

# Procedures for Media Disposal, Destruction, and Redeployment

## 1. Objective

The objective of this document is to establish procedures for the implementation of the University's Media Disposal, Destruction, and Redeployment Protocol. Primarily, these procedures explain the process of preparing media for redeployment (reassignment), as well as offering additional resources and tools for erasing data.

## 2. General Principles

2.1. Reasonable steps must be taken to ensure that all Business Information is rendered unrecoverable prior to reuse or disposal of the media on which it is stored

2.1. Between the time that media containing Business Information is removed from service, and the time it is sanitized or destroyed, it must be safeguarded. Storage space should meet at least the same security requirements as the original usage environment.

2.1. Transfer of equipment to the Office of Equipment Management for disposal, surplus or redeployment must include certification that the media has been appropriately sanitized.

## 3. Procedures

The following media transfers are common at the University and each entails different sanitization methods.

The Minimum Action listed is based on the sensitivity of the data, and on the potential for physical access to the storage media. The latter involves a distinction between "keyboard access" or ordinary usage, and "laboratory access," i.e., methods that involve physically dismantling a device in a laboratory and examining the storage media with special equipment.

**DOD 5220.22 Standard**—Triple Overwrite of data with verification. Write all locations with a pattern; write with the complement; write with a random pattern; verify.

### 3.1 Examples

**Reconfiguration Only:** A computer or other media is reconfigured for the same individual or set of individuals; there is no change in access.

- **Risk:** Computer is not accessible for laboratory attack and access permissions do not change.
- **Minimum action:** Hard disks can be reformatted and a new image installed without overwriting all existing data; removable media can be reformatted and reused as appropriate.

**Public Use:** A computer or other media is reconfigured for continued use in a public users room.

- **Risk:** Computer is not accessible for laboratory attack; users have only limited expectation of data security.
- **Minimum action:** Hard disks can be reformatted and a new image installed without overwriting all existing data.

**Reassignment within unit:** A computer or other media is reconfigured for use by a new user within the same unit.

- **Risk:** Computer is not accessible to laboratory attack; data access privileges have changed.
- **Minimum action:** Hard disk should be overwritten by software that meets the DOD 5220.22 standard for triple overwrite with verification, or ATA Secure Erase with verification.

**Redeployment:** A computer or other media is transferred to a different unit within the University.

- **Risk:** Data access permissions have changed; control of the physical device has passed to a new unit.
- **Minimum action:** Hard disk should be overwritten by software that meets the DOD 5220.22 standard for triple overwrite with verification, or ATA Secure Erase with verification.

**Surplus or Disposal:** A computer or other media is designated for surplus or disposal and is leaving University control.

- **Risk:** Computer is accessible to laboratory attack; data is leaving control of the University.
- **Minimum action:** Disks should be destroyed, degaussed, or overwritten by software that meets the DOD 5220.22 standard for triple overwrite with verification, or ATA Secure Erase with verification.

**Warranty Exchange:** A computer or other media is broken and, under warranty, must be returned for exchange.

- **Risk:** Media with data is leaving control of the University; media is accessible to laboratory attack.
- **Minimum action:** Unless vendor has a contractual agreement to maintain data security, media should be degaussed before returning to vendor.

**Note:** Degaussing of hard disks will almost certainly render the standard warranty invalid, unless a "retain your media" option has been purchased.

## 4. Additional Resources

### Resources for Media Sanitization

<http://cmrr.ucsd.edu/people/Hughes/DataSanitizationTutorial.pdf>

[http://ata.wiki.kernel.org/index.php/ATA\\_Secure\\_Erase](http://ata.wiki.kernel.org/index.php/ATA_Secure_Erase)

### Hard Disks: Windows

UCSD ATA Secure Erase Utility, <http://cmrr.ucsd.edu/hughes/subpgset.htm>. Be sure that the proper ATA protocol has been implemented by the manufacturer.

Darik's Boot and Nuke, <http://dban.sourceforge.net>.

KillDisk, <http://www.killdisk.com>

NoTrace, <http://www.comtechnologies.com>

DataEraser, <http://ontrack.com>  
UniShred Pro, <http://www.lat.com>  
WipeDrive, <http://www.accessdata.com>  
InTether Sanitizer, <http://www.infraworks.com>  
Gdisk.exe, Symantec Ghost  
CyberCide, <http://www.cyberscrub.com/cybercide/>  
East-Tec's DisposeSecure,  
East-Tec Sanitizer, <http://east-tec.com/sanitizer/index.htm>  
East-Tec Eraser, <http://east-tec.com/eraser/index.htm>  
Heidi's Eraser, <http://www.heidi.ie/eraser/>  
DriveCleanser, <http://www.acronis.com/products/drivecleanser>  
AutoClave, <http://staff.washington.edu/jdlarios/autoclave>  
BC Wipe, <http://www.jetico.com/download.htm>  
Burn 2.5, <http://www.securemac.com/burn.php>  
DiskWipe, [http://www.dtidata.com/products\\_disk\\_wipe.asp](http://www.dtidata.com/products_disk_wipe.asp)  
NTI Dragon Burn, [https://secure.ntius.com/esdsoft/dragonburn\\_v5\\_full.asp](https://secure.ntius.com/esdsoft/dragonburn_v5_full.asp)  
DataEraserPro, <http://www.ontrack.com/dataeraser>  
Paragon Disk Wiper, <http://www.disk-wiper.com/>  
ShredIt, [http://www.mireth.com/test/shredit\\_sp.html](http://www.mireth.com/test/shredit_sp.html)  
SuperScrubber, <http://www.jiiva.com/superscrubber/>  
WipeDrive, <http://www.whitecanyon.com/wipedrive-erase-hard-drive.php>

### **Hard Disks: Apple OSX**

<http://docs.info.apple.com/article.html?artnum=50447>  
<http://docs.info.apple.com/article.html?artnum=107437>  
<http://docs.info.apple.com/article.html?artnum=152060>  
<http://docs.info.apple.com/article.html?artnum=75102>

### **Unix**

[www.giac.org/practical/gsec/Ken\\_Hatfield\\_GSEC.pdf](http://www.giac.org/practical/gsec/Ken_Hatfield_GSEC.pdf)Linux

### **Solaris**

[http://www.sun.com/software/solaris/trusted/solaris/ts\\_tech\\_faq/purge.xml](http://www.sun.com/software/solaris/trusted/solaris/ts_tech_faq/purge.xml)

### **Cell Phones**

[http://wirelessrecycling.com/home/data\\_eraser/default.asp](http://wirelessrecycling.com/home/data_eraser/default.asp)

## **PalmOS**

<http://kb.palm.com/>; Search for SolutionID 15574, "Performing a factory reset before your palm device changes ownership or is sent away for repair." Or, for SolutionID 887 for older devices.

## **Blackberry Devices**

<http://www.blackberry.com>; Knowledge base article kb-02318, "How to delete all data, or all data and applications on the BlackBerry device."

- Enter kb-02318 in the search engine on the top right.
- Open the document. Select BlackBerry Technical Solution Center in the top left.
- In the search engine under BlackBerry Technical Solution enter kb02318;
- Select the article "How to delete all data or all data and applications on the BlackBerry Smartphone".
- Select the Wipe Handheld option and follow the instructions.

## **Flash media (thumb drives, memory cards and other solid state drives)**

Due to the manner in which data is written to solid state drives (SSD), a process that makes extensive use of randomization, tools that are effective in erasing fixed media will meet with varying degrees of success when used on SSDs. Given that, a SSD would require a highly sophisticated "laboratory attack" to recover lost data. All but the most sensitive data can be considered effectively erased using fixed media overwrite tools. To absolutely guarantee non-recovery, the drive should be physically destroyed.

## **CD, DVD, floppy disks**

Cross-cut shredding, or other means of physical destruction.

## **AIX, SGI, SANS, NAS and tape drives**

Use tools recommended by manufacturer.

## **Published Materials**

R. Kissel, M Scholl, S Skolochenko and L Xing. Guidelines for Media Sanitization: Recommendations of the National Institutes of Standards and Technology. NIST Special Publication 800-88.

DOD 5220.22 Standard: Automated Information System Security. Chapter 8, especially the Clearing and Sanitization Matrix.

H2E-HIPAA Guidance Document on the Destruction of Confidential Paper. Attachment A, Electronic Media Destruction.