

# CJIS METERS/NCIC Physical Protection

**Index Code:** 1106

**Effective Date:** 07/01/14 Rev 9/2/22

---

## **I. Purpose**

The purpose of this directive 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 directive focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

## **II. Policy**

It is the policy of the Queen Anne's County Office of the Sheriff to protect the Law Enforcement Information Network (LEIN) based CJI and associated information systems. A physically secure location is a facility or an area, a room or a group of rooms within a facility or an area, with both the physical and personnel security controls sufficient to protect the LEIN-based CJI and associated information systems. The perimeter is the physically secure location that 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 Queen Anne's County Office of the Sheriff shall be identified with a sign at the entrance.

## **III. Visitors' Access**

A visitor is defined as a person who visits the Queen Anne's County Office of the Sheriff on a temporary basis, who is not employed by the Queen Anne's County Office of the Sheriff and has no unescorted access to the physically secure location within the agencies where LEIN-based CJI and associated information systems are located. Visitors shall:

- A. Check in before entering a physically secure location by:
  1. Providing a form of identification used to authentic visitor.
  2. If visitors' badges are issued, the visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.
- B. Be accompanied by an agency escort at all times to include delivery or service personnel. An escort is defined as authorized personnel who accompanies 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 to monitor a physically secure location does not constitute an escort.
- C. Show agency personnel a valid form of photo identification.
- D. Follow all agency policies for authorized unescorted access to include the following:
  1. A Non-Criminal Justice Agency (NCJA), such as information technology personnel who require frequent unescorted access to restricted area(s), will be required to establish a Management Control Agreement between the Office of the Sheriff and NCJA. Each NCJA employee with CJI access will have an appropriate state and national fingerprint-based record background check prior to this restricted area access being granted.
  2. Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to establish a CJIS Security Addendum between the Department of Emergency Services and each private contractor personnel. Each private contractor personnel will have an appropriate state and national fingerprint-based record background check prior to this restricted area access being granted.
- E. Not be allowed to view screen information mitigating shoulder surfing.

F. 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 shall be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be immediately notified.

G. Not be allowed to sponsor another visitor.

H. Not enter into a secure area with electronic devices unless approved by the Local Area Security Officer (LASO), to include cameras and mobile devices. Photographs are not allowed without permission of assigned personnel.

I. All requests by groups for tours of the 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 the 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.

#### **IV. Authorized Physical Access**

A. Only authorized personnel will have access to physically secure non-public locations. **The Office of the Sheriff** 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 the necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

B. All personnel with CJI physical and local 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 check 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** 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 as indicated below.

a. All authorized **agency**, Noncriminal Justice Agencies (NCJA) **technicians** and private contractors or vendors 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 CJIS 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.

a. Report the loss of issued keys, proximity cards etc. to authorized agency personnel and document such loss on an incident report.

b. If the loss occurs after normal business hours or on weekends or holidays, personnel are to have authorized credentials **such as** proximity cards de-activated and/or door locks possibly rekeyed.

c. Safeguard and not share passwords, Personal Identification Number (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 **agency** supported computers with CJJ access (See Personally Owned Device Policy).

Use of electronic media is allowed only by authorized **agency** personnel. Controls shall be in place to protect electronic media and printouts containing CJJ while in transport. When CJJ is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

8. Encrypt emails when electronic mail is allowed to transmit CJJ-related data such as in the case of Information Exchange Agreements.

a. Agency Discretion for allowance of CJJ via emails.

b. If CJJ is transmitted by email, they must be encrypted (FIPS 140-2) end-to-end and the email recipient must be authorized to receive and view CJJ.

9. Report any physical security incidents to the **agency** LASO to include facility access violations, loss of CJJ, loss of laptops, Blackberries, flash (thumb) drives, CDs/DVDs and printouts containing CJJ.

10. Properly release hard copy printouts of CJJ 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 Sanitation and Destruction Policy).

11. Ensure data center with CJJ are physically and logically secure.

12. Keep appropriate **agency** security personnel informed when CJJ 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. Not use food or drink around information technology equipment.

14. Know which door to use for proper entry and exit of the **agency** and only use marked alarmed fire exits in emergency situations.

15. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped open and take measures to prevent piggybacking entries.

**V. Terminal Agency Coordinator (TAC)** The Terminal Agency Coordinator (TAC) serves as the point of contact at the **agency** 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.

**VI. Local Agency Security Officer (LASO)**

Each Local Agency Security Officer (LASO) shall:

A. Identify who is using the CSA (MI) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

B. Identify and document how the equipment is connected to the state system.

C. Ensure that personnel security screening procedures are being followed as stated in this

directive.

D. Ensure the approved and appropriate security measures are in place and working as expected. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

#### **VII. Agency Coordinator**

An Agency Coordinator (AC) is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractors(s)/vendors(s) and the **agency**. 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 and vendor employees and operators, scheduling of initial training, testing and certification testing, and all required reports by LEIN/NCIC.

#### **VIII. CJIS System Agency Information Security Officer (CSA ISO)**

The CJIS System Agency Information Security Officer (CSA ISO) shall:

A. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

B. 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.

C. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.

D. 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, and establish a security incident response and reporting procedure to discover, investigate, document and report to the CSA, affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

#### **IX. Information Technology Support**

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

A. 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, flash (thumb) drives and internet connections as authorized by the **agency**. 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.

B. Be knowledgeable of required **agency** technical requirements and policies, taking appropriate preventative measures and corrective actions to protect CJIS at rest, in transit and at the end of life.

C. 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.

D. Properly protect the **agency** CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions)

1. Install and update antivirus on computers, laptops, MDTs servers, etc.
2. Scan any outside non-agency owned CDs DVDs, flash drives, etc., for viruses, if the **agency** allows the use of personally owned devices.

E. Data backup and storage centralized or decentralized approach.

1. Perform data backups and take appropriate measures to protect all stored CJI.
2. Ensure only authorized vetted personnel transport off-site tape backups or any other media that

store CJI that is removed from physically secured location.

3. Ensure any media released from the agency is properly sanitized /destroyed.
  
- F. 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.
  
- G. Access control measures:
  1. Address least privilege and separation of duties.
  2. Enable event logging of:
    - a. Successful and unsuccessful system log-on attempts.
    - b. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
    - c. Successful and unsuccessful attempts to change account passwords.
    - d. Successful and unsuccessful actions by privileged accounts.
    - e. Successful and unsuccessful attempts for users to access modify or destroy the audit log file.
  3. 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.
  
- H. Account Management in coordination with TAC:
  1. Agencies shall ensure that all user IDs belong to currently authorized users.
  2. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
  3. Authenticate verified users as uniquely identified.
  4. Prevent multiple concurrent active sessions for one user identification for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
  
  5. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
  
6. Passwords:
  - a. Be a minimum length of eight (8) characters on all systems.
  - b. Not be a dictionary word or proper name.
  - c. Not be the same as the User ID.
  - d. Expire within a maximum of 90 calendar days.
  - e. Not be identical to the previous ten (10) passwords.
  - f. Not be transmitted in the clear or plain text outside the secure location.
  - g. Not be displayed when entered.
  - h. Ensure passwords are only reset for authorized user.

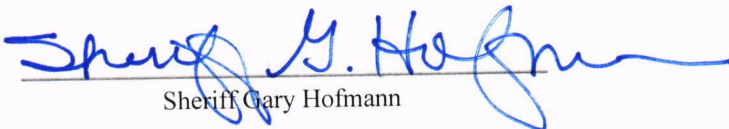
**X. Penalties**

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.

**XI. CALEA References:** None

**XII. Proponent Unit:** Administrative Services

**XIII. Cancellation:** Policy dated 07/01/14

  
Sheriff Gary Hofmann