27.00.090 CJIS MEDIA PROTECTION AND DISPOSAL

Purpose

The intent of this policy is to ensure the protection of Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

Scope

The scope of this policy applies to any digital or non-digital media containing FBI Criminal Justice Information (CJI) while being stored, accessed, or physically moved from a secure location from the Bellevue Police Department.

All employees shall always protect and control digital and physical CJI and will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported.

CJIS Media Storage and Access

"Digital media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory/SD card(s).

"Non-Digital" or "Physical media" includes printed documents and imagery that contain CJI.

- ❖ To protect CJI, all employees shall adhere to the following:

  - Securely store digital and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.

  - To ensure that only authorized users have access to CJI, it must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For digital devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. Computers should be locked or logged off of when the user is not in the immediate vicinity.

  - CJI in any form must be properly disposed of by shredding or through shredding bins.

  - The use of digital and non-digital media is restricted to agency-owned systems that have been approved for use in the storage, processing, or transmission of CJI by controls set forth by the department, ITD, and the current FBI CJIS Policy.

  - CJI shall not be accessed using any personally owned digital devices unless the device has been specifically authorized for department use.

  - CJI shall not be accessed using any publicly accessible computers. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

  - In accordance with the COB Technology Resource Usage Policy, BPD Policy 16.00.250, and the current FBI CJIS Policy, the use of personally-owned media devices is prohibited on any agency/COB-owned systems that store, process, or transmit CJI. Furthermore, no employee shall use any digital media device on agency/COB-owned devices that have no identifiable owner.

- All hardcopy CJI printouts maintained by the Department must be maintained in a secure area accessible only to authorized users.

CJIS Media Marking and Transport

Any digital or non-digital media shall be clearly marked with the name/department of the recipient prior to secure transport. Furthermore, digital media transported outside of physically secure locations or controlled areas shall either be encrypted or be transported in a securable pouch.

Digital and non-digital media containing CJI is exempt from marking if it remains within a physically secure or controlled area.

All employees will control, protect, and secure digital and non-digital media from public disclosure during transport by:

- ❖ Limiting the collection, disclosure, sharing and use of CJI to only those people that require access

- ❖ Securing hand carried confidential digital and paper documents by:

  - Storing CJI in a secure package.

  - Only viewing or accessing the CJI digital or document printouts in a physically secure location by authorized personnel.

  - For hard copy printouts or CJI documents:
    - Package hard copy printouts in such a way as to not have any CJI information viewable.
    - Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

  - Not taking CJI home or when traveling unless authorized by the Department and disposing of confidential documents in a shredder or shred bin.

Dissemination to another Law Enforcement agency is authorized if the agency and the personnel receiving it are an Authorized Recipient of such information or the other agency is performing personnel and appointment functions for criminal justice employment applicants and the dissemination is authorized by BPD dissemination guidelines.

CJIS Media Disposal

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, printouts, and other similar items used to process, store and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by the City of Bellevue Information Technology Department, Records Management Services and the Bellevue Police Department.

- ❖ Non-Digital media shall be disposed of by one of the following methods (as appropriate):

  - Placed in Bellevue Police Department issued crosscut shredders.

  - Non-Digital or physical media (to include CDs) is placed in specified secured confidential shred bins within the police department to be destroyed by the City of Bellevue's current secured destruction vendor.

- ❖ Digital media vessels(hard-drives, tape cartridge, printer ribbons, flash drives, printer and copier Hard-drives, etc.), with the exception of CDs (see above) shall be disposed following the City of Bellevue Information Technology Department's Data Handling and Disposal Policy.

Breach Notification and Incident Reporting

Any inadvertent or inappropriate CJI disclosure; improper disclosure, improper use, lost, or reported as not received must be promptly reported to the employee's immediate supervisor and through the chain-of-command to the Terminal Agency Coordinator (TAC). A written report containing a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident must be submitted to the TAC within 24 hours.

Review of this policy and related procedures will occur annually and following any security incidents involving digital and/or non-digital media.

The Cloud & CJI

COB does not use any cloud computing to process CJI. Agency members shall use only cloud storage systems made available by ITD for any other department needs (e.g.: Microsoft One Drive)