

Best Practices in Disposal of Computers and Electronic Storage Media

*Guidelines for end users and computer
support personnel to follow when
disposing of computers or storage media
that may contain sensitive information*



Best Practices in Disposal of Computers and Electronic Storage Media

Guidelines for end users and computer support personnel to follow when disposing of computers or storage media that may contain sensitive information

Overview

At some point in the life cycle of a computer its owner will decide to dispose of the equipment. When this occurs, it is important to take action to ensure that confidential or sensitive information is not revealed to the eventual recipient of the equipment. The same issues apply to storage media such as optical disks, backup tapes, etc. This document describes best practices to follow prior to disposal of equipment or media.

This document explains the issues and gives an overview of steps you should take. For specific instructions and examples, please see the MSU computing knowledge base article number [6567](#) (Go to help.msu.edu and enter the article number in the search box.).

The Problem

Many users of computers believe that if they delete a file from their computer no one can retrieve it. In one study, researchers at MIT acquired 100 hard drives on the used market and found confidential information

such as social security numbers and health records on a large percentage of the devices.

Virtually any computer – laptop, desktop, or server – in use at MSU may at some time contain confidential or sensitive information. Some computers may house huge amounts of such information. It is therefore prudent to thoroughly sanitize computer hard drives and other storage devices before disposal or repurposing.

The same concerns apply to backup and archival media such as CD-R, CD-RW, DVD-R, DVD-RAM, ZIP drives, other backup tapes – any media that might contain confidential or sensitive information. When an individual or unit at MSU disposes of backup or archival media the information should be “scrubbed” or the media destroyed.

Records Retention

Before “scrubbing” or destroying a hard drive or other form of storage, be sure to retain copies of any institutional data as required by federal or state law, contract, or MSU policy. University Archives provides guidance on university records retention policies on their Web site at <http://www.msu.edu/unit/msuarhc> .

This document pertains to electronic storage media – primarily digital media. Similar concerns apply to paper records and to analog media such as audio cassette tapes, video tapes, etc. Units should be aware of and respect both records retention and privacy considerations no matter what format or media is involved.

Deletion Is Not Destruction

Many do not realize that operating system file deletion commands do not physically remove data from hard drives and other storage devices. Instead, file deletion merely marks the area of the hard drive as available for re-use.

“Disk doctor” or forensic detection tools can allow someone to retrieve information previously stored on the hard drive even after it is invisible to the computer’s operating system. Failure to understand this has proved embarrassing and costly to Fortune 1000 companies, to governments, to universities, and to individuals.

Specifically:

- Deleting a file in the operating system does not remove the file. In Windows by default the file goes into the Recycle Bin where it may be trivially retrieved.



- Even after the file is removed from the Recycle Bin, traces of it remain on the hard drive.
- Even an operating system “Format” operation does not fully erase information on a hard drive.
- Deleting an e-mail message from the In-box and emptying the trash bin or deleted items may not physically remove it from the hard drive.
- Deleting a record from a database may not remove all traces of the information.
- Even if data is thoroughly deleted from a primary storage device such as a hard drive, copies or traces may remain on backup tapes, CD-R or other optical disks, or portable media such as flash (“thumb”) drives.

Data or traces of data may remain in many places:

- The Web browser cache, which may hold many megabytes of Web pages viewed.
- Any password management tools, whether Web browser or other software.
- Any temporary storage.
- Embedded within documents. For instance, Microsoft Word keeps historical information as documents are edited. That information can be retrieved even if the Word application does not display it.

Thus, it is prudent to ensure that there is no possibility that sensitive information remains accessible when equipment or media is disposed:

- Whenever a computer is disposed or reassigned, the hard drive should be “sanitized,” removing all data.
- Whenever any storage media are disposed, all data should be removed, or the media destroyed.

Disposal versus Repurposing

When equipment becomes obsolete, units may choose several courses of action at Michigan State University.

- Send the equipment to MSU Surplus for sale or other disposal.

- Reassign the equipment for some other purpose. For instance, a laptop computer might be reassigned to a graduate student or a retired faculty member.

Whether the equipment is sent to Surplus or repurposed, it is prudent to ensure that the hard drive contains no sensitive information. For instance, suppose a computer was used by an administrative assistant in the business office to handle personnel transactions. Rather than try to ascertain whether the computer might house sensitive information, the prudent course is to totally sanitize the hard drive.

Sanitizing Hard Drives and Backup Tapes

Specialized software is available to “sanitize” (or scrub, or wipe clean) a hard drive before it is disposed or repurposed. This software makes several passes over the entire surface area of every platter of the hard drive, in compliance with standards set by the U.S. Department of Defense.

See the MSU computing knowledge base article [6567](#) for examples and instructions.

Magnetic tapes can be erased using a degaussing device, which randomizes the magnetic patterns on the media, rendering it unreadable.

Destroying Storage Media

Some media cannot be sanitized. For instance, a CD-R permanently retains the data initially written to it. Physical destruction is the only solution. For CD-R discs and other optical media, some shredders on the market are able to destroy the disc in a fashion similar to shredding paper.

For particularly sensitive information, it is prudent to physically destroy the media, even if it could be sanitized or degaussed. For instance, if you have a server hard drive or RAID array or backup tapes that house social security numbers or health information, you may wish to physically destroy the device or media.

Exercise caution when physically destroying media. For instance, before breaking a compact disc, be sure you are wearing protective eyewear.

“Accidental Disposal” – Loss or Theft

If a computer – or a device such as a thumb drive – is lost or stolen, any information on the device can fall into the hands of someone who may harvest confidential information for identity theft.

⋮

In one case, a major university had a laptop computer stolen with confidential information, including social security numbers, on the hard drive. This occurred despite a university policy that prohibits the storage of confidential information on portable devices.

The prudent course is to never store confidential information on portable devices.

Daily Safeguards

Some computers – desktop, laptop, or server – are used daily to process sensitive information. When such computers are disposed or repurposed, the steps discussed in this memo should be followed. But it is also prudent to take steps every day:

- Acquire, install, and use software that cleans known areas of vulnerability, such as the browser cache, temporary files, the Recycle Bin, etc.
- Log out of secure applications when not in use.
- Employ a screen saver with password protection and configure it to employ a short timeout period.
- Turn the computer off when not in use.
- Do not leave passwords written down in a place near the computer.
- Do not store confidential or sensitive information on portable devices such as laptops or thumb drives.
- Whenever possible, encrypt sensitive information on any medium on which it is stored.