MEDIA SANITIZATION/DESTRUCTION AND PROTECTION

AUTHORITY: Administrative Directive

RESCINDS: Procedure Manual Item 1-5-306, dated 10/20/19

FORMS: None

PURPOSE: To outline proper disposal/sanitization/destruction of media and ensure the protection of Criminal Justice Information (CJI).

I. GENERAL INFORMATION

A. Sanitation/Destruction

1. This policy applies to all Orange County Probation Department (OCPD) employees, contractors, temporary staff, and other workers at OCPD with access to California Law Enforcement Telecommunications System (CLETS)/National Crime Information Center (NCIC), Criminal Justice Information (CJI) systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits CLETS/NCIC CJI and classified/sensitive data that is owned or leased by OCPD.

2. These rules are in place to protect sensitive and classified information, as well as employees and OCPD. Inappropriate disposal of OCPD and CJI data and/or media may put employees, OCPD, and CLETS/NCIC at risk of both civil and criminal liability.

B. Protection

1. This policy applies to any electronic or physical media containing Federal Bureau of Investigations (FBI) CJI, while being stored, accessed, or physically moved from a secure location. This policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media. Transporting CJI outside the Agency's assigned physically secure area must be monitored and controlled.

   Authorized OCPD personnel shall protect and control electronic and physical CJI while at rest and in transit. OCPD will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to OCPD's **Agency Coordinator.** Procedures shall be defined for securely handling, transporting, and storing media.

2. The intent of the this policy is to ensure the protection of CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime

reports data), or is purged/destroyed in accordance with applicable record retention rules.

This policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy 5.1. OCPD may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

3. Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

II. PROCEDURE

A. Sanitation/Destruction

1. When no longer usable, hard drives, diskettes, tape cartridges, compact discs (CDs), ribbons, hard copies, printouts, and other similar items used to process, store, and/or transmit CJI and classified/sensitive data shall be properly disposed of in accordance with measures established by OCPD.

2. Physical media (printouts and other physical media) shall be disposed of by one of the following methods:

a. Shredded using OCPD issued crosscut shredders.

b. Placed in locked shredding bins for Paper Depot to come on-site and crosscut shred, witnessed by OCPD personnel throughout the entire process.

c. Incinerated using OCPD incinerators or witnessed by OCPD personnel on-site at agency or at contractor incineration site, if conducted by non-authorized personnel.

3. Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the following methods:

a. Over writing **–** at least **three (**3**)** times

An effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

b. Degaussing

A method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a metal surface) are fairly weak and cannot effectively degauss magnetic media.

c. Destruction

A method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring the platters have been physically destroyed so no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from OCPD's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

B. Protection

1. Media Storage and Access

To protect CJI, OCPD personnel shall:

a. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.

b. Restrict access to electronic and physical media to authorized individuals.

c. Ensure only authorized users remove printed form or digital media from the CJI.

d. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques, and procedures.

e. Not utilize any device other than those issued by OCPD to access, process, store, or transmit CJI (see Policy G-12, *Personally Owned Electronic Devices*).

f. Store all hardcopy CJI printouts maintained by OCPD in a secure area accessible to only those employees whose job function require them to handle such documents.

g. Safeguard all CJI by OCPD against possible misuse (see PMI 1-4-207, *Physical Protection of CJI*, and PMI 1-4-208, *CLETS*).

h. Take appropriate action when in possession of CJI while not in a secure area:

(1) CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

(2) Precautions must be taken to obscure CJI from public view, such as use of an opaque file folder or envelope for hardcopy printouts. For electronic devices like laptops, use session lock and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

(a) When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers, and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

(b) When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

i. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a "need-to-know" basis.

j. Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI. (see PMI 1-4-207, *Physical Protection of CJI*)

2. Media Transport

a. Dissemination to another agency is authorized if:

(1) The other agency is an authorized recipient of such information and is being serviced by the accessing agency, or

(2) The other agency is performing personnel and appointment functions for criminal justice employment applicants.

b. OCPD personnel shall:

(1) Protect and control electronic and physical media during transport outside of controlled areas.

(2) Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

c. OCPD personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

(1) Use of privacy statements in electronic and paper documents.

(2) Limiting the collection, disclosure, sharing, and use of CJI.

(3) Following the least privilege and role-based rules for allowing access. Limit CJI access to only those people or roles that require access.

(4) Securing hand carried confidential electronic and paper documents by:

(a) Storing CJI in a locked briefcase or lockbox.

(b) Only viewing/accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.

(c) For hard copy printouts or CJI documents:

- Package hard copy printouts in such a way as to not have any CJI information viewable.

- If mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED AS "CONFIDENTIAL". Packages containing CJI material are to be sent by method(s) that provide complete shipment tracking and history, and signature confirmation of delivery. (agency discretion)

(5) Not taking CJI home or when traveling unless authorized by OCPD administrator(s). **A crosscut shredder must be used when** disposing confidential documents, **the shredder must be locked.**

3. Breach Notification and Incident Reporting

The **Department** shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

4. Roles and Responsibilities

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

a. OCPD personnel shall notify his/her supervisor and **the AFD Safety and Facilities Manager**, and an incident-report form must be completed and submitted within twenty-four (24) hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.

b. PSD will ensure the CLETS Security Point of Contact (SPOC) is promptly informed of security incidents.

c. The CLETS SPOC will:

(1) Establish a security incident response and reporting procedure to discover, investigate, document, and report to Orange County Sheriff Department, the affected criminal justice agency, and the FBI CJIS Division Information Security Office (ISO) major incidents that significantly endanger the security or integrity of CJI.

(2) Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement Point of Contact's (POCs) within their area.

(3) Act as a single POC for their jurisdictional area for requesting incident response assistance.

5. Penalties

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution, and/or termination from employment.

REFERENCES:

Procedures:	1-4-207	Physical Protection of Criminal Justice Information
	1-4-208	California Law Enforcement Telecommunications Systems (CLETS)

CLETS Policies, Practices and Procedures (and Statutes)
FBI CJIS Security Policy

V. Sanchez

APPROVED BY: Dana Schultz Digitally signed by Dana Schultz Date: 2022.02.09 09:14:12 -08'00'