Background

Computing systems (including desktops, laptops, tablets, networking equipment, cellular phones, smart phones, PDAs and other mobile devices) store data on a wide variety of storage media (e.g., hard drives, USB flash drives, solid state drives, floppy disks, CD-ROM's, DVD's, Blu-Ray's, tapes, memory, etc.). This data must be securely removed from the media once the data and/or device is no longer required in order to prevent unauthorized disclosure of the data. This is particularly important if the device contains restricted or controlled data as defined in the Data Protection Policy 9.1.1.

Data could be disclosed through many avenues including computers or equipment sold, recycled or disposed without appropriate media destruction practices, equipment with storage media returned to vendors as defective or as a trade-in for new equipment, or mobile media not being properly destroyed after use.

Media that will not be reused should be physically destroyed. Media that will be reused should be properly sanitized by using an approved method.

In addition to the Information Security Data Retention Policy 9.1.17, each college or department should have a record retention schedule that dictates when different types of information may be discarded or destroyed as defined by UC Records Management.

Standard

This document utilizes the Department of Defense (DOD) Directive 5220.22 and the National Institute of Standards and Technology (NIST) Special Publication 800-88 as the basis for this standard.

- DOD Directive 5220.22 states that functional drives should be overwritten 3 times prior to disposal or reuse.

- NIST Special Publication 800-88 goes into fine detail explaining the need for proper media sanitization, types and trends of media, types of sanitization, roles and responsibilities, and much more information related to this topic.

While the delete or format command is commonly considered to be the logical method of removing unwanted data files, these methods are not satisfactory for data sanitization. Although data/files may seem to have disappeared, it is very likely that the data is still present and can be recovered by using various software tools.

When restricted data is stored on media that is to be transferred to another individual or department, it is imperative that extra measures be taken to wipe the media before it leaves your area of responsibility. This document describes some common methods and software to assist you with the sanitization process.
For additional information of any questions, please review the NIST Special Publication 800-88 - Guidelines for Media Sanitization and/or contact the UCIT Office of Information Security at infosec@uc.edu or 513-558-ISEC (4732).

Sanitization

The most common techniques for properly sanitizing media are:

1. **Overwriting** – Overwrite the hard 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. This is commonly referred to as “wiping” and is the most common method of sanitization.

2. **Destruction** – Physically destroy the drive and render it unusable.
   - This is a good alternative for defective hard drives or those that would be too costly to repair. For added security on functional hard drives, the disk should be overwritten or degaussed prior to destruction.

3. **Degaussing** – Randomize the magnetic domains, 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.

### Destruction Practice by Media

<table>
<thead>
<tr>
<th>Media</th>
<th>Reuse</th>
<th>Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Disk</td>
<td>DOD 5220.22 erase prior to format</td>
<td>Physical destruction or degauss</td>
</tr>
<tr>
<td>Floppy Disk</td>
<td>Degauss or erase prior to format</td>
<td>Physical destruction, degauss, or erase</td>
</tr>
<tr>
<td>Caseless Optical (CD/DVD)</td>
<td>Typically N/A</td>
<td>Physical destruction (break into pieces or uniformly abrade surface)</td>
</tr>
<tr>
<td>ZIP/Cartridge</td>
<td>DOD 5220.22 erase</td>
<td>Physical destruction or degauss</td>
</tr>
<tr>
<td>Solid state, USB/Flash</td>
<td>Erasing is unpredictable, but nonetheless recommended prior to format</td>
<td>Physical destruction</td>
</tr>
<tr>
<td>Tapes</td>
<td>Degauss</td>
<td>Physical destruction or degauss</td>
</tr>
</tbody>
</table>

### Wiping Utilities

The following utilities meet industry best practices for data sanitization on common read/write media for hard disks, floppy disks, and USB flash drives.

<table>
<thead>
<tr>
<th>Utility</th>
<th>Disk</th>
<th>File</th>
<th>PC/Win</th>
<th>Mac</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Darik's Boot and Nuke (DBAN)</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Floppy or CD bootable x86 system</td>
</tr>
<tr>
<td>Eraser</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Active@ Kill Disk</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Disk Utility (OSX native)</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Wipe/Shred (Linux native)</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Common Linux distributions</td>
</tr>
<tr>
<td>Dd/dcflddd</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>UNIX utility</td>
</tr>
</tbody>
</table>
Disposition of Assets

This standard applies to the sanitization of data. Please refer to the Asset Disposition Policy for the proper disposition of university assets.

Related Links

Asset Disposition Policy 2.1.15
Data Protection Policy 9.1.1
Information Security Data Retention Policy 9.1.17
University of Cincinnati Records Management
NIST Special Publication 800-88 - Guidelines for Media Sanitization

Phone Contacts

UCIT Office of Information Security 513-558-ISEC (4732)
UCIT Integrated Help Desk 513-556-HELP (4357)