<INSERT AGENCY NAME>

Media Disposal

|  |
| --- |
| *The purpose of this template is to assist your agency in creating its own procedures. These are the minimum topics that must be covered:*   1. *The items below in red must be specific and reflect your agency’s current practices.* 2. *Remove any items that are not applicable to your agency.* 3. *Formalize with the date and your agency name.* 4. *Remove the red box once the procedure is updated and completed.*   *If your procedure does not reflect the actual practice at your agency, then you will be found out of compliance.*  *ACCESS Section revised March 2021* |

**Purpose**

The purpose of this policy is to outline the proper disposal of media (physical and/or electronic). These rules are in place to protect sensitive and classified information, employees and the agency. Inappropriate disposal of Criminal Justice Information (CJI), Criminal History Record Information (CHRI) and/or media may put employees, the agency, the state and the Federal Bureau of Investigation (FBI) at risk.

**Scope**

This policy applies to all employees, contractors, temporary staff, and other workers at *<Insert Agency Name>*, with access to CJI/CHRI systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits CJI/CHRI and classified and sensitive data that is owned or leased by *<Insert Agency Name>*.

**Policy**

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit CJI/CHRI and classified and sensitive data shall be properly disposed of in accordance with measures established by *<Insert Agency Name>*.

Physical media (hard copies, print-outs, ribbons and other similar items) shall be disposed of by one of the following methods:

Pick one or more of the following options, where applicable

1. Shredding using agency issued crosscut shredders
2. Placed in locked shredding bins for *<Insert Private Contractor Name]* to come on-site and shred, witnessed by agency personnel throughout the entire process
3. Incineration witnessed by agency personnel onsite at the agency or non-authorized contractor incineration site

Electronic media (hard drives, diskettes, tape cartridges, CDs, flash drives and other similar items) shall be disposed of by:

*Describe in detail your method of destruction for electronic media. The method must be clear and provide an easy to understand and repeatable process.*

***Examples:***

*We overwrite magnetic hard drives using Killdisk on a three pass DOD wipe setting.*

*We use an SSD wiping utility in the BIOS to zero out the SSD.*

*We physically destroy the hard drives by drilling holes in the platters.*

*We physically destroy all electronic media using a commercial shredding service. All destruction is witnessed by authorized agency personnel.*

*For magnetic tape backups, we degauss using a degaussing appliance.*

IT systems that have been used to process, store, or transmit CJI/CHRI and/or sensitive and classified information shall not be released from *<Insert Agency Name>*‘s control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

**Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.