Removing Sensitive Data

Removing Sensitive Data

On this page:

Overview

Sometimes sensitive and private information can remain behind and be accessed on your device even after you think it has been "erased," making the device a target for criminal activity.

The sections below outline the steps you can take to ensure your data doesn't inadvertently become exposed when you willingly separate yourself from your devices.

The media sanitizing information on this page is offered as a suggested guideline only. IS&T currently only offers such services to departments, labs and centers via IS&T Field Support.

Removing Data from Mobile Devices

There are plenty of people who will happily buy a used device. When these items are purchased, data from previous owners can be retrieved with a little "know-how." The "smarter" the phone, the more likely it is to contain data such as bank account passwords, personal emails, or personal photos.

Phones retain data two ways:

1. On the SIM card or SD card, which can be removed
2. Stored in flash memory (the device's internal memory) - the data in memory can be retained if not properly erased, even if the device's battery is drained or removed.

Recommended steps:

1. Back up and Transfer Important Data

Back up any important data and transfer important files to your new phone, or temporarily to your computer. This includes pictures, documents, books, applications and media.

2. Delete Files from Memory

While most users remember to remove the SIM or SD card, they often forget about the internal memory. To delete memory data, users should complete a "hard reset," which returns the hardware to original factory condition. Each phone has a different hard reset procedure; some can only be done by a technician or by contacting the service's customer support. In other words, deleting information using the "clear" option in the interface is not a secure method for erasing data.

The following are suggestions per platform:

- **Android**: A factory data reset can be done by going to Menu > Settings > Privacy > Factory data reset. Conversely, you can also dial *2767*3855# which will cause the phone to power off and then power back on in a factory reset. There is some inconsistency with how certain Android phones react to the dial reset, so it may not completely wipe some phones. Also keep in mind that rooted Android smartphones may react unpredictably to a factory data reset. Additional information regarding resetting an Android device is found here

- **iPhone**: Users can erase all content from the device itself. The reset command is in the Settings menu under the General category. Steps before selling or giving away your iPhone, iPad or iPod touch. It's also possible to perform a factory data reset by connecting the phone to a computer and using iTunes. In the source list, click on the iPhone, then click on the Summary tab and choose Restore. The user will have the option to restore to a backup copy of the data or "Set up as a new phone." Choose to set it up as a new phone and all personal data will be wiped.

- **Blackberry**: Go to Options > Security Options > General Settings > Menu > Wipe Handheld. Additional information regarding resetting a Blackberry to factory state is found here.

- **Windows Phone**: Go to Settings > About > Reset Phone. There are additional methods to perform a hard reset using just physical buttons (volume and camera buttons, for instance), but they vary based on manufacturer and model. Users will need to look up the method for a specific device. Additional information regarding a Windows phone reset can be found here.

- More on mobile devices can be found here.

3. Additional privacy concerns to be aware of:

- Users can not always rely the company they donate or return the phone in regards to a secure erase. Research has found that not all companies that claim to scrub data before reselling or recycling your phone actually do so.
- Follow the manufacturer's instructions for hard resetting the phone. If you can't find your manual or need assistance, the IS&T Service Desk may be able to assist.
- The phone's cellular service provider (AT&T, Verizon, Sprint, etc.) may offer assistance with erasing the data. They may even have a recycling program available or will erase the data for their clients.
- If you are donating your phone to a charitable organization, ask if they change out the software. If not, your private data might not be removed.
- If applicable, remove the Subscriber Identity Module (SIM) card or microSD card and store it in a safe place. This portable memory chip, used in some models, holds your personal identity information and may contain phone book data and text messages. You can use the same card in your new phone if it supports the technology.
- Portable devices such as USB flash drives and iPods can also contain private information. These should be erased using the manufacturer's recommendations.
- When in doubt about whether sensitive information is retained on your device, you may want to consider physically destroying it.

Removing Data From Computers

Do not wait too long to remove the data from an old computer. You may not be able to find the power adapter or get the computer to POST. However, even if the computer is "broken", others may have the skills to access the data stored on it. (Back in 2003, grad students from MIT were able to recover private data on discarded disk drives. Of the 158 drives, only 12 had been properly sanitized.).

Recommended steps:

1. Know the Misconceptions of Erasing Files

- Reformatting a drive (the "format" command on a Windows machine) doesn't actually overwrite each block of data. To properly sanitize a hard drive, you will need to overwrite every block.
- Deleted data using the "erase" command can often be retrieved. Tossing files into the computer's trash bin and then emptying the trash deletes the record of the file, but not the data the file points to. Think of it as removing the labels from folders in a file cabinet: the folders and information in them still exist, even if retrieving the data now takes more time and effort.

2. Keep Them Out of Landfills

It helps the planet to consider recycling computer equipment responsibly. According to the International Association of Electronics Recyclers, the world's massive heap of what's called eWaste currently consists of about a billion pieces of computer equipment.

3. Securely Erase Using a Software Tool

If there could be any sensitive information on the equipment, make sure the hard drive is completely erased ("wiped").

To wipe the drive yourself, use a utility tool that overwrites every sector of the hard drive with binary 1s and 0s. Tools that meet government security standards overwrite each sector multiple times for added protection. There are many tools that meet this standard. For more information, see: Software Options.

4. Using a Service

- If you only have a few computers, hard drives or thumb drives, MIT Facilities will pick them up at no cost (items must weigh under 50 lbs). Facilities will NOT remove the data from the drives. The items are then prepared for pickup by third-party vendor, IRN, a recycling

company, who must destroy the drives of computers they recycle. They guarantee to remove data according to MA data protection law standards. Contact recycling@mit.edu for more information. Learn more about eWaste disposal at MIT.
- For large amounts of equipment, consider paying a service to wipe the drives for you. The potential liability if sensitive data gets out could easily justify the cost. MIT has an agreement with NCS-Global, an IT Asset Disposition services firm, to manage the disposal of IT products across the Institute, in collaboration with VPF Property. After de-activating equipment through VPF Property, DLCs should contact Shiva Nanda (603-926-4300 x235 Direct) at NCS to arrange for the pick-up and disposition of equipment. The company provides a certificate ensuring secure data disposal when the equipment has been processed for repurposing.
- If your area uses IS&T Field Support services, a consultant will arrange for your systems to be wiped and will store your device(s) in a secured location prior to being picked up by NCS GLOBAL.
- If not using any of the above options, make sure to use vendors who are National Association for Information Destruction (NAID) certified.

5. Other Options

When erasing the data is no longer an option because of the item's condition, physically shredding or otherwise destroying the item is the only way to protect the remaining data from access. If you use IS&T Field Support, consult with your representative regarding options.

Software Options

The software tools listed below are just a sampling of those available for wiping hard drives. They are provided for informational purposes only and are not currently supported or recommended by IS&T. If you have used any of these tools, or even other ones not listed, please send us your feedback. We would be happy to hear about your experience, whether good or bad, so that we can forward on the information and keep this page updated.

The IS&T Service Desk is not trained and does not offer support for the following software options. Customers should contact the vendor directly with usage questions.

> **Warning**: These products are designed to irretrievably erase data on your hard drive. You will not be able to recover data after running these tools on a disk. Make sure you have copied or backed up any data you need to retain.

Windows

Product	Platforms	Options	Procedure
Active@KillDisk	DOS, Any Windows platform	Free or purchase	Overwrites data using zeros. The professional version conforms to U.S. Dept of Defense (DOD) standards.
Darik's Boot & Nuke	Any Windows platform	Free	Completely and permanently erases all content of any hard disk it detects by overwriting it with random numbers.
Ontrack Eraser	Any Windows platform	Purchase	Permanently deletes information by overwriting all data on the hard drive or on selected partitions of a drive.
Eraser	Windows OS	Free	Securely deletes specific files. Can delete files manually via right click on the file (or Recycle Bin), or set up a scheduler. Can also overwrite all 'free space.'
R-Wipe & Clean	Any Intel-compatible platform running Windows OS	Free trial or purchase	Shreds specific files or folders using either fast or secure erase algorithms.
Softpedia/DP Wiper	Any Windows platform	Free	Overwrites data from one to 35 passes and has DOD-compliant wiping.
ShredIt	Any Windows platform	Free trial or purchase	The program's overwrite methods include user-defined options with up to 35 passes.
WipeDrive	Any Windows platform	Purchase	Overwrites data as many times as you need and runs a verification test

Macintosh

Product	Platforms	Options	Procedure
Darik's Boot & Nuke	Apple Power Mac and Intel computers	Free	Completely and permanently erases all content of any hard disk it detects by overwriting it with random numbers.
Disk Utility Secure Erase	Mac OS X 10.4 or later	Built into the OS	Overwrites data as many times as you need from select hard drives using several options.

NetShred X	Mac OS X 10.1 or later	Free	Erases files your browser and email program leave behind.
Permanent Eraser	Mac OS X 10.3.9 or later	Free	Uses Gutmann Method: overwrites 35 times, scrambles original file names, truncates file size to nothing.
Secure Empty Trash	Mac OS X 10.3 or later	Built into the OS	Shreds specific files. Move the file to the Trash, and then the "Secure Empty Trash" is accessed from the Finder menu. Overwrites data 7 times.
ShredIt	Minimum OS 7	Purchase	The program's overwrite methods include user-defined options with up to 35 passes. Can also overwrite rewritable CDs (Mac version only).

Unix

Product	Platforms	Options	Procedure
`shred`	Various	Free	Built in secure delete utility present on the majority of *nix systems.
Active@KillDisk	Various	Free or purchase	Overwrites data using zeros. The professional version conforms to U.S. Dept of Defense standards.
BC Wipe	Various	Free trial or purchase	Repeatedly overwrites a special pattern to the hard drive to destroy its files.
Darik's Boot & Nuke	Various	Free	Completely and permanently erases all content of any hard disk it detects by overwriting it with random numbers.

Additional Resources

When data has been safely removed and the item is ready to be recycled, see the Department of Facilities page on recycling and eWaste pickup, or send email to recycling@mit.edu.

Related Links

- Safe Electronic Waste Recycling
- Data Removing or Destruction
- Software Tools to Find, Delete or Protect Data
- How can a computer be recycled at MIT?