Federal Electronics Challenge
Electronics Stewardship One Byte @ A Time

Sample Policy and Guidance Language for Federal Media Sanitization

Updated: 6/28/2012

PURPOSE

The language below is an example of federal policy and guidance language requiring a specific 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.

Please feel free to edit this language to fit your organizational needs, and to adhere to your organization's own policies and guidance. Text in brackets must be customized for your organization.

SAMPLE POLICY AND GUIDANCE LANGUAGE FOR FEDERAL MEDIA SANITIZATION

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]. Unauthorized disclosure of certain information could subject the [Department/Agency] to legal liability, negative publicity, monetary penalties, and the possible loss of funding. Additionally, most of the software at [Department/Agency] is licensed under special agreements which prohibit the transfer of this software outside of the [Department/Agency].

This procedure is designed to ensure that information technology (IT) resources do not contain confidential data or licensed software 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].

This procedure applies not only to hard drives but to all other electronic storage media including: compact discs (CDs), digital versatile discs (DVDs), Universal Serial Bus (USB drives), Zip disks, Jaz disks, other diskettes and tapes.

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. These studies generally recommend two methods for disk sanitation:

- The 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 process is detailed in the U.S. Department of Defense (DoD) National Industrial Security Program Operating Manual DoD 5220.22-M (see http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf).

[Department/Agency] staff and contractors must adhere to the following media sanitization requirements:

- Use approved techniques for proper sanitization of hard drives and electronic storage media, including:
    - *Overwriting hard drives utilizing 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. A random test of hard drives must 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.
    - *Degaussing hard drives or other storage media.* Degaussing results in the randomization of the magnetic domains, generally 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. This option, followed by physical destruction, <u>must</u> be used for any system containing a hard drive or electronic storage media that has information categorized as high confidentiality. A random test of hard drives must be made after degaussing.
    - *Physically destroying hard drives or other storage media.* Hard drives should be destroyed when protection cannot be reliably ensured or the technology is old or cannot be handled by the available sanitization tools. If the media being sanitized cannot be economically repaired or sanitized for reuse, the media will be destroyed. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive or storage media. Physical destruction is the most economical and practical method of media sanitization for CDs, DVDs, USB drives, Zip disks, Jaz disks, diskettes and tapes.
    - All media that is physically destroyed, degaussed, or otherwise rendered unusable must be recycled following environmentally sound practices.
- Prior to disk sanitization, 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, including:
    - 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 primary responsibility for sanitizing computer systems, electronic devices and media, rests with the [Offices/Facilities], including:

- [Responsible staff title] 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.
- 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.

REFERENCES

The NIST Guidelines for Media Sanitization are available at: http://csrc.nist.gov/publications/PubsSPs.html (See "SP 800-88").

The FEC provides an additional resource on media sanitization, *Media Sanitization Considerations for Federal Electronics at End-of-Life*, available at: http://www2.epa.gov/fec/media-sanitization-considerations-federal-electronics-end-life-6282012.

CONTACT INFORMATION

If you have questions related to this resource or need other assistance with the Federal Electronics Challenge, please contact your Regional Champion: http://www2.epa.gov/fec/technical-assistance.

Visit the FEC online: http://www2.epa.gov/fec/

E-mail the FEC: fec@epa.gov