Electronic Media Disposal/Redistribution Standard

- Standard - SBIT-102
- Status - Adopted August 1, 2010
- Source - IU South Bend University Information Technology Services (UITS)

Scope
This standard applies to all departments and users of Indiana University South Bend data and all information technology electronic computing devices/removable storage media that are either:
a) purchased by the University, or:
b) contains University data, irrespective of computing device/removable storage media ownership.

Rationale
The use of information technologies has become critical in support of most if not all Indiana University operations. This dependence has resulted in a very large, very diverse, and very complex technology environment. At the same time, much more data is being stored, accessed, and manipulated electronically, which has resulted in an increased risk of unauthorized disclosure or modification of personal, proprietary, sensitive, or institutional data. It is very important that everyone associated with providing and using these technology services is diligent in their handling of technology media and executing due diligence to assure data integrity.

Standard Statement
All computing devices which contain hard drives are to be wiped to Department of Defense (DoD) Standard 5220.22-M specifications and verified as fully wiped prior to being reissued, retired, stored as surplus, offered for sale, auction, offered as trade-in fodder or otherwise relinquished from Indiana University South Bend control.
All removable storage media which can electronically store data are to be wiped to Department of Defense (DoD) Standard 5220.22-M specifications or destroyed prior to being reissued, retired, stored as surplus, offered for sale, auction, offered as trade-in fodder or otherwise relinquished from Indiana University South Bend control.

Procedures

University Issued Computing Device with a Hard Drive

1. Once a computing device will be removed from use by the assigned individual, the Information Technology department is to be contacted immediately to take possession of the computer/computing device/external hard drive.
2. Information Technologies will wipe the hard drive with a sanctioned utility that performs an erasure to DoD specifications.
3. A sanctioned utility, such as a hex viewer, will be used to verify that the drive wipe was completed.
4. The identification number from the device and dates of wiping and verification will be logged.

Removable Storage Media
Once removable storage media will be removed from use by the assigned individual, the individual is to wipe the media if the media stored University data at any time.
Note: Removable Storage Media is never be used to store sensitive data.

Damaged Computing Equipment or Removable Storage Media
If a computing device or removable storage media is damaged or is unable to be wiped with a utility, the data on the device/media is to be erased with an electromagnetic degausser of adequate strength to assure efficient erasure.
In the case of CD's or other types of media that can't be electronically erased, the media is to be destroyed to an adequate level to assure that no data is retrievable.

Definitions

Computing Devices
includes all types of computing equipment which runs software and has storage devices, (usually but not limited to hard drives), such as desktop computers, servers, laptops, netbooks, tablets, or the like.

Drive Wiping Utility
is software which overwrites an entire storage device with random binary characters to assure that data originally contained on the storage device is irretrievable.

Hard Drive
is what stores all your data. It houses the hard disk, where all your files and folders are physically located.

Hex Viewer
is software which displays the hexadecimal equivalent of the binary data stored on electronic media.

Removable Storage Media
includes all types of devices which store data, such as flash drives, Optical Discs (CD, Blue-Ray or DVD), MP3 players, Memory cards (CompactFlash card, Secure Digital card, Memory Stick), PDAs, floppy disks, external drives, electromagnetic tape, or the like.

Sanctions
Failure to comply with Indiana University South Bend information technology standards and policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); to the individual's employment (up to and including immediate termination of employment); civil or criminal liability; or any combination of these.

Related Policies, Laws, and Documents

- IT-01 Appropriate Use of Information Technology Resources
- IT-02 Misuse and Abuse of Information Technology Resources
- IT-07 Privacy of Information Technology Resources
- Institutional Purchasing Policies
- SBIT-101 Sensitive Data Storage
- HIPAA Regulations
- PCI-DSS Standards

Campuses, schools, colleges, departments, and other administrative units may have issued local policies and standards governing the appropriate use of information technologies deployed specifically to support that unit's activities. Managers of information technology services may have issued service-level polices and standards governing the appropriate use of their services. In order to understand and adhere to these requirements, users of these resources are responsible for consulting with appropriate unit or service staff.

Consultation:

The IU South Bend Microcomputer Support Team in collaboration with the University Information Security Officer (UISO) are available to provide consultation or advice related to technology use or misuse to any university, campus, or unit administrators or individual personnel.

Standard History

- Approved August 1, 2010
- Updated June 18, 2015