Media Sanitization Guideline

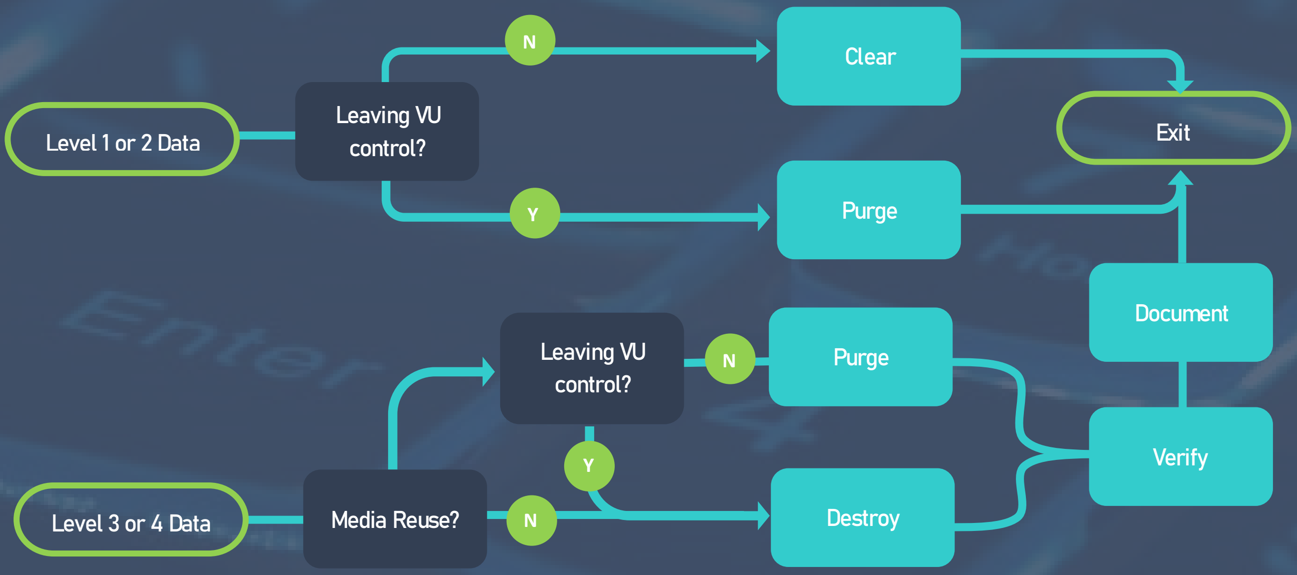
Media is the material carrying data, such as paper or electronic storage devices. Media sanitization is a process of removing data from media so that it cannot be retrieved or reconstructed. It is a key step in assuring data confidentiality.

When data is no longer needed it should be sanitized from the media that it was on. Some examples of when media sanitization should be employed may include:

- A device is transferring ownership,
- A device is at the end of its useful life and will be retired or surplused, or
- Data retention is no longer allowed by contract or regulation and must be destroyed.

There are multiple ways that media can be sanitized. The method used should be based on the sensitivity of the data; however, available methods can vary depending on the media type and its manufacturer. The most restrictive method available should be used when possible. This guidance document can be used to help the Vanderbilt community practice appropriate measures for keeping VU data safe.

Once you have determined that media needs to be sanitized, use the decision flow to help guide which method to use.



See Vanderbilt's Data Classification Policy for more information on data sensitivity levels.

Full details can be found in NIST SP800-88: Guidelines for Media Sanitization.

Additional guidance can be found at Educause Guidelines for Information Media Sanitization.

Sanitization Methods

Media Type	Examples	Clear	Purge	Destroy
		Applying software or hardware products to overwrite target data with non-sensitive data or using a menu option to reset to the factory state. It cannot be used on damaged media or if the media is not rewritable.	Applying software or hardware products to overwrite target data with non-sensitive data or using a menu option to reset to the factory state. It cannot be used on damaged media or if the media is not rewritable.	Applying physically destructive techniques to render data recovery infeasible and subsequently the makes the media unusable. Destroying also clears and purges.
Magnetic Media	Magnetic disks and tapes, ATA/SCSI Hard Disk Drives	Overwrite using at least 1 pass of a random, fixed value (e.g., all zeros) or non-sensitive signals	Degauss, Secure erase unit, or Sanitize with overwrite or cryptographic erase	Incinerate or Shred
Flash Based Storage	Solid State Drives, memory cards	Overwrite using at least 1 pass of a random, fixed value (e.g., all zeros) or non-sensitive signals	Sanitize with block erase or cryptographic erase	Shred, Disintegrate, Pulverize, or Incinerate
Locally Attached Hard Drives	USB, Firewire	Overwrite using at least 1 pass of a random, fixed value (e.g., all zeros) or non-sensitive signals	Not always available, refer to the manufacturer	Shred, Disintegrate, Pulverize, or Incinerate
Optical Media	CD/DVD, Blu-ray disk	N/A	N/A	Optical disk grinding, Incinerate, Shred
Network Device	Router, switch	Perform full manufacturer's reset	Not always available, refer to the manufacturer	Shred, Disintegrate, Pulverize, or Incinerate
Office Equipment	Printer, fax, etc.	Perform full manufacturer's reset	N/A	Shred, Disintegrate, Pulverize, or Incinerate
Paper	Paper, microform	N/A	N/A	Cross cut shred, Disintegrate, Pulverize, or Incinerate to white ash

How do I accomplish sanitization at VU?

Clear

Contact your IT administrator (e.g., for VUIT-managed electronic devices submit a ticket). Alternatively, see the table of Example Clearing Software for potential clearing tools.

Purge

Contact your IT administrator (e.g., for VUIT-managed electronic devices submit a ticket).

Destroy

- Paper: Use Shred-It containers.
- Electronic devices in the VUIT Data Center: Submit a ticket to VUIT's Network Operations Center.
- All other electronic devices: Submit a ticket to the FutureVU Sustainability office (i.e., Campus Recycling Program, Computer and Electronics Waste).

FAQs

What is Cryptographic Erase?

A purging method in which the Media Encryption Key (MEK) for the encrypted target data (or the Key Encryption Key – KEK) is sanitized, making recovery of the decrypted target data infeasible.

What does it mean to degauss?

A purging method that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Degaussing any current generation hard disk will typically render the drive permanently unusable since these drives store track location information on the hard drive. Also called demagnetizing.

What is a full manufacturer's reset?

A clearing method that deletes the file pointers but does not directly rewrite storage contents.

In the decision flow, what does it mean to verify?

The process of testing the media to ensure the data cannot be read.

In the decision flow, what does it mean to document?

The process of recording sanitization completion details such as Media type/manufacturer/model/serial #, Media owner/data owner/data classification; Sanitization method used/tool used/person performing method/verification.

Example Software for Clearing

		Compatible Operating Systems			
Software Application	License / Cost Type	Windows	MacOS	Linux	Description
Darik's Boot and Nuke (DBAN)	Shareware	Yes	Yes	Yes	Data erasure for full volumes or partitions. Terminal interface.
Disk Utility	Freeware		Panther or later		Data erasure for full volumes or partitions. Application with a graphical user interface.
Disk Wipe	Freeware	XP or later			Data erasure for full volumes or partitions. Application with a graphical user interface.
Eraser	Freeware	Windows 7 or later			Data erasure for full volumes, partitions, and single files. Application with a graphical user interface.
KillDisk	Free and Professional	Windows	MacOS	Linux	Data erasure for full volumes or partitions. Application with a graphical user and command-line interfaces. Provides completion certificate.
dd	Freeware		Panther or later	Kernel 2.0 or later	Data erasure for full volumes, partitions, and single files. Command-line tool.
Shred	Freeware		Panther or later	Kernel 2.0 or later	Built-in dd, wipe and shred tools.
sDelete	Freeware	Vista / 2008 or later			Data erasure for full volumes, partitions, and single files. Command-line tool.
Secure rm	Freeware	Vista or later		Kernel 2.0 or later	Data erasure for full volumes, partitions, and single files. Command-line tool.
Wipe	Freeware			Kernel 2.0 or later	Data erasure for full volumes, partitions, and single files. Command-line tool.

Example Media Sanitization Form

Data Owner Information

Owner Name & Title	Fname Lname, Professor
Owner Email	email@vanderbilt.edu
Other Contact Name(s)	Fname Lname, Lab Manager
Other Email	email@vanderbilt.edu

Sanitization Information

Data Classification	○ Level 1 Public ○ Level 3 Restricted ○ Level 2 Private ○ Level 4 Critical
Media Type	CD/DVD, USB, etc.
Manufacturer / Make / Serial	Companyname / Version N / #1234
Sanitization Method	Clear / Purge / Destroy
Sanitization Date	00/00/0000
Proof	Certificate of destruction / screenshot / or task results