ADM 408
Security Policy #8
Disposal Procedure

Purpose of Policy

All media containing PII and sensitive company data, will be disposed of in a manner that destroys the data and does not allow unauthorized access to the data.

Procedures for computer/hardware disposal

1) The Security Officer or delegate will periodically notify the Information Technology (IT) department/company/individual of equipment that needs to be disposed of.

2) The Security Officer or delegate will periodically determine data sensitivity of data to be disposed of. (See Data Classification Table below)

3) IT will assess the condition of the equipment, and:
   a. IT will track the disposal of the device (type of hardware, serial number, etc). See **Appendix E: Media Disposal Log**
   b. IT will run approved wiping software on all devices to make sure all PII and sensitive company data is removed from the device.
      i. This may include physical destruction (See Methods of Destruction below)
   c. IT will verify the hardware's data has been removed.
   d. IT will dispose of the hardware.

4) The Security Officer or delegate / IT will document the destruction of the asset and keep a record. See **Appendix E: Media Disposal Log.**

5) If taken to outside facility - The media shall be taken to an approved, certified facility for erasure or destruction. A letter of certification regarding date and time of erasure/destruction shall be obtained.

Data Classification Table:

1) **Low (Unclassified)** - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
    - Basic operating system, personal files, etc.

2) **Med (Sensitive but not Confidential)** - Erase the data using any means such as reformatting or degaussing.
    - This would be for business related information which is not considered sensitive company data.

3) **High (Confidential)** - The data must be erased using an approved technology to make sure it is not readable using special technology techniques. (See method of destruction below)
    - This would be for PII and sensitive company data.

Examples of hardware devices include:

- Workstation
- Laptop
- Tablet (iPad/Android)
- Smartphones
- Server hard drives
- Memory stick (USB drives)
- CD ROM disk / DVD ROM
- Storage / Backup tape(s)
- Hard drives
- Copiers / Scanners / Fax machines
- Any equipment that contains PII or sensitive company data

Methods of Destruction Table:

Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable.)
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. • Disintegration, Pulverization, Melting, and Incineration. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm).