Media Sanitization and Disposal Best Practices

Federal Student Aid

An OFFICE *of the* U.S. DEPARTMENT *of* EDUCATION

What is Media Sanitization?

Media sanitization is a process by which data is irreversibly removed from media, or the media is permanently destroyed. Media sanitization is a key element in protecting personal privacy and proprietary information. The principal goal of media sanitization is to ensure that sensitive data is not unintentionally released.

Common media include physical documents, desktop and laptop computers, mobile devices, external hard drives, USB drives, and memory devices.

Why is Media Sanitization Important for Educational Institutions?

Educational institutions collect and maintain massive amounts of sensitive student data, including personal, academic, and financial, to provide their services. Proper data management, especially data destruction, is critical in protecting sensitive information against unauthorized access or disclosure.

This fact sheet discusses guidelines for media sanitization to ensure data is properly destroyed according to the National Institute of Standards and Technology (NIST). Educational institutions are encouraged to carefully evaluate their existing policies on media sanitization to make sure they adhere to these guidelines, or to create policies if none currently exist.

Media Sanitization Methods

Media sanitization methods come into play not only when storage devices reach end-of-life, but also when they are being repurposed for use within an educational institution. NIST Special Publication 800-88, Rev. 1, "Guidelines for Media Sanitization" provides methodological guidance for sanitizing media so that all data is irretrievable. Clear, Purge, and Destroy are actions that can be taken to sanitize media:

- **Clear** uses standard rewriting techniques and tools to provide moderate protection against simple, non-invasive data recovery techniques. Most storage media support some level of Clear and media can be reused after Clear sanitization.
- **Purge** uses state-of-the-art laboratory overwrite, block erase, and cryptographic erase methods. It provides a higher level of media sanitization than Clear and is thus used when handling more confidential data. The storage media can be reused after Purge sanitization.
- **Destroy** uses physical destruction techniques, such as shredding, pulverizing, and incinerating, to render data recovery infeasible. Destroy can be used when media is beyond overwriting methods due to its physical condition or when it contains highly confidential data. Media cannot be reused.

Educational institutions can determine what media sanitization method to use according to data confidentiality level, whether the media will be reused, and media type.

Media Sanitization Steps

1 Categorize Media According to Data Confidentiality Level

Inventory all hardware, software, storage devices, systems, files and any other data accessible by employees according to data confidentiality level. Media sanitization should be based on the confidentiality of the data on the media, rather than the media itself. Consult Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, for both information and information systems security categories.

2 Determine Media Life Cycle Stage

Hardware and media that is being repurposed and reused within an educational institution may have different data destruction processes than media that has reached end-of-life. A common data vulnerability occurs when devices change hands within an institution, or are sold, without properly removing data. determines what type of sanitization method (Clear, Purge, or Destroy) is needed based on data confidentiality, media life cycle stage, and cost. If media are not intended for reuse, the simplest sanitization method may be Destroy.

3 Sanitize Media

Properly sanitize media based on the media type. Consult Appendix A of the NIST Guidelines for Media Sanitization for a comprehensive list of specific sanitization techniques for various media, including obsolete equipment. Common applications in higher education are below:

- **Paper documents:** NIST guidelines recommend Destroy by using crosscut shredders that produce particles that are 1 mm x 5 mm in size (or smaller).
- **Desktop and Laptop Computers, External Hard Drives:** For Clearing, NIST guidelines recommend overwriting media by using organizationally approved and tested overwriting technologies/methods/tools.
- **Mobile Devices:** For Clearing or Purging, NIST guidelines recommend manually erasing all information and then performing a full manufacturer's reset to factory default settings.

See Appendix for a list of open-source media sanitization tools.

4 Document and Verify Data Sanitization

Require sanitization documentation and signature certification regardless of the media sanitization method. Verify that sanitization occurred and review a media sample to ensure that no data is recoverable. Without verification, inadequate sanitization methods can be implemented and leave school data exposed.

Resources

- NIST Special Publication 800-88, Rev. 1, "Guidelines for Media Sanitization"
- Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)

Media Sanitization Best Practices

- Create and abide by your school's media sanitization policy, which is a formal document outlining processes for data destruction within your institution.
- Media sanitization method (Clear, Purge, or Destroy) should be based on the sensitivity of the data, not the media type.
- Data storage devices, regardless of data confidential level, should be destroyed prior to disposal. Remove hard drives from desktops and laptops prior to disposal.
- Avoid using file deletion, disk formatting, and one-way encryption to dispose of sensitive data. These methods leave most of the data intact and vulnerable to retrieval by bad actors.
- Shred physical documents so they are safe for disposal or recycling.
- Sanitize faulty storage media before returning it to the manufacturer for service or replacement. Many data breaches happen this way.
- Verify all data sanitization procedures to ensure data is irretrievable.
- Document all media sanitization with signature confirmation by the individual performing the sanitization.
- When drafting written agreements with third parties, include provisions specifying that all personally identifiable information (PII) provided must be destroyed when no longer needed, including copies in system backups, temporary files, or other storage media.

Federal Student Aid recognizes the importance of strong data security. Find more FSA cybersecurity resources at **fsapartners.ed.gov/title-iv-program-eligibility/cybersecurity.**

Appendix

If your institution has not purchased a standard overwriting tool, freeware and open-source options are listed below. The list is for informational purposes only and the tools are not supported or endorsed by FSA. Customers should contact the vendor directly with usage questions.

- Active@ Kill Disk
  https://www.killdisk.com/eraser.html
- Darik's Boot and Nuke
  https://dban.org/
- Disk Utility Secure Erase
  https://support.apple.com/guide/disk-utility/erase-and-reformat-a-storage-device-dskutl14079/mac
- Edenwaith Permanent Eraser
  http://www.edenwaith.com/products/permanent%20eraser/
- Softpedia DP Wiper
  https://www.softpedia.com/get/Security/Security-Related/DP-WIPER.shtml