27.00.080 CJIS PHYSICAL SECURITY AND ACCESS

Purpose

The purpose of this policy is to provide guidance for agency personnel for the physical and electronic protection of Criminal Justice Information (CJI).

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Criminal History Records Information (CHRI), is a subset of FBI CJIS provided data. Criminal history record information means information contained in records collected by criminal justice agencies, other than courts, on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom. Includes information contained in records maintained by or obtained from criminal justice agencies, other than courts, which records provide individual identification of a person together with any portion of the individual's record of involvement in the criminal justice system as an alleged or convicted offender. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI.

All physical 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 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 Bellevue Police Department shall be identified with a sign at the entrance, or through the use of badge access entry.

Visitors Access

A visitor is defined as a person who visits the Bellevue Police Department facility on a temporary basis who is not employed by the Bellevue Police Department and has no authorized unescorted access to the physically secure location within the Bellevue Police Department where FBI CJI and associated information systems are located. Visitors who are attending events or training in the Personnel Services Unit (PSU) may be instructed to go directly to PSU and will be asked to sign a class roster rather than a visitor access log. Commissioned law enforcement officers and civilian intelligence/crime analyst personnel from outside agencies are not classified as visitors.

Escorted visitors will check in at the Records Unit front counter located in the Police lobby prior to entering the physically secure location. The visitor will present a State or Federal issued photo identification for authentication. The visitor is required to enter information into the Police Visitor Log: date, time in and time out, visitor's name, agency/company, purpose of visit, and name of police escort. Records will document verification of photo identification.

- **Visitor Guidelines:**

  - Visitors will be accompanied by a Bellevue Police Department employee at all times while within the physically secure location to ensure the protection and integrity of the 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. Visitors not known to the employee will show a valid form of photo identification.

- Visitors will not be allowed to view CJI information on computer screens.

- Photographs or video recording are not allowed without permission of the Bellevue Police Department assigned personnel. BPD personnel should monitor any use of electronic devices by visitors to ensure this policy is complied with.

- Any BPD employee conducting an authorized tour of BPD facilities must ensure that no CJI information is inadvertently viewed by anyone on the tour.

Authorized Physical Access

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

The BPD Records Supervisor TAC maintains a current list of authorized personnel. Physical access points into the department's secure areas will be authorized before granting access. The department has 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.

Employees should be aware of who is in their secure area before accessing confidential data, take appropriate action to protect all confidential data and CJI information displayed on monitors and ensure that viewing by the public or escorted visitors is not allowed.

- ❖ Any physical security breech to include facility access violations, loss of CJI, loss of laptops, electronic devices, thumb drives, CDs/DVDs and printouts containing CJI should be reported immediately to a supervisor.

All personnel that are not escorted with CJI physical and logical access must contact the Records Supervisor/TAC for the following security clearance protocol:

1. Meet the minimum personnel screening requirements prior to CJI access
    a. Agencies must conduct a state of residency and fingerprint-based background check for all department 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.
    b. Non-department city employees, 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. Refer to the *CJIS Security Policy* for handling cases of felony convictions, criminal records, arrest histories, etc.
2. Complete Security Awareness Training
    a. The BPD Records Supervisor TAC will facilitate the Security Awareness Training for all authorized department personnel, non-criminal justice agency personnel, City of Bellevue ITD and private contractor/vendor, within six months of being granted duties that require CJI access and/or work in areas with CJI. The security awareness training is required 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 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 loss of issued keys, proximity cards, etc. to authorized agency personnel.

b. If the loss occurs after normal business hours, weekends or holidays, personnel are to call the City of Bellevue Facilities 24/7 FIXIT (425) 452-4610 to request a badge de-activation and/or door locks possibly rekeyed.
c. 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, per the Bellevue PD Technology Resource Usage Policy and the City of Bellevue Technology Usage Policy.
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 City of Bellevue IT Department and PD Records Supervisor/TAC to include facility access violations, loss of CJI, loss of laptops, Blackberries, 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.

Roles and Responsibilities

- Terminal Agency Coordinator (TAC)

The Bellevue PD Records Supervisor TAC serves as the point-of-contact at the Bellevue Police Department 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 state CJIS systems policies.

The Records Supervisor TAC manages the CJIS security clearance protocol for private contractor(s)/vendor(s) and the Department. The private contractor/vendor is subject to the CJIS Security Addendum. The TAC is 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 NCIC.