Sheridan Police Department
Policies and Procedures
12.4 Replaces 302.1
Chapter 12 – Evidence & Property
Section 4 – Disposal of Physical Computer Media

Date: January 1, 2013
Revised: 1/15/2015, 10/11/2017,7/23/2021, 03/11/2022

Signature:

The purpose of this policy is to outline the proper disposal of media at the Sheridan Police Department. These rules are in place to protect sensitive and classified information, employees and the Sheridan Police Department. Inappropriate disposal of Sheridan Police Department and FBI media may put employees, the Sheridan Police Department, and the FBI at risk.

12.4.1 Destruction/Disposal of Physical and Digital Computer Media

A. When no longer usable, diskettes, tape cartridges, ribbons, digital media storage devices (jump drive, scan disks, etc) hard copies, print-outs, and other similar items used to process or store classified and/or sensitive data shall be properly disposed of in accordance with measures established by the Sheridan Police Department. The following procedures will be followed:
    1. When no longer usable, hard copies and print-outs shall be placed in properly marked shredding bins.
    2. Diskettes and tape cartridges shall be taken apart and placed in the properly marked shredding bins.
    3. After media has been shredded it will be placed in appropriate bins to be incinerated or disposed of properly.
    4. Hard drives on rented/leased copiers will be erased of department data via overwriting, wiping, degaussing, and/or destruction.

B. IT systems that have processed, stored, or transmitted sensitive and/or classified information shall not be released from the Sheridan Police Department's control until the equipment is sanitized and all stored information has been cleared. For sensitive, but unclassified information, the sanitization method shall be approved by the Sheridan Police Department. For classified systems, National Security Association approved measures shall be used. The following procedures will be followed:
    1. Employees will send all hardware that processes and/or stores classified and/or sensitive data to the Sheridan Police Department IT Administrator to be properly disposed.

C. The Chief of Police's designee will dispose of hardware and digital media storage devices by one of the following methods:
    1. Overwriting - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. The number of times the media is overwritten depends on the level of sensitive information
    2. Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets

(e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

3. Destruction - a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc. Also, computers that are used to transmit classified and/or sensitive information must protect residual.

D. Documentation will be done by the designee after the hardware is destroyed stating what process was used, what was media was destroyed, the date of the destruction. This documentation will be kept for a period of no less than four years by the Sheridan Police Department.

E. Disposal and destruction of all physical and digital media shall be performed by or witnessed by the Chief of Police's designee, the City of Sheridan IT Manager, or his/her designee, or authorized department personnel.

12.4.2 Media Protection

A. Electronic and physical media containing Criminal Justice Information (CJI) while at rest, stored, or actively being accessed shall be protected from unauthorized access, use, viewing, dissemination etc. "Electronic Media included memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, back up medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" included printed documents and imagery that contain CJI.

B. To protect CJI Sheridan Police Department personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures.
5. Not use personally owned information systems to access, process, store, or transmit CJI unless there is established and documented, the specific terms and conditions for personally owned information system usage.
6. Not utilize 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.
7. Store all hardcopy CJI printouts in a secure area accessible to only those employees whose job function requires them to handle such documents.
8. Safeguard all CJI against possible misuse
9. Take appropriate action when in possession of CJI while not in a secure area:
    a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
    b. 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 electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of

the physically secure location, the data shall be immediately protected using encryption.

i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption.
ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140--2 standards and approved by the City of Sheridan IT Manager.

10. Lock or log off computers when not in the immediate vicinity of the work area. Not all personnel have the same CJI access permissions and need to keep CJI protected on a need-to-know basis.

C. Media Transport: Dissemination to another agency is authorized if:
1. The other agency is an Authorized Recipient of such information and is being serviced by the Sheridan Police Department, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants. Department personnel shall:
   a. Protect and control electronic and physical media during transport outside of controlled areas.
   b. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel. The authorized personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:
      i. Use of privacy statements in electronic and paper documents.
      ii. Limiting the collection, disclosure, sharing and use of CJI.
      iii. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.
      iv. Securing hand carried confidential electronic and paper documents by: Storing CJI in a locked briefcase or lockbox; Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
      v. For hard copy printouts or CJI documents: Package hard copy printouts in such a way as to not have any CJI information viewable.
      vi. Not taking CJI home or when traveling unless authorized by The Sheridan Police Department LASO. When disposing confidential documents, use a shredder.

D. Breach notification and incident reporting: If CJI is improperly disclosed, lost, or reported as not received the following procedures must be followed:
1. Personnel shall notify their immediate supervisor.
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. Agency personnel shall cooperate to the best of their ability with requests from the CSA ISO in regards to security incidents.