Data Removal Guidelines

Cory Crew - 2024-09-12 - Comments (0) - Secure Disposal

1.0 Overview

For the general user, the delete or format command appears to be the logical method of removing unwanted data files. These methods, however, are like sweeping something under the carpet: you may not be able to see it, but it's still there. All that deletion has done is remove the pointer to the files, with the data itself residing in unallocated space on the hard drive. This means that data recovery is possible using various software tools.

When sensitive information is stored on the hard drive of a machine that is to be surplussed or transferred to another individual or department, it is therefore imperative that extra measures be taken to wipe clean the hard drive before the computer leaves your area of responsibility. This document describes some common methods and software to assist you with the sanitization process. It also includes links to articles that provide detailed technical descriptions of what occurs during this process.

2.0 Sanitizing Techniques

The NIST Special Publication 800-88, Guidelines for Media Sanitization, provides an overview of sanitization techniques and requirements. According to the publication, the purpose of sanitization is "to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort", and describes the three categories of action to be taken to sanitize media as:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

See Section 5 of the document for a more detailed summary of sanitization techniques, and Appendix A for sanitization requirements for specific media/device types.

The three most common techniques for properly sanitizing hard drives are:

- **Physically destroying the drive, rendering it unusable**. This is a good

alternative for defective hard drives or those that would be too costly to repair. For added security, the disk should be overwritten or degaussed prior to destruction. ***N.B.*** Hard drives, cell phones, and PDAs that are no longer needed and contain data covered under the Brown Restricted Information Policy can be brought to the offices of ISG for crushing and disposal. Please contact ISG to schedule an appointment.

- **Degaussing the drive to randomize the magnetic domains – most likely rendering the drive unusable in the process.** Degaussing, or demagnetizing, applies a reverse magnetizing field to data stored on magnetic media, erasing the contents by returning the magnetic flux to a zero state.
- **Overwriting the drive's data so that it cannot be recovered.** Overwriting replaces previously stored data on a drive or disk with a predetermined pattern of meaningless information, rendering the data unrecoverable.

Note that when removing sensitive information, don't forget storage devices such as thumb drives, back-up external hard drives and CDs. Also, be sure to erase any stored names and numbers from phones and fax machines.

EXTRA: OIT has a hard drive crusher *used for crushing no-longer needed drives containing data covered under the Brown Restricted Information Policy. Contact the OIT Service Center for more details and to arrange an appointment.*

3.0 Suggest Software

The following chart is a collection of suggested disk wiping software. The inclusion of any title does not indicate an endorsement by Brown University or the Office of Information Technology, and has only been provided as an aide in making a decision that best matches your specific needs. See also the articles in the "Further Reading" section below for more suggestions.

Program	Cost	Platform	Comments
BitRaser	$20 for 1 license, $99 for 10	Windows, Mac & Server	NIST tested and approved.
Darik's Boot and Nuke (DBAN)	Shareware	Windows & Mac	Self-contained boot disk that securely wipes the hard disks of most computers; consumer-grade, appropriate for bulk or emergency data destruction.
Disk Utility	Free	Mac OS X	Securely erases data as well as disk's empty space (latter prevents the recovery of erased files without erasing the entire disk).

Program	Cost	Platform	Comments
East-Tec DisposeSecure	$29.95	OS independent	Erase computer hard drives, partitions or media devices; US DOD compliant.
Eraser	Shareware	Windows	Completely removes sensitive data from a hard drive by overwriting it several times with carefully selected patterns.
KillDisk (Active@KillDisk)	Freeware version, Pro versions start at $49.95	Windows & Linux	Powerful and compact software allowing you to destroy all data on hard disks, SSD and USB drives completely, excluding any possibility of future recovery of deleted files and folders; a hard drive and partition eraser utility.
Linux	Free	Linux	Use built-in *dd*, *wipe* and *shred* tools. See other recommendation in Section 4.3.
Paragon Hard Disk Manager for Home and Business	Home version: $79.95; Business / workstation version: $99.00	Windows, Mac & Linux	Multi-purpose backup and disk management tool that meets DoD sanitizing standards; includes 10 different disk sanitization methods
sDelete	Free	Windows	A command line utility that allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk; DoD-compliant secure delete program.

4.0 Removal Tips

4.1 Windows

Each of the software products listed above comes with specific instructions, some with an easy-to-use interface. Dell's Data Wipe Supported Hard Drive Sanitize Actions lists the commands in support of NIST standards, and also includes links to related data removal articles, such as Dell Data Wipe. Microsoft provides steps for using its Surface Data Eraser. See also How to Wipe a Drive on Windows 10 or Windows 11 from How-To Geek.

4.2 Macintosh

In addition to the software offered above, Mac computer hard drives can be cleared by zeroing their data. Note that zeroing data (aka "low level" format) may take a long time and

depends on the hard disk size. It is recommended to use the "8-way random" feature in conjunction with the "zero all data" option. See their Disk Utility User Guide for Erase and reformat a storage device in Disk Utility on Mac for details.

4.3 Linux/Unix & Solaris

- Linux / Unix: Securely Wipe Disk (2023) | Data Deletion in Linux File Systems (2023) | 4 Linux tools to erase your data (2021) | How to wipe free disk space in Linux (2020) | How to Securely Delete Files on Linux (2019)
- Solaris: Sanitizing Sensitive Information in the Diagnostic Collection | Erasing Disks Securely (2015)

5.0 Related Links

Further Reading:

- 35 Best Free Data Destruction Software Programs (June 2023)
- Best Data Destruction Software (May 2023)
- ST18-005: Proper Disposal of Electronic Devices, US-CERT (October 2018)
- Guidelines for Information Media Sanitization, EDUCAUSE (October 2015)
- Special Publication 800-88: Guidelines for Media Sanitization, by the National Institute of Standards and Technology, NIST (revised December 2014)

Related Sites at other Universities:

- Carnegie Mellon: Data Sanitization and Disposal Tools
- Stanford University: Data Sanitization Policy and Guidelines
- University of Minnesota OIT Security: Media Sanitization Standard