Policy Title: **Physical Protection of Criminal Justice Information Data**	Effective Date: May 1, 2018		Policy Number: **4.33**
Accreditation Reference:	Review Date: June 25, 2027	Supersedes: October 15, 2014	Pages: 3
Attachments:	L. Shane Nelson, Sheriff		

I. PURPOSE

The purpose of this policy is to provide guidance for agency members, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

II. DEFINITIONS

CJI means Criminal Justice Information.

CJIS refers to Criminal Justice Information Systems.

IT is Information Technology.

FBI is the Federal Bureau of Investigations.

III. POLICY

A. Physically Secure Location

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI 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 Sheriff's Office shall be identified with a sign at the entrance.

B. Visitor Access

A visitor is defined as a person who visits the Sheriff's Office facility on a temporary basis who is not employed by the Sheriff's Office and has no unescorted access to the physically secure location within the Sheriff's Office where FBI CJI and associated information systems are located.

Visitors shall:

1. Check in before entering a physically secure location by:
    a. completing the visitor access log,

b. Issue a visitor badge which shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.

2. Be accompanied by a Sheriff's Office escort at all times, including delivery or service personnel. An escort shall accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. Strangers in physically secure areas without an escort should be challenged.

3. Follow Sheriff's Office policy for authorized unescorted access.

   a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the Sheriff's Office and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check 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 Security Addendum between the Sheriff's Office and private contractor personnel. Private contractor personnel will have state and national fingerprint-based record background checks prior to this restricted area access being granted.

4. Not be allowed to view screen information.

C. Authorized Physical Access

Only authorized personnel will have access to physically secure non-public locations. The Sheriff's Office will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized members will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All members with CJI physical and logical access must:

1. meet the minimum personnel screening requirements prior to CJI access.

2. complete security awareness training.

All authorized Sheriff's Office, Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.

3. Be aware of who is in their secure area before accessing confidential data.

   a. Take appropriate action to protect all confidential data.

   b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.

4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc. Report loss of issued keys, proximity cards, etc., to authorized agency personnel.

5. Do not use personally owned devices on the Sheriff's Office computers with CJI access. See Policy 4.31 Computer, E-Mail and Mobile Computing Device Use.

6. Use of electronic media is allowed only by authorized Sheriff's Office 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.

7. If CJI is transmitted by email to recipients inside or outside the agency, the email must be encrypted. The email recipient must be authorized to receive and view CJI.

8. Report any physical security incidents to the Sheriff's Office's Forensic Lieutenant, including facility access violations, loss of agency-issued mobile computing devices, thumb drives, CDs/DVDs and printouts containing CJI.

D. Enforcement

Members violating any aspect of this policy may have their access to computer resources restricted and are subject to discipline, up to, and including, termination of employment.