

Disposal of Media Policy and Procedures

1.0 Purpose

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

2.0 Scope

This policy applies to employees, contractors, temporary staff, and other workers at <Agency Name>, including all personnel with access to sensitive and classified data and media. This policy applies to all equipment that processes classified and sensitive data that is owned or leased by <Agency Name>.

3.0 Policy

When no longer usable, diskettes, tape cartridges, ribbons, 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 <Agency Name>. The following procedures will be followed:

- When no longer usable, hard copies and print-outs shall be placed in properly marked shredding bins.
- Diskettes and tape cartridges shall be taken apart and placed in the properly marked shredding bins.
- After media has been shredded it will be placed in appropriate bins to be incinerated or disposed of properly.

IT systems that have processed, stored, or transmitted sensitive and/or classified information shall not be released from <Agency Name'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 <Agency Name>. For classified systems, National Security Association approved measures shall be used. The following procedures will be followed:

- Employees will send all hardware that processes and/or stores classified and/or sensitive data to <Agency Name> <Security Personnel> to be properly disposed.

<Agency Name> <Security Personnel> will dispose of hardware by one of the following methods:

- **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.
- **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.
- **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 data. This can be accomplished with the use of integrated encryption technology. This technology uses a device or software which encrypts all data as it is written to the disk. When the user retrieves a file, the data is automatically decrypted for the owner to use. This encryption/decryption process is typically transparent to the user. Should the hard drive be removed, no useable data can be retrieved.

4.0 Enforcement

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