

Procedures to Sanitize Computers & Storage Media Devices

The most efficient and economical means of sanitizing computers and/or a storage media device is to overwrite the entire device with zeroes.

In some circumstances it is best to physically destroy the storage device. Some examples include:

- Non-Functioning Computers
- Non-Functioning Storage Media Devices
- Ineffective sanitization process
- Sanitization process is not economically feasible

When physical destruction is used, departments are still responsible for sending the remains to Property Disposition for proper disposal.

Sanitizing

How to sanitize PC Hard Drives

To sanitize PC hard drives we recommend that departments use either Active @ Kill Disk or DBAN (Darik's Boot and Nuke); both of which are available in a commercial, and a free version. For the majority of systems the free version is sufficient to accomplish the policy requirements and carries no time limit.

NOTE: For systems containing sensitive information we recommend using a minimum of 3-passes, preferably a 7-pass method which will guarantee that all data is rendered useless.

Using Active @ Kill Disk

Prepare a boot diskette or boot CD by downloading and running the boot disk creator or downloading and burning the ISO image from the Active @ Kill Disk website. (<http://www.killdisk.com>)

- Boot the system from the diskette or CD.
- Kill Disk will start automatically, select Active@ Kill Disk [Free].
- Select your drive from the listing, and then use the F10 key to initiate the process.
- For the free version, default settings are sufficient, use the F10 key to confirm erase.
- When erasing is complete, Kill Disk will terminate.

NOTE: The free version is only capable of running a single pass of zeros, which is sufficient for policy requirements but will not be adequate on machines which contain sensitive information. Sanitizing multiple hard drives in a single computer, or running multiple passes of zeros requires the purchase of the commercial Kill Disk product. Pricing and license terms are available on the Active@ Kill Disk Website.

Using DBAN

Prepare a boot CD by downloading and burning the ISO Image from the DBAN website. (<http://www.dban.org>)

- Boot the system from the CD.
- DBAN will start automatically.

Note: For policy requirements "dodshort" method is sufficient, for sensitive information we recommend using the "dod" method, this a 7-pass method used by the Department of Defense.

- Type “dodshort” for a 3-pass wipe; or “dod” for the 7-pass wipe, and press return, DBAN will automatically begin to erase the primary hard disk.
- When erasing is complete, DBAN will terminate.

How to sanitize Macintosh Hard Drives (Prior to OSX)

- Boot the system from the Mac OS CD.
- Run the Drive Setup Utility under the Utilities folder on your Mac OS CD.
- Start by selecting the hard drive you wish to low-level format.
- Under the Function menu, select Initialization Options.
- Select Low Level Format (a check mark will appear) and click OK.
- Click Initialize at the bottom of the main screen.
- Again click Initialize.

Sanitizing a OSX Macintosh

- Boot the system from the OSX Installation CD or DVD.
- From the Utilities menu at the top, choose Disc Utility.
- Then select the hard-disk you wish to sanitize.
- Under the Erase Tab, there is a Security Options section.
 - For most sanitation purposes the Zero-Out Option is satisfactory.
 - **For sensitive information, we recommend using the 7-Pass Erase Option to ensure the data is rendered completely unrecoverable.**
- Click OK then click Erase.

How to sanitize Sun Systems

(x86/x64 AMD Based – 2003 and newer)

As tested on the Ultra 20 Sun System; these machines are capable of booting from a CD just like a PC and should be handled in a similar manner, using either Active@ Kill Disk or DBAN, detailed instructions can be found in the PC Section.

Other Sun Systems

For the systems prior to 2003 we recommend that you remove the hard drives for destruction, hard drives removed should be separated and boxed for shredding through Property Disposition.

How to sanitize other architectures and servers

There are many types of architectures, processors, and operating systems in use at the University of Michigan. No single sanitization method will work on all platforms. For systems where sanitation is not possible, we would recommend that you remove all hard drives and/or storage disks and separate them for disposal.

Alternative Destruction of Unsanitized Hard Drives

Hard drives which contain sensitive information that cannot be sanitized through conventional means should be removed from the systems, boxed and set-aside for shredding through Property Disposition. The department is responsible for covering the cost (\$3.00 charge per hard disk), and will be issued a "Certificate of Destruction".

Physical Destruction

Physical destruction should only be used in the following instances:

- When computers or hard drives are inoperable.
- When data tapes such as DDS (Digital Data Storage), DLT (Digital Linear Tape), DAT (Digital Audio Tape), or DC (Data Cartridge) cannot be overwritten through reformatting or initialization.

Destruction Process

- Remove the hard drive, tape, or cartridge from the computer or storage unit.
- Get on all your safety equipment, Hard-Hat, Safety Glasses, and Gloves.
- Place the device flat or on its side and strike it with a heavy hammer until it is crushed. **NOTE:** Pay particular attention to damaging the platters inside the hard drives where data is magnetically recorded. This type of damage will normally discourage the average person from attempting to recover any data.
- All destroyed hard drives, tapes, and other storage media must be sent to Property Disposition for proper disposal.

Assignment of Responsibility

Instructions for Non-Technical Departments or persons sending surplus computers to Property Disposition: Property Disposition computer consultants will provide assistance and direction to any department/person encountering problems with the sanitization process. Please feel free to contact us by email: ljdixon@umich.edu or by telephone (734)763-7206.

Property Disposition will provide departments with the option of service legal agreements, which are negotiable to sanitize your computers and storage devices on a continuing basis. Contact Steve Sinelli by email: ssinelli@umich.edu or by telephone (734)763-7303.