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 Escalon 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 Escalon 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 Escalon 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.

(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, Escalon 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).

812.5 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.

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 Police Services 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).

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).

812.5.2 TRANSMISSION GUIDELINES

Protected information, such as restricted Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should not be transmitted via unencrypted radio. When circumstances reasonably indicate that the immediate safety of officers, other department members, or the public is at risk, only summary information may be transmitted.

In cases where the transmission of protected information, such as Personally Identifiable Information, is necessary to accomplish a legitimate law enforcement purpose, and utilization of an encrypted radio channel is infeasible, a MDC or department-issued cellular telephone should be utilized when practicable. If neither are available, unencrypted radio transmissions shall be subject to the following:

- Elements of protected information should be broken up into multiple transmissions, to minimally separate an individual's combined last name and any identifying number associated with the individual, from either first name or first initial.
- Additional information regarding the individual, including date of birth, home address, or physical descriptors, should be relayed in separate transmissions.

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

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 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).

812.6.2 MEDIA PROTECTION

The following standards establish reasonable for the handling, transmission, storage, and disposal of confidential and sensitive CJI and/or PII.

Definition for the terms “confidential” CJI, CHRI and “personal” PII.

Criminal Justice Information (CJI)

Criminal Justice Information (CJI) is the term used to refer to all of the FBI CJIS 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 data. The following categories of CJI describe the various data housed by the FBI CJIS architecture:

1. Biometric Data - data derived from one or more intrinsic physical or behavioral trains of human typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include fingerprints, iris scans, and facial recognition data.
2. Identity History Data – textual data that corresponds with an individuals' biometric data providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data - information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data - information about vehicles and property associated with crime accompanied by any personally identifiable information (PII).
5. Case/Incident History – information about the history of criminal incidents.

Criminal History Record Information (CHRI)

Criminal History Record (CHRI), sometimes informally referred to as "restricted data", is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI.

Personal Information (PII)

PII is information that can be used to distinguish or trace an individual's identity such as a name, social security number, or biometric records, alone or when combined with other personal or identifying information that is linked or likable to a specific Individual, such as a date and place of birth, or mother’s maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment may include PII. A criminal history record example inherently contains PII, as would a Law Enforcement National Data Exchange (N-DEx) case file.

All information classified, as confidential, personal, and/or protected information must be properly stored, transmitted, transported, and disposed of in a manner to protect it from unauthorized access or disclosure, alteration or misuse. Regardless of its form or method of dissemination (i.e., hard copy, fax, etc.), CJI requires protection throughout its life.

In accordance with FBI/CJIS Security Policy Area 8: Media Protection, the California Eastern Probation (CAEP) standards are outlined as follows:

Media Storage and Access

Storage of printed electronic media or containers with CJI and/or PII may only be stored at approved locations, with a locking mechanism in place, staffed by persons who have been fingerprint background checked. When printed material is not in use and the CAEP employee is out of the room, material is to be kept locked in a cabinet. All operators having direct access into CLETS system CJI, must log off and lock CLETS terminals when they away from the area. Storage of CJI and/or PII on desktop computers, computing devices (iPads, etc.), or personal telecommunications devices and hard disks is prohibited by CAEP ISO/SPOC.

Transportation

Printed material, electronic media, or containers with CJI and/or PLI may only be handled or transported by approved person who have been fingerprint background checked

When it is necessary for an office to move to another location, plans must be made to protect and account for all protected CJI and/or PII information. All CJI and/or PII must be securely moved. The media must be handled in such a manner that it does not become misplaced or available to unauthorized personnel.

The term “media" in its usage here is inclusive of paper and electronic formats, such as all removable tapes, disk drives,

flash drives and entire computers if its hard drives are not removed.

While in relocation status, the following procedures apply:

The media must remain in the custody of the CAEP employee and accountability must be maintained throughout the move to media does not become misplaced or lost during the move.

The media must be in locked cabinets or sealed packaging cartons while in transition.

In the event the media must be hand-carried by a CAEP employee in connection with a trip or in the course of daily activities, it must be kept with that employee and protected from unauthorized disclosures (i.e., locked briefcase).

Backup media, such as removable tapes and optical discs, and portable electronic devices must be encrypted prior to movement.

CJI and/or PII should not be transmitted on the email systems. If, however, CJI and/or PII must be transmitted, either in the body of an email or as an attachment the email must be encrypted. CAEP staff must work with CAEP IT to ensure an encryption solution is in place to send and receive CJI and/or PII information via the email.

If an email is received or sent by any CAEP staff that is not encrypted and contains CJI and/or PII, they must report it to the ISO/SPOC and CAEP Agency CLETS Coordinator.

Multi-function printers (MFPs) must be securely configured and anti-virus software installed on CAEP CLETS equipment (transport precaution).

Digital Media Sanitization and Disposal

Electronic Media

Electronic media records on decommissioned servers or other storage devices are to be securely erased using DOD approved methods or the physical media destroyed.. Electronic media may be re-used; however, the media should securely erased and sanitized where practical.

Media / Disposal Methods

CD/DVD media should be broken/ destroyed prior to disposal.

Hard Drives should be erased using DOD approved methods. Use vendor provided utility for built-in “secure erase” function. Break/destroy the hard drive (drill several hole through platters, shred, smash to point where platters and PCBs are broken)

Tapes should be erased DOD approved methods (degauss) and destroy (shred)

Flash Drives should be broken/destroyed prior to disposal.

Electronic media may be placed in locked confidential shredder bins and subsequently destroyed by a contracted vendor on-site (CAEP escorted/witnessed).

Printed material may be in confidential shredder bins and subsequently destroyed by a contracted vendor on-site

(CAEP escorted/witnessed). CAEP offices that have their own crosscut shredders (aka confetti shredders) may be used. "Snip cut" shredders are to be used for CD and/or PII confidential data.

Notification of Mishandling of Confidential CJI and/or PII

Any mishandling of confidential CJI and/or PII while stored, transmitted, or disposed of that result in suspected or actual unauthorized access, disclosure, and/or modification must be reported to the ISO/SPOC and Agency CLETS Coordinator.

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.

812.8 CALIFORNIA RELIGIOUS FREEDOM ACT

Members shall not release personal information from any agency database for the purpose of investigation or enforcement of any program compiling data on individuals based on religious belief, practice, affiliation, national origin or ethnicity (Government Code § 8310.3).