Procedures to Sanitize Computers & Storage Media Devices Agency Wide

Sanitizing

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

The Physical Destruction\Recycling section below explains the complete process for removing drives and preparing them for destruction.

How to sanitize PC Hard Drives

To sanitize PC hard drives that do not contain sensitive data 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 you must use software that will make a minimum of 3-passes, preferably a 7-pass method which will guarantee that all data is rendered useless. This software must also print out regulatory compliant certificates for audit purposes. This will require the commercial version, please see the Network Admin (NA) to get access to this software. If you choose to just remove the drive for destruction instead, then you must make a minimum 1-pass wipe before removing it, if at all possible.

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. (Killdisk Website)

- 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.
- Fill out Form MISC-374E "Certification for Media Sanitation\Destruction" and then attach a completed "Certified Clean Media To Be Recycled" sticker to the outside of the computer enclosure before sending to M&R.
- A MISC-374D "Property Disposal Form" will also have to be completed for each computer\device before sending to M&R.

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.

Using DBAN

Prepare a boot CD by downloading and burning the ISO Image from the DBAN website. (DBan Website)

- 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.
- Fill out Form MISC-374E "Certification for Media Sanitation\Destruction" and then attach a completed "Certified Clean Media To Be Recycled" sticker to the outside of the computer enclosure before sending to M&R.
- A MISC-374D "Property Disposal Form" will also have to be completed for each computer\device before sending to M&R.

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.
- Fill out Form MISC-374E "Certification for Media Sanitation\Destruction" and then attach a completed "Certified Clean Media To Be Recycled" sticker to the outside of the computer enclosure before sending to M&R.
- A MISC-374D "Property Disposal Form" will also have to be completed for each computer\device before sending to M&R.

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.
- Fill out Form MISC-374E "Certification for Media Sanitation\Destruction" and then attach a completed "Certified Clean Media To Be Recycled" sticker to the outside of the computer enclosure before sending to M&R.
- A MISC-374D "Property Disposal Form" will also have to be completed for each computer\device before sending to M&R.

How to sanitize other architectures and servers

There are many types of architectures, processors, and operating systems in use at the University of Arkansas Cooperative Extension Service. No single sanitization method will work on all platforms. For systems where sanitation is not possible, it is recommend that you remove all hard drives and/or storage disks and separate them for disposal following the Physical Destruction\Recycling section below.

Alternative Destruction of Unsanitized Hard Drives

Hard drives which contain sensitive information that cannot be sanitized through conventional means should be removed and separated for disposal following the Physical Destruction\Recycling section below.

Physical Destruction\Recycling

Physical destruction should only be used in the following instances:

- When computers or hard drives are inoperable.
- When data is deemed too sensitive to trust any wipe software methods.
- 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

- Complete a 1-pass wipe of the drive if at all possible before removal.
- Remove the hard drive, tape, or cartridge from the computer or storage unit.
- Attach a "No Hard Drives" sticker to the outside of the enclosure.
- Fill out Form MISC-374E "Certification for Media Sanitation\Destruction".
- Deliver the drive and a copy of the form to the NA for secure storage until pickup by the vendor choosen to do drive destruction.

Documentation Retention

Copies of all forms will be kept by the NA for a minimum of 5 years. These include:

- MISC-374D "Property Disposal Form"
- MISC-374E "Certification for Media Sanitation\Destruction"
- Certificate of Destruction from the vendor

Quick Reference:

Hard Drive Remaining in Computer\Equipment	
Public Data	**Sensitive Data**
1-Pass wipe by approved software	3-7 Pass wipe by approved software (see the NA for licensed software)
Sticker applied to outside of enclosure "Certified Clean Media To Be Recycled"	Sticker applied to outside of enclosure "Certified Clean Media To Be Recycled"
Form MISC-374E "Certification for Media Sanitation\Destruction"	Form MISC-374E "Certification for Media Sanitation\Destruction"
Form MISC-374D "Property Disposal Form"	Form MISC-374D "Property Disposal Form"
Deliver to Warehouse with copy of MISC-374D	Deliver to Warehouse with copy of MISC-374D
Deliver copy of MISC 374D and MISC 374E to NA for document retention	Deliver copy of MISC 374D and MISC 374E to NA for document retention

Hard Drive Removed from Computer\Equipment for Destruction	
Public Data	**Sensitive Data**
Form MISC-374E "Certification for Media Sanitation\Destruction"	1-Pass wipe by approved software if possible
Form MISC-374D "Property Disposal Form"	Attach "No Hard Drives" sticker to outside of enclosure
Deliver enclosure to Warehouse with copy of MISC-374D	Form MISC-374D "Property Disposal Form"
Deliver hard drive to NA for secure storage with copy of MISC-374E	Deliver enclosure to Warehouse with copy of MISC-374D
	Deliver hard drive to NA for secure storage with copy of MISC-374E