



Sample Policy for Disk/Media Sanitization

Updated: 09/21/2010

PURPOSE

The included document is an example of a federal policy requiring a specific disk/media sanitization process.

DISCLAIMER

The document is an example of a media sanitization policy. The information in this example **does not** supersede any federal agency's policies, procedures, guidance, or requirements with respect to media sanitization and data security. The Federal Electronics Challenge (FEC) encourages you to check within your own agency for existing agency or department disk and/or media sanitization policies, procedures and guidance. FEC Partners should discuss media sanitization and data security issues with their facility/property management, and information technology and security experts.

Federal agencies and facilities should reference the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (NIST Special Publication 800-88) for comprehensive information on media sanitization options.

REFERENCES AND RESOURCES

Additional information is available in the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (NIST Special Publication 800-88), available at: <http://csrc.nist.gov/publications/PubsSPs.html>.

The FEC provides an additional resource on media sanitization, *Media Sanitization Considerations at Electronics End-of-Life*, available at: <http://www.federalelectronicschallenge.net/resources/docs/sanitization.pdf>.

CONTACT INFORMATION

If you have questions related to this resource or need other assistance with the Federal Electronics Challenge, please contact your Regional Champion. The list of FEC Regional Champions is available at <http://www.federalelectronicschallenge.net/champions.asp>.

Partners may also request technical assistance via email to partner@electronicschallenge.net.

FEDERAL ELECTRONICS CHALLENGE

Website: <http://www.federalelectronicschallenge.net/>

E-mail: info@electronicschallenge.net

Sample Department/Agency Policy Procedures for Disk Sanitization

Approval Date:

Review Date:

Subject: All electronic information and licensed software must be properly removed when disposing of computers and other office electronics with hard drives and other storage media devices. A large volume of electronic information is stored on computer hard disks and other electronic media throughout the [Department/Agency]. Much of this information is sensitive to disclosure due to its confidentiality. Most of the software at [Department/Agency] is licensed under special agreements which prohibit the transfer of this software outside of the [Department/Agency]. These concerns apply not only to hard drives but to all other electronic storage media including, Personal Digital Assistants (PDAs), removable media such as CDs, DVDs, Universal Serial Bus (USB drives), Zip drive media, Jaz drives, backup disks, diskettes and tapes.

Purpose: Unauthorized disclosure of certain information could subject the [Department/Agency] to legal liability, negative publicity, monetary penalties, and the possible loss of funding. This procedure is designed to ensure that information technology (IT) resources do not contain information of a confidential nature before they are transferred outside of any [Department/Agency] facility for reuse, donation, recycling, or destruction. IT resources and electronic storage media will be cleaned of all information. Anything categorized as National Security Information Systems is not covered by this procedure, see [Agency Policy XYZ].

Procedures: [Department/Agency] staff and contractors must use approved techniques for proper sanitization (See Definitions) of hard drives and electronic storage media.

[Department/Agency] staff and contractors must ensure that any [Department/Agency] records stored on computer hard disks or electronic media are properly identified and captured in the [Department/Agency]'s recordkeeping system in accordance with [Department/Agency] policy and procedures prior to disk sanitization.

- Ensure that all [Department/Agency] records are properly identified and captured:
 - Electronic mail (email) is stored and accessed through the [Department/Agency]'s approved electronic recordkeeping system.
 - Electronic files that are not email must be stored and accessed through a paper-based system, and the current policy for capturing and maintaining these electronic records is “print and file.”
 - All records must be maintained for the duration of their approved retention period. (See Records Schedule at [Department/Agency intranet site]).
 - In some cases, printing may cause loss of context, (e.g., databases and complicated spreadsheets). In those cases, the records may be maintained electronically, but must be readable, accessible and usable for the entire life of the records and dispositioned in accordance with the applicable Records Schedule.

The following techniques may be used for proper sanitization:

- Overwriting hard drives utilizing Department of Defense (DOD) accepted software. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information, effectively rendering the data unrecoverable. At a minimum, a triple pass overwrite method should be used, where data is overwritten with 0's, then 1's, and then once with pseudo random data. Any system containing a hard drive or electronic storage media that has information categorized as high confidentiality must be overwritten seven times with a pattern of 0's, then 1's. A random test of hard drives should be made after overwriting. **Note:** After overwriting, the hard drive is still physically functional and can accept formatting. Therefore, office equipment with properly overwritten hard drives can be reissued, donated, or otherwise reused.
- Degauss (See Definitions) a hard drive or storage media. Degaussing results in the randomization of the magnetic domains – most likely rendering the drive or media unusable in the process. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack. If the media being sanitized cannot be economically repaired or sanitized for reuse via overwriting, then the media will be degaussed and recycled following an environmentally sound process. This option,

followed by physical destruction, must be used for any system containing a hard drive or electronic storage media that has information categorized as high confidentiality. If degaussing is performed “in house” at [Department/Agency], then a random test of hard drives should be made after degaussing.

- Physically destroying the storage media, rendering it unusable. Hard drives should be destroyed when protection can not be reliably ensured or the technology is old or can not be handled by the available tools. If the media being sanitized cannot be economically repaired or sanitized for reuse, the media will be destroyed and recycled following an environmentally sound process. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive or storage media.
 - For destruction of a CD/DVD, the most economical form of destruction is a CD/DVD shredder.
 - Zip drive media, Jaz drive media, and flash/USB drives should be physically destroyed.

Sanitization Tools: See Attachment 1.

Audience: All [Offices/Facilities] are subject to this Procedure.

Background: Studies of disk sanitization indicate that simply deleting files from the media or formatting a hard drive is not sufficient to completely erase data so that it cannot be recovered. Also, when you delete files in Windows by moving them into the Recycle Bin all data remains on the hard disk. These studies generally recommend two methods for disk sanitation. First method is the destruction of the media either by physical force or by electromagnetic degaussing. However, destroying a hard drive lessens the value of the computer system for any other use. The second method is disk sanitization, the overwriting of all previously stored data with a predetermined pattern of meaningless information, such as a binary pattern, its complement, and an additional third pattern. This has been detailed in the U.S. Department of Defense National Industrial Security Program Operating Manual DoD 5220.22-M (see <http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf>).

Authorities: Federal Information Processing Standards (FIPS 200), Minimum Security Requirements for Federal Information and Information Systems (see “FIPS 200” available at: <http://csrc.nist.gov/publications/PubsFIPS.html>).

Waivers: Waivers for these Procedures will not be considered.

Roles and Responsibilities: The primary responsibility for sanitizing computer systems, electronic devices and media, rests with the [Offices/Facilities]. Additional responsible parties:

1. Information Management Officials (IMOs) or their designees are responsible for the sanitization of all [Department/Agency]-owned electronic devices and computer systems in their [Offices/Facilities] prior to removal from any [Department/Agency] facility. This responsibility may be delegated within the [Offices/Facilities] as deemed appropriate.
2. All [Department/Agency] employees and [Department/Agency] contractors are responsible for the sanitization of computer systems and other electronic storage media as described by these procedures before disposal.

Definitions: *Degauss* – to neutralize (erase) the magnetic field. Degaussing a magnetic storage medium removes all the data stored on it. An electromagnetic degausser is a device used for this purpose.

Sanitization, sanitized –the end result after all data is obliterated. This includes all associated file system structures, operating system formatting and information from fixed disk or electronic storage media.

Recertification Date: Three years from approval date.

Additional Information Please contact [XX] at [phone number] or [email].

Attachment 1

(The suggested tools referenced below are current as of [date])

[Department/Agency] recommends but does not endorse the following products:

Tools for overwriting hard drives using DOD approved packages:

- [List software products, description, URL for more information]

Tools for degaussing hard drives:

- [List hardware products, description, URL for more information]

Tools used for physical destruction/shredding:

- [List hardware products, description, URL for more information]