Protected Information

804.1 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 Irvine 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.

804.1.1 DEFINITIONS

Definitions related to this policy include:

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

804.2 POLICY

Members of the Irvine 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.

804.3 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.

804.4 ACCESS TO PROTECTED INFORMATION

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

Upon separation from Irvine Police Department, the employee's access to systems containing criminal justice information (CJI) will be immediately terminated. If personnel are reassigned or transferred to alternate positions within the Irvine Police Department and no longer require access to CJI, the employee's access to systems containing CJI will be revoked.

804.4.1 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).

804.5 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 Records Supervisor 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).

804.5.1 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).

804.5.2 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.

804.6 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.

804.6.1 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).

804.7 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.

804.7.1 COMPUTER TERMINAL SECURITY
Computer terminal equipment capable of providing access to automated criminal offender record information is located within Public Safety to preclude access by unauthorized persons. Information system devices shall be positioned in such a way as to prevent unauthorized individuals from accessing and viewing CORI.Screen protectors shall be used if the monitor is in view of unauthorized individuals.

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

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

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

804.8 TRAINING PROGRAM
All personnel authorized to process or release CORI shall be required to complete a training program prescribed by the Agency CLETS Coordinator. The Training Bureau shall coordinate the course to provide training in the proper use, control, and dissemination of CORI.

804.9 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.

Each suspected incident of unauthorized or improper use of CORI, or failure to take physical security measures to protect CORI, will be investigated by the Office of Professional Standards. Violations will result in action which may include disciplinary action, criminal penalties and/or financial liability for the cost of improper use.

804.10 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).