<INSERT AGENCY NAME>

Physical Protection

|  |
| --- |
| *The purpose of this template is to assist your agency in creating its own procedures. These are the minimum topics that must be covered:*1. *The items below in red must be specific and reflect your agency’s current practices.*
2. *Remove any items that are not applicable to your agency.*
3. *Formalize with the date and your agency name.*
4. *Remove the red box once the procedure is updated and completed.*

*If your procedure does not reflect the actual practice at your agency, then you will be found out of compliance.**ACCESS Section revised August 2023* |

**Purpose:**

The purpose of this policy is to provide guidance for agency personnel, 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 Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

**Physically Secure Location:**

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control. 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.

**Visitors Access:**

Visitor specifications need to be established per agency purview and approval. A visitor is defined as a person who visits the agency on a temporary basis who is not employed by the <Insert Agency Name> and has no unescorted access to the physically secure location within the agency where CJI and associated information systems are located.

Visitors must:

If your agency chooses to have a visitor log please include it in your agency policy.

1. Be accompanied by an agency personnel escort at all times to include delivery or service personnel. An escort is defined as authorized personnel who 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. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort
2. Show a valid form of photo identification
3. Follow policy for unescorted access
	1. Noncriminal Justice Agency (NCJA) like city or county IT who require unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the <Insert Agency Name> and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background checks prior to this restricted area access being granted
	2. Private contractors/vendors who have unescorted access to restricted area(s) will be required to establish a Security Addendum with each private contractor personnel. Each private contractor personnel will appropriately 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 mitigating shoulder surfing
5. Be escorted to a public area of the facility when they do not have any legitimate business in a restricted area. Strangers in physically secure areas without an escort should be challenged
6. Not be allowed to sponsor another visitor
7. Not enter into a secure area with electronic devices unless approved by the Information Technology point of contact to include cameras and mobile devices. Photographs are not allowed without permission of the <Insert Agency Name> assigned personnel
8. Be referred to the proper agency point of contact for scheduling requests for tours. 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

**Authorized Physical Access:**

Only authorized personnel will have access to physically secure non-public locations. 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 personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel that are not escorted with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access
	1. Agencies must conduct a state of residency and national fingerprint-based background checks for all agency personnel and IT personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI prior to employment or assignment
	2. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times
2. Complete Security Awareness Training
	1. All authorized <Insert Agency Name> and NCJA personnel, like city or county IT and private contractor/vendor, will receive Security Awareness Training within six months of being granted duties that require CJI access and annually thereafter
3. 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 the 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.
	1. Report loss of issued keys, proximity cards, etc. to authorized agency personnel
	2. If the loss occurs after normal business hours, weekends or holidays, personnel are to call the <Insert Agency Name> POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed
	3. Safeguard and do not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures
5. Properly protect from viruses, worms, trojan horses, and other malicious code.
6. Web usage - allowed versus prohibited; monitoring of user activity. (allowed versus prohibited is at the agency’s discretion)
7. Use of electronic media is allowed only by authorized personnel. 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
8. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI
9. Report any physical security incidents to the <Insert Agency Name>’s IT POC to include facility access violations, loss of CJI, loss of laptops, thumb drives, CDs/DVDs and printouts containing CJI
10. Properly release hard copy printouts of CJI only to authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a “need to know” basis
11. Ensure data centers with CJI are physically and logically secure
12. Keep appropriate agency security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies
13. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries

**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. Violation by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.