# Electronic Media Sanitization

## Background

Computing systems (including desktops, laptops, tablets, networking equipment, cellular phones, smart phones and other 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 Export Controlled or Restricted data as defined in the Data Governance & Classification Policy.

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

## Standard

The NIST Special Publication 800-88r1 - Guidelines for Media Sanitization is used as the primary guide for this document. NIST Special Publication 800-88r1 explains the need for proper media sanitization, types of sanitization, roles and responsibilities and much more information related to this topic.

The Electronic Media Sanitization Standard is mandatory for media that contains Export Controlled or Restricted data and is recommended for media that contains Controlled data. Export Controlled data may have additional sanitization requirements, see Export Controls Office for additional information.

Each college or department must adhere to the University General Retention Schedule unless the college or department has an approved unique schedule.

When Export Controlled or Restricted data has been stored on media where that media is to be reused or forwarded to UC Surplus Management for appropriate disposition, it is imperative that measures be taken to sanitize the media before it leaves control of the department of responsibility. This

document describes some common methods and software to assist you with the sanitization process.

While the delete or the 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 and 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.

Appropriate verification must be done after the electronic media has been wiped to ensure data is not recoverable or that the media has been destroyed.

Data owners who store data on cloud based file storage must use tools, techniques and best practices in cooperation with the cloud vendor to delete data as needed.

## Sanitization

The following list provides a general description of each of the three most common techniques for sanitizing media:

1. **Clear** – Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard read and write commands to the storage device, or using a menu option to reset the device to the factory state. Clearing protects information from a keyboard attack but not from a laboratory attack. In most cases, this is completed via the GUI via a “Reset to Factory Settings” or similar command.

2. **Purge –** Purging is the act of erasing data using third party sanitization utilities so that it is unlikely that a laboratory attack can recover the data. Newer drive technologies like solid-state drives (SSD) purge using a technique called cryptographic erase. Purging may be a better alternative than destroying a device when you factor in environmental concerns and the desire to reuse the media. In most cases, this may be referred to as “wiping” a device with a utility to over-write content which makes the original data unrecoverable. In the case of cryptographic erase, the secret key used to decrypt the data is destroyed making recovery of encrypted data not possible.

3. **Destroy** – Destruction of media is the most secure form of sanitization. Physical destruction can be accomplished using a variety of methods, including shredding, pulverizing and disintegration.

A term that is **not** a sanitization technique but should be defined is **Disposal**. Disposal is the act of discarding media with no sanitization considerations. Examples of disposal would include discarding paper in recycling container

without shredding, deleting electronic data using file delete function built into the operating system and discarding non-sanitized electronic storage media in a standard trash bin. Disposal of media or equipment containing Export Controlled or Restricted Data without sanitization is a violation of the Data Governance and Classification Policy.

When purging data follow the guidelines established by NIST Special Publication 800-88r1 - Guidelines for Media Sanitization which states "a single write pass should suffice to purge the media. Optionally: Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified."

Using standard purge techniques may not work properly on SSD's as they require the use of Cryptographic Erase. Cryptographic Erase involves first encrypting the SSD, then purging the encryption keys, eliminating the possibility of decrypting the drive while at the same time allowing the drive to be reused.

## Recommended Destruction Practice by Media

| Media | Data Classification | Reuse in Department | Reuse or Sale Outside of Department |
|---|---|---|---|
| Hard Disk nonSSD | Controlled | Clear | Purge |
| | Restricted | Purge | Purge |
| SSD | Controlled | Clear | Crypto-erase |
| | Restricted | Purge | Crypto-erase |
| USB/Flash | Controlled | Clear | Crypto-erase |
| | Restricted | Purge | Crypto-erase |
| Floppy Drive / Zip Drive | Controlled | Clear | Purge |
| | Restricted | Purge | Physical Destruction |
| CD / DVD / Blu-ray | Controlled | N/A | N/A |
| | Restricted | N/A | N/A |
| Tapes | Controlled | Clear | Purge |
| | Restricted | Purge | Physical Destruction |

The Export Controls Office generally recommends all media that contained Export Controlled data be destroyed. Please contact the Export Controls Office for additional information.

## Mobile device (Mobile Phone and Tablet)

The theory behind mobile device sanitization is simple, but the execution differs depending on the operating system version and device. First,

copy/backup any data that may be needed in the future. Next, remove any removable media if the device has one, this is usually some type of microSD card. Verify that the device is encrypted. If the device is already encrypted, then do a factory reset. If the device is not encrypted; encrypt the device, then do a factory reset. Encrypting the device then doing a factory reset, deletes the encryption key (Cryptographic Erase). There is no way to decrypt the device, effectively rendering the data on the device deleted.

Some mobile operating systems and/or devices don't encrypt the microSD card, remove and physically destroy the microSD card. Do not pass the microSD card along with the mobile device.

## Sanitization 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.

| Utility | Disk | File | PC / Win | Mac | Other |
|---|---|---|---|---|---|
| Darik's Boot and Nuke (DBAN) | Y | N | Y | Y | Floppy or CD bootable x86 system |
| Eraser | Y | Y | Y | N | N |
| Active@ Kill Disk | Y | N | Y | Y | N |
| X-Ways Secure | Y | N | Y | N | N |
| Disk Utility (OSX native) | Y | Y | N | Y | N |
| Wipe/Shred (Linux native) | Y | Y | N | N | Common Linux distributions |
| Dd / dcfldd | Y | Y | N | N | UNIX utility |

## Disposition of Assets

This standard applies to the sanitization of data. Please refer to the UC Surplus Management department for the proper disposition of university assets. Contact the Surplus Management Department to enquire about the availability and cost of industrial shredding of devices and hard drives.

## Contact Information

IT@UC Office of Information Security 513-558-ISEC(4732) Infosec@uc.edu

## Related Links

Data Governance & Classification Policy
Export Controls Office

NIST Special Publication 800-88 - Guidelines for Media Sanitization
UC Surplus Management
UC Records Management

## History

Issued: 07/10/2013
Revised: 10/31/2016
Revised: 12/16/2016
Revised: 04/26/2017