Carnegie Mellon

Guidelines for Data Sanitization and Disposal

Document Information	
Status	Published
Published	10/01/2007
Last Updated	01/21/2010
Version	1.2

Revision History

Version	Published	Author	Description
1.0	10/01/2007	Jason Carr Doug Markiewicz	Original publication
1.1	01/29/2009	Doug Markiewicz	Updated EH&S hyperlink in Additional Information.
1.2	01/21/2010	Doug Markiewicz	Updated to reflect publication of the Guidelines for Data Classification and a new classification scheme.

Purpose

The purpose of this Guideline is to provide instructions on proper sanitization of data in both electronic and paper form. This Guideline also provides instruction on secure disposal of electronic storage media.

Applies To

This Guideline applies to all Carnegie Mellon University ("University") personnel who are responsible for the sanitization of potentially sensitive information and/or the disposal of electronic storage media.

Definitions

The National Institute of Standards and Technology ("NIST") has defined four methods of data sanitization in NIST *Special Publication 800-88, Guidelines for Media Sanitization*. These four methods are as follows:

- *Disposal* is defined as the act of discarding media with no other sanitization considerations. Examples of Disposal include discarding paper in a recycling container, deleting electronic documents using standard file deletion methods and discarding electronic storage media in a standard trash receptacle.

- *Clearing* is defined as a level of sanitization that renders media unreadable through normal means. Clearing is typically accomplished through an overwriting process that replaces actual data with 0's or random characters. Clearing prevents data from being recovered using standard disk and file recovery utilities.

- *Purging* is defined as a more advanced level of sanitization that renders media unreadable even through an advanced laboratory attack. In traditional thinking, Purging consists of using specialized utilities that repeatedly overwrite data; however, with advancements in electronic storage media, the definitions of Clearing and Purging are converging. For example, Purging a hard drive manufactured after 2001 only requires a single overwrite. For the purpose of this Guideline, Clearing and Purging will be considered the same. Degaussing is also an acceptable method of Purging electronic storage media; however, this typically renders the media unusable in the future.

- *Destroying* is defined as rendering media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting. This is a common sanitization method for single-write storage media such as a CD or DVD for which other sanitization methods would be ineffective. This is also a common practice when permanently discarding hard drives.

Electronic Storage Media is defined as any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP disks, magnetic tapes and SD cards.

Non-public Information is defined as any information that is classified as Private or Restricted Information according to the Guidelines for Data Classification.

Regulatory Requirements

There are numerous state and federal regulations that contain provisions related to the sanitization and disposal of data. For example, at least 10 states have enacted laws that require destruction of "personal information" when it is no longer needed for business. The Health Insurance Portability and Accountability Act ("HIPAA") requires formal documentation of disposal procedures to ensure health information is properly sanitized prior to being discarded. Additional details on these regulatory requirements can be obtained by contacting the Information Security Office at iso@andrew.cmu.edu.

Guidelines

The following are recommendations for when data sanitization should occur:

- All paper-based media should be disposed of when it is no longer necessary for business use, provided that the disposal does not conflict with University data retention policies, including the Policy for Financial Records Retention and the Policy on University Historic Records, or any regulatory requirements (e.g. electronic discovery).

- All electronic storage media should be sanitized when it is no longer necessary for business use, provided that the sanitization does not conflict with University data retention policies, including the Policy for Financial Records Retention and the Policy on University Historic Records, or any regulatory requirements (e.g. electronic discovery).

- All electronic storage media should be sanitized prior to sale, donation or transfer of ownership. A transfer of ownership may include transitioning media to someone in your department with a different role, relinquishing media to another department, or replacing media as part of a lease agreement.

The Guidelines for Data Classification defines three classifications of data: Public, Private and Restricted. The following table illustrates what levels of sanitization are generally acceptable based on these classifications. For media that contains more than one classification of data, the sanitization method selected should be consistent with the most restrictive classification.

Classification	Disposal	Clearing & Purging	Destroying
Public	X	X	X
Private		X	X
Restricted		X	X

The following are recommended tools and techniques for sanitization and disposal of paper-based media:

- Cross shredding should be used for Clearing and Purging of paper-based media.

- A third-party document destruction services should be leveraged for Destroying paper-based media. A Certificate of Destruction should be requested, as evidence that documents were destroyed, and retained for future reference. If a document destruction service is not available, the Information Security Office should be contacted for further guidance at iso@andrew.cmu.edu.

The following are recommended tools and techniques for sanitization and disposal of Electronic Storage Media:

- Clearing and Purging of writeable Electronic Storage Media should be performed using tools recommended by the Information Security Office (ISO). ISO recommends seven overwrites for media manufactured prior to 2001 and a single overwrite for media manufactured after 2001.

- Destruction techniques should be used when Clearing and Purging are not effective (e.g. single-write media or media that is permanently write protected).

- Cross shredding should be used for Destroying non-writeable CDs, DVDs and Floppy Disks. If cross-shredding capabilities are unavailable, destruction should be handled by the University's Environmental Health and Safety Department as specified below.

- Destruction of all Electronic Storage Media should be handled by the University's Environmental Health and Safety Department ("EHS"), unless otherwise specified in this Guideline. EHS will coordinate destruction with a third-party service provide and retain a Certificate of Destruction for all media that is destroyed. The process for initiating this service can be found on the EHS website under Computer Recycling.

- In situations where a third-party warranty or repair contract prevents proper sanitization of Electronic Storage Media, the Information Security Office should be contacted for further guidance.

Additional Information

If you have any questions or comments related to this Guideline, please send email to the University's Information Security Office at iso@andrew.cmu.edu.

Additional information can also be found using the following resources:

- EDUCAUSE / Internet2 Practical Data Sanitization Guidelines for Higher Education
  https://wiki.internet2.edu/confluence/display/secguide/Guidelines+for+Data+Sanitization

- Environmental Health and Safety's Media Destruction Service
  http://www.cmu.edu/ehs/waste-environment/computers.html

- Environmental Health and Safety's Computer Recycling Pickup Request Form
  https://ehs-alert.fms.bap.cmu.edu/forms/WastePickup.php?ahaid=3

- Guidelines for Data Classification
  http://www.cmu.edu/iso/governance/guidelines/data-classification.html

- National Institute of Standards and Technology SP800-88, Guidelines for Media Sanitization
  http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

- Information Security Office Data Sanitization Tools
  http://www.cmu.edu/iso/tools/data-sanitization-tools.html

Appendix A – Product Matrix

The following table provides a list of data sanitization tools that can be used to satisfy requirements for Clearing or Purging data. The information Security Office has recommended a secure file deletion tool for each platform.

Tool	Recommended	Features	Hyperlink
MS Windows			
BCWipe		Fee based utility for securely deleting files and sanitizing hard drives	http://www.jetico.com/products.htm
Darik's Boot and Nuke ("DBAN")		Free open source utility for sanitizing hard drives. (Commercial version also available)	http://dban.sourceforge.net/
Eraser	✓	Free GUI based utility for securely deleting files and sanitizing hard drives	http://sourceforge.net/projects/eraser/
Microsoft SDelete		Free command line utility for securely deleting files	http://www.microsoft.com/technet/sysinternals/FileAndDisk/SDelete.mspx
Secure Erase		Free DOS based utility for sanitizing ATA and SATA hard drives	http://cmrr.ucsd.edu/Hughes/SecureErase.html
Apple Macintosh			
Secure Empty Trash	✓	Built-in functionality for securely deleting files (OSX 10.3 or later)	N/A
Permanent Eraser		Free add-on utility for enhanced secure file deletion (OSX 10.2 or later)	http://www.apple.com/downloads/macosx/system_disk_utilities/permanenteraser.html
UNIX/Linux			
BCWipe		Fee based utility for securely deleting files and sanitizing hard drives	http://www.jetico.com/products.htm
Darik's Boot and Nuke ("DBAN")		Free open source utility for sanitizing hard drives. (Commercial version also available)	http://dban.sourceforge.net/
SRM	✓	Free command line utility for securely deleting files. Acts as a replacement for the rm command.	http://srm.sourceforge.net/