PHYSICAL PROTECTION OF CRIMINAL JUSTICE INFORMATION (CJI)

Table of Contents

Policy Statement

The purpose of this policy is to provide guidance for Whatcom County Sheriff's Office (WCSO) 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.

Persons Affected

The intended target audience is personnel, support personnel, and private contractor/vendors with access to CJI whether logically or physically.

Directives Affected

None

Definitions

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.

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

Authorized personnel – Authorized personnel are people who may enter the WCSO unescorted and are pre-authorized to enter the facility. This includes law enforcement personnel and Whatcom County employees who have passed a national fingerprint based records check and need access to conduct their daily business. For those Noncriminal Justice Agency employees, a Management Control Agreement will be established with their department or office.

Escort - An escort is defined as an authorized person 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.

Visitor Access

1. Check in before entering a physically secure location by:
    a. Complete the visitor access log, which includes: name and visitor's agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.
    b. Document badge number on visitor log. The visitor badge shall be worn on approved visitor's outer clothing and collected by the staff at the end of the visit
2. Be accompanied by a WCSO escort at all times to include delivery or service personnel.

3. Show WCSO personnel a valid form of photo identification.
4. Follow the WCSO policy for authorized unescorted access.
    a. Noncriminal Justice Agency (NCJA) like Whatcom County IT who requires frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the WCSO 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 WCSO 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 allowed to view screen information mitigating shoulder surfing.
6. 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.
7. Not allowed to sponsor another visitor.
8. Not enter into a secure area with electronic devices unless approved by the Information Technology to include cameras and mobile devices. Photographs are not allowed without permission.
9. Be referred to the proper agency point of contact for scheduling requests for tours. Visitor rules apply for each visitor within the group.

Authorized Physical Access

Only authorized personnel will have access to physically secure non-public locations. WCSO 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. 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.
    b. 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 WCSO, Noncriminal Justice Agencies (NCJA) like 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. The training logs are available on CJIS Online.
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 WCSO personnel.

   b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the WCSO DSO to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.
   c. Safeguard and not share passwords, and all other facility and computer systems security access procedures. See Whatcom County AD152001Z Using Computer Systems.
5. Properly protect from viruses, worms, trojan horses, and other malicious code.
6. Monitor user web activity.
7. Use of electronic media is allowed only by authorized Whatcom County 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. Report any physical security incidents to the Whatcom County's IT Point of Contact to include facility access violations, loss of CJI, loss of laptops, thumb drives, CDs/DVDs and printouts containing CJI.
9. 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. Ensure data centers with CJI are physically and logically secure.
10. Ensure data centers CJI are physically and logically secure.
11. Keep appropriate WCSO 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.
12. 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.

Roles and Responsibilities

Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the WCSO for matters relating to CJIS information access. The TAC administers CJI systems programs within the agency and oversees compliance with FBI and state CJI systems policies.