Data Destruction Standard

Purpose

To establish standards for Data Destruction that ensure confidentiality of University data and also protects the Personal Information (PI) and Personal Health Information (PHI) of University staff and students from unintentional data disclosure.

Scope

This standard is intended for use by all University of Manitoba staff involved in the process of Electronic Data Removal and Destruction.

Definitions

Electronic Devices: All electronic equipment that has a storage device or persistent memory. Such devices may include but are not limited to, desktop computers, laptops, servers, personal data assistants, cell phones, printers, copiers, routers, switches, and firewall hardware.

Electronic Media: All media on which electronic data can be stored, including, but not limited to: hard disk drives, magnetic tapes, diskettes, CDs, DVDs, BRDs (Blu-Ray Disks). Solid-state drives including all solid state drives, USB storage devices, and flash based memory cards.

Clear: As per the NIST 800-88 Rev. 1 Guideline, a method of sanitization that 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, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported)

Purge: As per the NIST 800-88 Rev. 1 Guideline, a method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

PART A – Physical Destruction for Media to be Recycled or Disposed

Physical Destruction of Hard Disk Drives

Hard Disk Drives to be recycled or disposed of must be physically destroyed whenever possible, by crushing or shredding the media using the service provided by IST. Destruction services are offered on both the Fort Garry and Bannatyne Campuses. If a unit is offsite and delivery of hard disk drives to either campus is not practical or secure, please follow the appropriate Clear Data from Electronic Media procedures in PART B of the Data Destruction Standard and before shipping/transporting the drives for recycling.

Physical Destruction of Solid State Drives

Solid State Drives to be recycled or disposed of must be physically destroyed whenever possible, by crushing or shredding the media using the service provided by IST Destruction services are offered on both the Fort Garry and Bannatyne Campuses.

If a unit is offsite and delivery of solid state drives to either campus is not practical or secure, please follow the appropriate Clear Data from Electronic Media procedures in PART B of the Data Destruction Standard and then recycle the drives.

If a device containing a solid state drive cannot readily be physically destroyed, follow the appropriate Clear Data procedure before recycling the device (with the media intact). For example, it may be impractical to remove or separate the electronic media from the remainder of the electronic device when the device is a sealed tablet, small laptop or a sealed external drive enclosure.

Recycling or Disposal of all electronic media other than Hard Disk and Solid State Drives

Recycling or Disposal or of all other electronic media must be by destruction. Devices such as magnetic tapes, floppy diskettes, Zip Disks, CDs, DVDs, BRDs and solid state devices, such as USB storage or Flash memory cards must be physically destroyed by degaussing, crushing or shredding, so that the data-containing component is unreadable by standard forensic recovery, before the item is disposed or recycled:

- Magnetic tapes will be degaussed and cut;
- Diskettes, CDs, BRDs will be shredded;
- Solid State Devices such as USB storage or Flash memory cards will be crushed, and Smartphones/Cellular phones will be purged according to vendor standards.

PART B – Clear Data from Electronic Media

Electronic media or devices transferred within the University, donated to an outside organization, returned to vendors at end of lease, or repaired by outside contractor must have data removed according to industry best practices for Clear (minimum) or Purge (preferred).

In the event of a non-functioning device going out for repair, or if it is undesirable or impossible to remove data before sending for repair, contact the IT Security Coordinator for guidance.

Networking Device Sanitization

Clear: Perform a full manufacturer's reset to reset the router or switch back to its factory default settings.

Purge: Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible and that the device does not simply remove the file pointers.

Mobile Devices

Apple iPhone and iPad

Clear/Purge: Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). The sanitization operation may take only minutes if Cryptographic Erase is supported or may take as long as several hours if media-dependent non-cryptographic sanitization techniques that leverage overwriting are applied by the device (depending on the media size).

Blackberry

Clear/Purge: Select the full sanitize option (typically in either the 'Options > Security Options > General Settings > [menu button] > Wipe Handheld' OR in 'Options > Security Options > Security Wipe' menu), making sure to select all subcategories of data types for sanitization. The sanitization operation may take several hours depending on the media size.

Google Android OS Devices

Clear: Select the full sanitize option (typically in the 'Menu > Settings > [Privacy OR SD and Phone Storage]> Factory data reset' menu).

Purge: Android settings and capabilities may be modified by device vendors or service providers, and therefore no assumptions should be made about the level of assurance provided by performing a factory data reset. Some versions of Android support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (and potentially the service provider as well, if applicable) to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible and that the device does not simply remove the file pointers.

Office Equipment Sanitization (includes copy, print, fax, and multifunction machines)

Clear: Perform a full manufacturer's reset to reset the office equipment to its factory default settings.

Purge: Most office equipment only offers capabilities to Clear (and not Purge) the data contents. Office equipment may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible and that the device does not simply remove the file pointers. Office equipment may have removable storage media, and if so, media-dependent sanitization techniques may be applied to the associated storage device.

ATA Hard Drives (PATA, SATA, eSATA, etc…)

Clear: Overwrite media by using an IST approved and validated overwriting tool such as:

DBAN – http://www.dban.org/
(Link to Instructions)

Eraser - http://eraser.heidi.ie/

The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.

Purge: Two options are available:

1. **Apply the ATA Sanitize command**, if supported. One or both of the following options may be available:

a. The overwrite command. Apply one pass of a fixed pattern across the media surface. Some examples of fixed patterns include all 0s or a pseudorandom pattern.

Optionally: Instead of one pass, use three total passes of a pseudorandom pattern, leveraging the invert option so that the second pass is the inverted version of the pattern specified.

b. If the device supports encryption and the requirements described in this document have been satisfied, the Cryptographic-Erase (also known as sanitize crypto-scramble) command.

Optionally: After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase.

2. **Apply the ATA Secure Erase command**. The ATA Sanitize command is preferred to ATA Secure Erase when the ATA Sanitize command is supported by the device.

SCSI Solid State Drives (SSDs) this includes SCSI, SAS, Fiber Channel, etc.

Clear: Overwrite media by using an approved and validated overwriting tool such as:

DBAN – http://www.dban.org/
(Link to Instructions)

Eraser - http://eraser.heidi.ie/

(Check out the others and update)

The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.

Purge: Apply the SCSI Sanitize command, if supported. One or both of the following options may be available:

a. The block erases command.
b. If the device supports encryption, the Cryptographic-Erase (also known as sanitize crypto-scramble) command.

Optionally: After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erases command is not supported, the Clear procedure could alternatively be applied.

References

Use of Computer Facilities Policy and Procedures
http://umanitoba.ca/admin/governance/governing_documents/community/252.html

Access and Privacy Policy and Procedures
http://umanitoba.ca/access_and_privacy/governance.html

Records Management Policy and Procedures
http://umanitoba.ca/access_and_privacy/governance.html

Freedom of Information and Privacy Act - http://www.gov.mb.ca/chc/fippa/
Personal Health Information Act - http://www.gov.mb.ca/health/phia/