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 and Apple Hard Drives

To sanitize PC and Apple hard drives ITS recommends that departments use Kill Disk available through ITS.

NOTE: For systems containing sensitive information ITS recommends using a minimum of 1-pass random NIST 800-88.

Using Kill Disk

Prepare a boot USB thumb drive or boot CD by downloading and running the boot disk creator or downloading and burning the ISO image from the ITS website. ([http://documentation.its.umich.edu/node/478](http://documentation.its.umich.edu/node/478))

- Boot the system from the USB thumb drive or CD.
- Kill Disk will start automatically
- Select your drive from the listing to initiate the process.
- When sanitation is complete, Kill Disk will generate a conformation certificate that can be printed or saved as a PDF.

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 Kill Disk, 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

Kill Disk is the preferred method to sanitize server drives (if this method does not work contact ITS or HITS)

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

- **Shredding is the only recommended method of physical destruction**

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: cmcpeake@umich.edu or by telephone (734)764-2590.

Property Disposition will provide departments with the option of service level 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.