Protected Information

808.1 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 Kitsap County Sheriff's Office. This policy addresses the protected information that is used in the day-to-day operation of the Office and not the public records information covered in the Records Maintenance and Release Policy.

808.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the Kitsap County Sheriff's Office 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.

808.2 POLICY

Members of the Kitsap County Sheriff's Office will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

808.3 MEMBER AND VISITOR ACCESS

808.3.1 KCSO MEMBER IDENTIFICATION

Members shall wear their commission or identification (ID) card at all times while in office facilities, unless in uniform and/or displaying a KCSO badge. The identification shall be worn in a manner that is clearly visible. The information on the card must be current and contain a photo of the authorized cardholder. Commission and identification cards are issued by the KCSO Office of Professional Standards.

808.3.2 AUTHORIZED CONTRACTORS, COUNTY EMPLOYEES AND EXTERNAL LAW ENFORCEMENT EMPLOYEES

Authorized Kitsap County employees, contractors and vendors who have completed the necessary CJIS security training and background checks and who have unescorted access to KCSO, shall be in uniform and/or display appropriate identification when in KCSO facilities. Members of other law enforcement agencies wearing their uniform, identification or badge shall have unescorted access to KCSO facilities. The visitors in this category need not sign in or out on the visitor log if they are displaying the appropriate uniform and/or identification.

Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to have a state and national fingerprint-based record background check prior to the restricted areas access being granted. The individuals will additionally be required to complete the CJIS security awareness training facilitated by the agency TAC.

Noncriminal Justice Agency (NCJA) such as Kitsap County IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement and/or an Inter-Agency Agreement between KCSO and the NCJA. Each NCJA employee with CJI access will appropriately have a state and national fingerprint-based record background check prior to the restricted areas access being granted. The individuals will additionally be required to complete the CJIS security awareness training facilitated by the agency TAC.

808.3.3 AUTHORIZED VISITORS

An authorized visitor is defined as a person who is invited to a KCSO facility on a temporary basis and has either escorted or unescorted access to the physically secure locations within the KCSO where protected information and/or systems reside.

A visitor's log shall be maintained by the reception desk personnel at each office. Badges are colored coded and issued according to the nature of the visit and legitimate business needs.

Green badges: The green colored badges are only issued to Law Enforcement Officers from other agencies or KCSO personnel who do not have their commission/identification card or badge with them. Visitors with green badges shall be granted unescorted access.

Yellow badges: The yellow badges are issued only to those civilians given unescorted access to our offices and who do not have their official identification. Individuals issued yellow badges will have been fingerprinted and will have completed the CJIS security awareness training. Some examples of personnel who are allowed a yellow badge.

(a) Deputy Prosecutors and Prosecutor of the Kitsap County Prosecutor's Office

(b) Deputy Coroners and Coroner of the Kitsap County Coroner's Office

(c) Contractors or other office designated individuals (IS and Maintenance Staff).

Red badges: Red badges are issued to all other visitors to KCSO facilities. These individuals must be escorted by an authorized KCSO member.

Escorted visitors shall be accompanied by an authorized KCSO escort to ensure the protection and integrity of the physically secure location and any protected information contained therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort. Visitors are prohibited from utilizing still shot and video cameras which may capture CJI.

808.4 AUTHORIZED PHYSICAL ACCESS

Only authorized members will have access to physically secure non-public locations. KCSO will maintain and keep current, a list of authorized personnel. The office will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the office from physical, logical and electronic breaches.

All members with CJI physical and logical access must:

(a) Meet the minimum personnel screening requirements prior to CJI access.

(b) Complete security awareness training (non ACCESS Terminal Users).

(c) Complete ACCESS certification (ACCESS terminal Users).

(d) Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.

(e) Use of electronic media is allowed only by authorized KCSO members. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

(f) Report any physical security incidents to KCSO's LASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.

808.5 RESPONSIBILITIES

The Sheriff shall select a member of the Office 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 Licensing (DOL) records and the Washington Crime Information Center (WACIC).

(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.

808.5.1 TERMINAL AGENCY COORDINATOR (TAC)

The TAC serves as the point-of-contact at the Kitsap County Sheriff's Office for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the Office's compliance with FBI and state CJIS systems policies.

(a) Is the primary contact for all ACCESS related questions.

(b) Be available to assist with ACCESS and technical audits.

(c) Must be ACCESS level 2 certified.

(d) Shall conduct 5-year re-background checks on all personnel who use or work on the connection to ACCESS.

(e) Must keep their agency current with ACCESS updates to manuals and procedures.

(f) Will disseminate ACCESS related announcements and memorandums.

(g) Will report any misuse of ACCESS systems.

(h) Will facilitate certifying new users and removing individuals when appropriate.

(i) Will ensure compliance is maintained relating to CHRI.

(j) Responsible for agency monthly NCIC validations.

(k) Shall maintain a current terminal assignment list.

808.6 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Kitsap County Sheriff's Office 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. See the CJIS Access, Maintenance, and Security Policy for additional guidance.

808.6.1 PENALTIES FOR MISUSE OF RECORDS

It is a misdemeanor to furnish, buy, receive or possess criminal history record information without authorization by Washington law (RCW 10.97.120).

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

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

808.6.2 RELEASE OF CHRI

Only the persons listed below are authorized to release CHRI. Each authorized person releasing CHRI 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) Support Services Supervisor.

(c) Full-time employees of the Records Division.

(d) Personnel specifically designated in writing by Division Chiefs with the concurrence of the Criminal Records Security Officer.

808.6.3 RELEASE OF CHRI TO FIELD PERSONNEL
Personnel shall not have access to CHRI until a background investigation has been completed and approved.

808.6.4 RECORDS SUITABLE FOR RELEASE
Conviction records and CHRI may be disseminated as set forth in RCW 10.97.050.

808.7 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 (RCW 10.97.050).

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 Support Services Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Office 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 Division 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 deputies, other office members or the public is at risk.

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

808.7.1 RELIGIOUS AFFILIATION DISCLOSURE
Members shall not release personal information from any agency database for the purpose of investigation or enforcement of any government program compiling data on individuals based on religious belief, practice, affiliation, national origin, or ethnicity (RCW 42.60.020).

808.7.2 REVIEW OF CRIMINAL OFFENDER RECORD
An individual may review his/her criminal history record information held by this office after complying with established office requirements as authorized by RCW 10.97.080.

808.8 SECURITY OF PROTECTED INFORMATION

The Sheriff will select a member of the 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.

(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 Sheriff and appropriate authorities (RCW 19.255.010; RCW 42.56.590).

808.8.1 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).

808.9 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.

808.9.1 DESTRUCTION OF CHRI

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