and dissemination of CORI.

Elk Grove Police Department

Elk Grove PD Policy Manual

Protected Information

812.9 PENALTIES FOR MISUSE OF RECORDS

Penal Code §§ 11140 and 11144 make it a misdemeanor to furnish, buy, receive, or possess Department of Justice rap sheets without authorization by a court, statute, or case law.

Title 11, California Administrative Code § 702 provides that authorized persons or agencies violating the Regulations Regarding the Security of Criminal Offender Record Information in California may lose direct access to CORI maintained by the California Department of Justice.

Divulging the content of any criminal record to anyone other than authorized personnel is a violation of Policy.

Employees who obtain, or attempt to obtain, information from the department files other than that to which they are entitled in accordance with their official duties is a violation of Policy.