

## Physical Protection of Criminal Justice Information

- AUTHORITY:** Administrative Directive
- RESCINDS:** Procedural Manual Item 1-4-207, dated 10/20/19
- FORMS:** [CLETS Employee/Volunteer Statement](#)  
[CLETS Management Control Agreement](#)  
[CLETS Private Contractor Management Control Agreement](#)  
[FBI CJIS Security Addendum](#)
- PURPOSE:** Guidance for **Probation department** personnel, support (**collaborative personnel, Department of Education, HCA, etc.**) personnel, and private contractors/vendors protection of Criminal Justice Information (CJI).

### I. GENERAL INFORMATION

- A. All physical, logical, and electronic access must be properly documented, authorized, and controlled on devices that store, process, or transmit unencrypted Criminal Justice Information (CJI). This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

B. CLETS Physically Secure Location

A physically secure location is a facility or an area, room, or group of rooms within a facility with both the physical and personnel security controls sufficient to protect the CLETS-based CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the Orange County Probation Department (OCPD) shall be identified with a sign at the entrance.

C. Visitors

A visitor is defined as a person who visits any OCPD facility on a temporary basis, is not employed by the Department, and has no unescorted access to the physically secure location within OCPD where CLETS-based CJI and associated information systems are located.

### II. PROCEDURE

A. Visitor Access – Visitors shall:

1. Check in before entering a physically secure location.

2. Provide a form of identification used to authenticate the visitor. If OCPD issues visitor badges, the visitor badge shall be worn on approved visitor's outer clothing and collected by the **Department** at the end of the visit.
3. Be accompanied by an OCPD escort at all times; this includes delivery or service personnel. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
4. Follow the OCPD policy for authorized unescorted access (see PMI 1-4-202, *Security - Probation Offices*, and PMI 1-4-203, *Security Clearance Volunteers, Vendors, Contractors, and Orange County Public Works Personnel*).
  - a. Noncriminal Justice Agency (NCJA), such as city or county IT who require frequent unescorted access to restricted area(s), will be required to establish a Management Control Agreement (MCA) between the OCPD and NCJA. Each NCJA employee with CJL access will be required to complete a background investigation prior to this restricted area access being granted.
  - b. Private contractors/vendors, who require frequent unescorted access to restricted area(s), will be required to establish a Private Contractor Management Control Agreement (PCMCA) between the OCPD and each private contractor personnel. Each private contractor personnel will be required to sign a CJIS Security Addendum and complete a background investigation prior to this restricted area access being granted.
5. Not be allowed to view screen information, including shoulder surfing.
6. Not enter a secure area with electronic devices, unless approved by the Department; **this** includes cameras and mobile devices. Photographs are not allowed without permission of OCPD personnel.
7. **Not enter a restricted area if they do** not having any legitimate business in **said** area. **Should this occur, visitors** shall be courteously escorted to a public area of the facility and the building manager notified.
8. All requests by groups for tours of any OCPD facility will be referred to the proper **Department** point of contact for scheduling. Visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

B. Authorized Physical Access

1. To gain authorization, an individual must meet the minimum personnel screening requirements, which includes a background investigation. Only authorized personnel will have access to physically secured non-public locations. The Department will **maintain** a list of authorized personnel. All physical access points into the **Department's** secure areas will be authorized before granting access. The **Department** 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 **Department** from physical, logical, and electronic breaches.

2. All personnel with CJI physical and logical access must:
  - a. Complete Security Awareness training.
    - (1) All authorized OCPD employees and NCJA employees, such as County IT and private contractor/vendor personnel, will receive Security Awareness training within six (6) months of being granted duties that require CJI access and every two (2) years thereafter.
    - (2) Security Awareness training will cover areas specified in the CJIS Security Policy at a minimum.
  - b. Abide by Policy G-15, *County's Information Technology Usage Policy*.
  - c. Be aware of who is in their secure area before accessing confidential data.
    - (1) Take appropriate action to protect all confidential data.
    - (2) Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.
  - d. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
    - (1) Report loss of issued keys, proximity cards, etc. to authorized agency personnel.
    - (2) Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens, and all other facility and computer systems security access procedures.
  - e. Not use personally owned devices on OCPD's computers with CJI access.
  - f. Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.
    - (1) **The Probation Department must use discretion when allowing CJI to be transmitted through email.**
    - (2) If CJI is transmitted outside of the **Department** by email, the email must be encrypted (FIPS 140-2) end-to-end and email recipient must be authorized to receive and view CJI.



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

V. Sanchez

**APPROVED BY:**