Guidelines for Information Media Sanitization

Practical Information Media Sanitization Guidelines for Higher Education

Last reviewed: July 2015

Background

Much sensitive and private information at educational institutions is recorded and maintained outside central information technology systems on various desktop and portable devices and removable media. This information is recorded and maintained by university and college community members including full and part-time faculty, administrators and staff members.

Sensitive data may include information classified by the institution's administration; information protected by laws such as FERPA, HIPAA, GLBA, and state law; information that could lead to identity theft, institutional embarrassment, or loss of personal privacy; and licensed software or restricted intellectual property. Common storage devices and media include desktop, portable, and laptop computers; personal digital assistants (PDA's) and Cellular Telephones; removable storage such as CD's, DVDs, floppy disks, ZIP disks, external hard drives, USB drives, and MP3 players.

When these storage and media devices become obsolete or are no longer needed the sensitive or private data must be effectively removed from the storage media or be destroyed before the devices are recycled, reused, disposed of, or discarded. The removal process is variously called data removal, data/media sanitization, data/media destruction, or similar terms. This is distinct from the terms data de-identification or data masking which refer to modifying live data from production systems so the data can be used in development and testing environments without exposing the production data. In this document we will use media sanitization for compatibility with federal guidelines.

Current Practice

Many educational institutions have developed policies on removal of institutional data from obsolete or excess information technology assets. However, until the NIST Guidelines for Media Sanitization were issued in September 2006, little authoritative, comprehensive, and straightforward information and advice on media sanitization was available. As a result institutions have often chosen ineffective or excessively expensive policy approaches for assets scheduled for recycling, internal or external reuse, or disposal.

For example, some institutions specify simple disk formatting. This approach does not actually destroy the information on the media. Others specify complex and relatively costly Department of Defense procedures which go far beyond the requirements to defeat any data burglar without sophisticated laboratory equipment and a great deal of disposable time. Others require routine degaussing or total physical destruction in all cases. That approach ignores the actual information value and and the actual extent of any risks associated with the stored information while eliminating any residual device value either within the institution or to external organizations.

Educational institutions are encouraged to carefully re-evaluate their existing policies on media sanitization, or to thoughtfully create such policies if none currently exist, using the NIST Guidelines for Media Sanitization and the practical advice collated here.

> **Handy Hint**
>
> A list of higher education computer disposal policies and practices is available below.

The NIST Guidelines

The National Institute of Standards and Technology published **NIST 800-88 Revision 1, Guidelines for Media Sanitization**, in December 2014. This document provides the previously missing authoritative and comprehensive advice and forms the basis for a rational approach to protecting and eliminating sensitive data stored on no longer needed IT assets and media.

The NIST Guidelines identify four types of media sanitization to employ with different data security categories on various types of storage media and devices. The sanitization types in order of effectiveness and severity are Disposal, Clearing, Purging, and Destroying.

- **Disposal** involves simply discarding the media
- **Clearing** involves making the data on the media unreadable by normal means through measures such as overwriting
- **Purging** removes the data more robustly and protects the removed data from laboratory grade attacks
- **Destroying** makes the media unusable

The sanitization types are hierarchical in that Purging also Clears while Destroying also Purges and Clears. Full details on the four types of media sanitization are provided in section 2.4 and section 5 of the NIST Guidelines.

The NIST Guidelines, Section 3 covers recommended roles and responsibilities for staff members involved in media sanitization. A detailed process for deciding which type of media sanitization is appropriate in a specific case is laid out in the NIST Guidelines, Section 4.

NIST Guidelines, Appendix A recommends specific methods to accomplish each type of sanitization for a very broad range of media types and storage devices currently or historically used in information technology. NIST Guidelines, Appendix B presents a comprehensive glossary while NIST Guidelines, Appendix C covers tools and resources. NIST Guidelines, Appendix D provides advice for home users and telecommuters and NIST Guidelines, Appendix E lists technical references.

The NIST Guidelines roles and responsibilities and the decision-making process can map well into higher education institutions. In addition, individual community members can apply the sanitization recommendations in the absence of highly technical support staff.

Making Sanitization Decisions

The decision-making process for how to appropriately sanitize a device or media involves several steps. These include:

- **Assessing** the sensitivity and security category of the stored data
- **Selecting** the appropriate media sanitization type based on the category
- **Selecting** the appropriate media sanitization method for the type and media
- **Sanitizing** the media
- **Verifying** the result

To apply the NIST Guidelines most effectively, an institution should have a data classification policy to aid in assessing data sensitivity. The institution's specific classifications can then map into the low, moderate, and high security categories used in the NIST Guidelines' sanitization decision-making process. In addition, the policy should be well publicized so that the institution's community members can either accurately assess data sensitivity themselves or assist a specialist in making an assessment. In practical application, the highest security category of any data stored on the media should apply to the entire media. Section 2.5 of the NIST Guidelines provides a list of considerations for the entire decision-making process.

The assessment of sensitivity and risks should include consideration of issues such as license breaches and intellectual property disclosures as well as institutional disruption or embarrassment and loss of personal privacy and identity theft. A knowledgeable and responsible individual should certify the assessment.

Once the Security Category has been assessed, an appropriate media sanitization type should be selected based on the assessment. Then the most cost-effective technique for the media and sanitization type can be implemented. Cost considerations should include any loss of residual value from partial or complete destruction of a reusable data storage asset.

Most Common Practical Considerations

For the most common educational institution faculty and staff situations the assets to be sanitized will be paper; Windows, Macintosh, and Unix desktop and laptop computers; and peripheral devices and media. The computers will have hard drives and solid state storage and typically will also be used with removable media such as floppy disks, ZIP disks, CD's, DVD's, external hard drives, USB drives and MP3 players. In addition to MP3 players, Cellular telephones and PDA's are increasingly becoming sanitization concerns.

Media sanitization by Clearing will likely be sufficient for most common applications in higher education. Some highly sensitive data may require Purging if a potential thief is assumed to have access to laboratory-grade reconstruction facilities. It is likely that only a small fraction of institutional data would require sanitization by Destruction though that may be selected as the lowest cost alternative. The NIST Guidelines note that for many sorts of media the acts of Purging, Clearing, and/or Destroying may be equivalent. For example, crosscut shredding implements all three sanitization types for paper media.

Consult the NIST Guidelines, Appendix A for full detail on specific techniques to implement each type of sanitization on various media. The range of media types in the Appendix is quite comprehensive and includes devices such as copiers and fax machines and media such as paper, hard drives of all types, and many varieties of memory. Recommendations based on the appendix for some common cases are included below.

Floppy Disks, Zip Disks, CDs, DVDs

While Clearing or perhaps Purging would be appropriate for most examples of these media types, for normal volumes of magnetic or optical media with any level of sensitive data the most cost effective data sanitization method may well be Destruction. The residual value of floppy and zip disks is low, so Clearing or Purging may not be worth the effort. A cost-effective technique for secure Destruction of office volumes will likely be shredding in a crosscut or diamond-cut office paper shredder designed for optical disk destruction. A commercial provider can shred bulk volumes. Consult the NIST Guidelines, Appendix A for other alternatives.

Desktop and Laptop Computers, External Hard Drives

To sanitize the disks of these devices by Clearing, an overwriting tool can be used. If your institution has not purchased a standard tool, you can consider a number of open source or freeware tools such as:

- Active@ Kill Disk
- Darik's Boot and Nuke
- DP Wiper
- Eraser

Since none of the open source or freeware tools listed above will work with computers running a Macintosh operating system, consider using Jiiva's SuperScrubber, which is a disk sanitization product for the Mac. MIT's Information Services & Technology Department provides examples of additional software options for Windows, Macintosh, and Unix.

To Purge data from devices with modern ATA disk drives, consider using the Secure Erase utility from The University of California at San Diego or secure erase functions in commercial packages or operating systems. You can also use degaussers or degaussing wands, though these will effectively destroy a disk drive by making it permanently unusable. In these cases, physical Destruction may be more cost effective.

Compact Flash Drives, SD Cards

To sanitize these memory devices by Clearing an overwriting tool such as one of those listed above for disks can be used. If Purging is necessary, the devices should be physically destroyed by shredding, disintegrating, pulverizing, or incineration.

PDAs and Cellular Telephones

For Clearing or Purging the NIST Guidelines, Appendix A recommends manually deleting all information and then performing a full manufacturer's reset to factory default settings. It further recommends contacting the manufacturer for current sanitization procedures.

Other Considerations

Higher education institutions use many systems that fall outside the most common situations. These include complex systems such as servers, server systems, robust storage systems, and scientific instruments. In addition there is a good deal of obsolete and outdated equipment still in current use at higher education institutions. Provisions must also be made for equipment returned to manufacturers or sent for repair.

- **Complex Systems** - Systems administrators with servers, server systems, and more complex storage assets such as RAID arrays and computer-based scientific instruments should become familiar with the NIST Guidelines and should follow its recommendations and procedures for effective media sanitization and disposal.
- **Obsolete Equipment** - The NIST Guidelines, Appendix A is quite comprehensive and covers many historical media types such as core memory that might still be in service.
- **Warranty Service and Repair** - Storage assets returned to a vendor for warranty service or replacement or sent to an external party for repair should be sanitized to the same extent as assets to be disposed of, unless a binding business agreement covering data handling responsibilities and liabilities is in place. If sanitization is necessary but is impossible without physically destroying a media device, repairs should be made on-campus. Otherwise a robust business agreement and secure transport will likely be required.

Survey of Higher Education Computer Disposal Policies and Practices

- **Arizona State University**
  Arizona State's Property Control Manual states that property must be disposed of through Surplus Property. It further notes that the releasing department must securely wipe hard drives and other data-containing medium before transfer to Surplus Property. But it additionally notes that if the department fails, Surplus Property computer staff will handle the task.
- **Auburn University**
  Auburn's policy on electronic data disposal places responsibility for sanitizing devices and media with Deans, Directors and Department Heads. The policy requires data removal to DOD standards or destruction. The policy notes that OIT will sanitize equipment at standard hourly rates and discourages hard drive destruction.
- **Baylor University**
  Baylor's disposal policy states that central ITS will handle all data removal and computer disposal. It further states that ITS will erase data to DOD specifications or will destroy the device.
- **Lehigh University**
  The university's disposal policy requires that all data on hard drives be overwritten with zeros for disposal or for internal or external transfer.
- **New York University**http://www.nyu.edu/asset/surplus-computer.html
  Asset Management disposal procedures requires that units certify the secure destruction of all data in computers or electronic storage devices prior to disposal. Units may use an approved vendor to sanitize equipment and certify data destruction or may follow ITS guidelines to sanitize equipment.
- **Northwestern University**
  The NUIT disposal policy requires units to remove software and data before disposal or recycling. NUIT also provides a central service for formal disposal and suggestions for units that handle their own disposal.
- **University of Florida** Media Reuse and Data Destruction Standards for IT Workers
  Asset Management Services requires that data be destroyed in accordance with university standards for disposal. IT's media reuse and destruction standard specifies procedures and guidelines and provides links to an extensive list of resources.
- **University of Hawaii System** Disposal Guidelines for Unused Computer Equipment and Securely Deleting Electronic Information
  IT provides a policy on transfer and recycling of computer equipment. The policy includes a requirement to securely delete personal information as well as suggestions for recycling resources, programs, and vendors. The policy links to an "ask us" document with secure deletion procedures, tips, and instructions. The document also covers cell phones, PDAs, and storage media.
- **University of Illinois**
  The University of Illinois provides an Administrative Policy on Disposal of Digital Media as well as a Standard for the Disposal of Digital Media. Both are available in the EDUCAUSE Resource Library at the above URL. The administrative policy covers university compliance with digital media disposal requirements under Illinois law and references the new standard. The standard itself provides detailed procedures for sanitizing media commonly used in higher education, guidance on compliance with Illinois law, and references to useful federal sanitization documents.
- **University of Iowa**
  The CIO policy requires that "...computer and digital storage media must have all institutional data and licensed software reliably erased from the device prior to its transfer out of University control, and/or the media must be destroyed, using current best practices for the type of media." The policy includes links to resources for disposal and destruction.
- **University of Minnesota** Computer Recycling
  UMN's OIT unit provides overall computer recycling through a 3rd party vendor. The data deletion policy places the responsibility for deletion on the party responsible for placing non-public information on a computer, and provides a list of deletion software and techniques.
- **University of Pennsylvania** Computer Recycling and Disposal Options and Guidelines for the Destruction of Confidential Records
  The university's IT and Archive policies and recommendations specify removal of sensitive data from computers before disposal. They also recommend checking software license terms to see if the software must be deleted before transfer. The recommendations include information on removal techniques and vendors.
- **University of Washington**
  University Facilities Services Surplus Property unit purges data from surplus university computers using Department of Defense approved data destruction software following DOD guidelines or by destroying hard drive platters. Departments are expected to practice due diligence by deleting all files prior to surplussing their equipment, especially files which contain confidential data, such as personnel, patient, legal, or student information.

Questions or comments? Contact us.