Physical Protection Policy Sample

(Required Written Policy)

1.0 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.

2.0 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 LEIN-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 *[agency name]* shall be identified with a sign at the entrance.

3.0 Visitors Access:

A visitor is defined as a person who visits the *[agency name]* facility on a temporary basis who is not employed by the *[agency name]* and has no unescorted access to the physically secure location within the *[agency name]* where LEIN-based CJI and associated information systems are located. For agencies with jails with CJIS terminals, additional visit specifications need to be established per agency purview and approval.

Visitors shall:

1. Check in before entering a physically secure location by:
    a. Provide a form of identification used to authenticate visitor.
    b. If *[agency name]* issues visitor badges, the visitor badge 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 *[agency name]* 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.
3. Show *[agency name]* personnel a valid form of photo identification.
4. Follow *[agency name]* 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 *[agency name]* 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 requires frequent unescorted access to restricted area(s) will be required to establish a CJIS Security Addendum between the *[agency name]* and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.
5. Not be allowed to view screen information mitigating shoulder surfing.
6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.
7. Not be allowed to sponsor another visitor.

8. Not enter into a secure area with electronic devices unless approved by the *[agency name]* Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the *[agency name]* assigned personnel.
9. All requests by groups for tours of the *[agency name]* facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining 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.

4.0 Authorized Physical Access:
Only authorized personnel will have access to physically secure non-public locations. The *[agency name]* 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 personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.
    a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all 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.
    b. 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.
    c. Prior to granting access to CJI, the *[agency name]* on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.
    d. Refer to the CJIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.
2. Complete security awareness training.
    a. All authorized *[agency name]*, 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.
    b. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum.
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.
    a. Report loss of issued keys, proximity cards, etc to authorized agency personnel.
    b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the *[agency name]* POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.
    c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. (*See Disciplinary Policy).*
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. Do not use personally owned devices on the *[agency name]* computers with CJI access. *(Agency discretion)*. (*See Personally Owned Device Policy)*.

8. Use of electronic media is allowed only by authorized *[agency name]* 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.
9. Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.
    a. Agency Discretion for allowance of CJI via email.
    b. If CJI is transmitted by email, the email must be encrypted (FIPS 140-2) end-to-end and email recipient must be authorized to receive and view CJI.
10. Report any physical security incidents to the *[agency name]*'s LASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.
11. Properly release hard copy printouts of CJI only to authorized vetted and 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. (*See Media Sanitization and Destruction Policy)*
12. Ensure data centers with CJI are physically and logically secure.
13. Keep appropriate *[agency name]* 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.
14. Not use food or drink around information technology equipment.
15. Know which door to use for proper entry and exit of the *[agency name]* and only use marked alarmed fire exits in emergency situations.
16. 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.

5. 0 Roles and Responsibilities:

5.1 Terminal Agency Coordinator (TAC)
The TAC serves as the point-of-contact at the *[agency name]* for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and MI CJIS systems policies/addenda.

5.2 Local Agency Security Officer (LASO)
Each LASO shall:
1. Identify who is using the CSA (MI) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

5.3 Agency Coordinator (AC)
An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the *[agency name]*. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by LEIN/NCIC.

5.4 CJIS System Agency Information Security Officer (CSA ISO)
The CSA ISO shall:
1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.

3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

5.5 Information Technology Support

In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the *[agency name]* by performing the following:

1. Protect information subject to confidentiality concerns – in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, and internet connections as authorized by the *[agency name].* For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
2. Be knowledgeable of required *[agency name]* technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
4. Properly protect the *[agency name]*'s CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
    a. Install and update antivirus on computers, laptops, MDTs, servers, etc.
    b. Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if the *[agency name]* allows the use of personally owned devices. **(***See Personally Owned Device Policy***)**
5. Data backup and storage – centralized or decentralized approach.
    a. Perform data backups and take appropriate measures to protect all stored CJI.
    b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.
    c. Ensure any media released from the *[agency name]* is properly sanitized / destroyed. (*See Media Sanitization and Destruction Policy*)
6. Timely application of system patches—part of configuration management.
    a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
    b. When applicable, see the *[agency name]* Patch Management Policy.
7. Access control measures
    a. Address least privilege and separation of duties.
    b. Enable event logging of:
        i. Successful and unsuccessful system log-on attempts.
        ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
        iii. Successful and unsuccessful attempts to change account passwords.
        iv. Successful and unsuccessful actions by privileged accounts.
        v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
    c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
8. Account Management in coordination with TAC
    a. Agencies shall ensure that all user IDs belong to currently authorized users.

b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
c. Authenticate verified users as uniquely identified.
d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
f. Passwords
    i. Be a minimum length of eight (8) characters on all systems.
    ii. Not be a dictionary word or proper name.
    iii. Not be the same as the User ID.
    iv. Expire within a maximum of 90 calendar days.
    v. Not be identical to the previous ten (10) passwords.
    vi. Not be transmitted in the clear or plaintext outside the secure location.
    vii. Not be displayed when entered.
    viii. Ensure passwords are only reset for authorized user.

9. Network infrastructure protection measures.
    a. Take action to protect CJI-related data from unauthorized public access.
    b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.
    c. Enable and update personal firewall on mobile devices as needed.
    d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. *_Note: a police vehicle shall be considered a physically secure location._
    e. Ensure any electronic media that is removed from a physically secured location is encrypted in transit by a person or network.
    f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
    g. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the *[agency name]*. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.
10. Communicate and keep the *[agency name]* informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to *[agency name]*.

5.6 Visitor Access/Security

Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in each facility.

Prior to visitor gaining access to physically secure area:

1. The visitor will be screened by the *[agency name]* personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the *[agency name]*.
2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the *[agency name]*.
3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.
4. Escort personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to visitor departure.

All *[agency name]* personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the *[agency name]* officials. For *[agency name]*, the point of contacts to report any non-secure access is:

LASO Name:	LASO Phone:	LASO email:
AC Name:	AC Phone:	AC email:
State C/ISO Name:	C/ISO Phone:	C/ISO email:

6.0 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 of any of the requirements in this policy 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.

Other Related Resources:

- Media Sanitization and Destruction Policy (Required)
- Disciplinary Policy (Not Required)
- Personally Owned Device Policy (if allowed) (Required)
- FBI CJIS Security Policy
- Notification of Criminal Penalties Document
- Management Control Agreement
- FBI CJIS Security Addendum
- Security Awareness Training