Confidential Information - Access / Destruction

802.1 PURPOSE AND SCOPE

(a) The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the Oakley Police Department. This policy addresses the protected information that is used in the day-to-day operation of the Oakley Police Department and not the public records information covered in the Records Maintenance and Release Policy (OPDPM Section 805).

802.2 POLICY

(a) Members of the Oakley 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 REFERENCE(S)

(a) Criminal Justice Information Services (CJIS) Security Policy, US Department of Justice (US-DOJ), V 5.5, June 2016

(b) CLETS Policies, Practices and Procedures, California Department of Justice (CADOJ), September 2014

802.4 RELATED MANUAL SECTION(S)

(a) OPD Policy Manual Section 208, Station Security and Visitors

802.5 DEFINITIONS

(a) **Protected Information** - Any information or data that is collected, stored or accessed by members of the Oakley 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. For example, data obtained from the DMV Database is protected information and must be safeguarded from inadvertent release.

(b) **Criminal Offender Record Information (CORI)** - CORI shall include CII manual/ automatic manual/automated RAP Sheets and abstracts, CII Criminal Summaries, CII Criminal History Transcripts, FBI RAP Sheets, and any OPD Documents containing a list of prior arrests. Examples of documents would be RAP Sheet printouts, police reports, ARIES printouts, etc.

(c) **Criminal Justice Information (CJI)** - Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their

mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

(d) **Authorized Recipients** - Any person or agency authorized by court order, statute, or case law to receive CORI.

(e) **Right to Know** - Persons or agencies authorized by court order, statute, or decisional state law to receive the information.

(f) **Need to Know** - A necessity exists to obtain CORI in order to execute official responsibilities.

802.6 RESPONSIBILITIES

(a) The Chief of Police shall select a member of the Oakley Police Department to coordinate the use of protected information. This person shall be the Agency CLETS Coordinator.

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

1. 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).
2. 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.
3. 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.
4. Developing procedures to ensure training and certification requirements are met.
5. Resolving specific questions that arise regarding authorized recipients of protected information.
6. Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

802.7 ACCESS TO PROTECTED INFORMATION

(a) Protected information shall not be accessed in violation of any law, order, regulation, user agreement, department policy, directive, 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.

(b) Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited. Violators may be subjected to administrative and disciplinary actions and/or criminal prosecution.

802.7.1 MISUSE OF CRIMINAL JUSTICE INFORMATION (CJI)

(a) Any access and/or dissemination of CJI for unauthorized purposes are considered misuses of the system and the data it contains.

(b) Misuse of CJI may include but is not limited to:

1. Unauthorized requests, receipt, release, interception, dissemination, or discussion of CJI.
2. Improper use of information obtained from any CJI System and/or related applications and devices.
3. Violating the confidentiality of any data or record information and using it for personal purposes.

802.7.2 ACTIONS WHEN MISUSE IS SUSPECTED

(a) When an individual is suspected of misuse of CJI date, the investigation will be handled on a case-by-case basis. However, the following will occur in all circumstances:

1. The account of the individual user will immediately be suspended to prevent ongoing misuse while under investigation.
2. The Chief of Police will immediately be notified of the suspected misuse.
3. An internal investigation will be conducted.

802.7.3 PENALTIES FOR MISUSE OF RECORDS

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

(b) 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).

(c) If the investigation determines the release was inadvertent, the offender will complete additional training on CJI Security Awareness.

(d) If the investigation reveals there was misuse of the system, a CLETS Misuse Investigation Report will completed and forwarded to the California Department of Justice (Form in CLETS Policy Manual),

802.8 ACCESSING RECORD OF ARRESTS AND PROSECUTIONS REPORTS (RAP SHEETS)

(a) As a part of their normal duties, law enforcement officers may need to access and print offender RAP Sheets. Like accessing all CORI data, this must only be done on a need to know/right to know basis.

(b) When a RAP Sheet is accessed, the person making the inquiry is responsible for:

1. Entering the requesting officer's badge number, the reason, and the case file number for the inquiry into the requesting data mask.
2. Recording the necessary information in the "RAP Sheet" Binder in the Records Unit.
3. Stamping the front page of the RAP Sheet with the appropriate declaration stamp. The name of the individual responsible for the record will be written into the correct location on the stamp.
4. If the record is transferred to another agency (i.e., DA's Office) the transfer of responsibility will be listed on the face page of the record.
5. When no longer required, the record will be destroyed in accordance with this policy.

802.9 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

(a) Protected information may be released only to authorized recipients who have both a right to know and a need to know.

(b) 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.

(c) Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Oakley Police 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, OPDPM Section 805).

(d) Protected information, such as Criminal Justice Information (CJI), which includes Criminal Offender Record Information (CORI), 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.

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

(f) Law Enforcement Bulletins, TRAK or Critical Reach Fliers, or similar documents are for law enforcement personnel only.

(g) Cal-Photo information shall not be releases to the public.

(h) Criminal Justice Agency Documents not authored by a member of the City of Oakley Police Department will not be released to the public or the media. Release of these documents is the responsibility of the authoring agency (the custodian of the original record).

802.9.1 REVIEW OF CRIMINAL OFFENDER RECORD

(a) Individuals requesting to review their own California Criminal History Information shall be referred to the Department of Justice (Penal Code § 11121).

(b) Individuals shall be allowed to review their arrest or conviction record on file with the Oakley Police Department after complying with all legal requirements regarding authority and procedures in Penal Code § 11120 through Penal Code § 11127 (Penal Code § 13321). This process will only be performed by the Records Manager or their authorized designee.

802.10 SECURITY OF PROTECTED INFORMATION

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

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

1. Developing and maintaining security practices, procedures and training.
2. Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.
3. Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents including computer attacks.
4. Tracking, documenting and reporting all breach of security incidents to the Department of Justice and appropriate authorities.

802.10.1 MEMBER RESPONSIBILITIES

(a) 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).

802.11 TRAINING

(a) 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.

(b) All users will complete the appropriate Security Awareness Training as identified in OPDPM Section 208.21.

802.12 CALIFORNIA RELIGIOUS FREEDOM ACT

(a) 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).

802.13 DESTRUCTION OF CONFIDENTIAL INFORMATION

(a) **ALL** CORI and Confidential Information should be placed in the locked destruction bins as soon as the items are no longer needed. This includes data maintained on Compact Disks (CDs). The Oakley Police Department contracts with Shred-It to destroy/shred all physical media placed in the bins. The locked storage bins are located in Records, Investigations, the Report Room and the Admin Conference Room. No CORI or confidential information is to be thrown in wastebaskets or recycle bins.

(b) Once a month, Shred-It will be on site to destroy the items in our bins. Records personnel (or replacement) will oversee the collection of the bins with Shred-It. Once all the bins are collected personnel will accompany Shred-it to their truck and witness the onsite destruction/shredding of our media. A certificate of destruction will be provided at the time of destruction by Shred-It for our agency for record keeping purposes. All receipts of destruction will be forwarded to the Records Manager. The Records Manager is responsible for maintaining and updating the destruction log.

802.13.1 DESTRUCTION OF SECURE ELECTRONIC MEDIA

(a) This procedure outlines the proper handling and destruction of all electronic media that has been connected to the Police Department network. This procedure applies to all devices, regardless of what type of data has been stored on, or accessed by, the system the device was removed from.,

(b) Hard Drives and Tape Media

1. Hard drives and tape media will be stored in a secure area within the Police Department until they are scheduled to be destroyed. All retired or nonfunctional hard and tape media will be destroyed prior to their disposal.

2. When destruction is to be performed, an authorized member of the City of Oakley IT staff will transport the media to the City's degauss unit. Each item will be logged into the Media Destruction Log and destroyed. The media will not be left unattended until which time all media has been destroyed.

(c) Optical Media

1. Optical media will be stored in a secure area within the Police Department until they are scheduled to be destroyed.

2. All optical media will be physically destroyed (shredded) following the policy in place for the destruction of paper documents.

(d) Other Media (Static RAM devices, flash drives, etc.).

1. All miscellaneous media will be stored in a secure area within the Police Department until they are scheduled to be destroyed.

2. Once formatted, the media will be physically destroyed (shredded) following the policy in place for the destruction of paper documents.

802.14 REVIEW DATE

(a) 29 APR 16

(b) 5 JAN 20 (Lexipol)