Secure Deletion Procedure

Policy Title:
Secure Deletion Procedure

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This procedure applies to any electronic media which is required to be securely deleted because of the type of data it contains. In addition, please note that this policy covers all IoT devices. This procedure covers the process for securely deleting electronic media which either currently contains or previously contained information classified as Loyola Protected data or Loyola Sensitive data, which will be referred to as "covered data" in this procedure.

II. Definitions

Not Applicable.

III. Policy

Hard drives

When a computer with a hard drive containing covered data is replaced, it initially will be stored in accordance with the existing equipment replacement policy. When the hard drive would normally be placed back into circulation, it must first be securely deleted before this happens.

To securely delete a hard drive, an ITS technician will place the hard drive into a computer and boot a copy of an approved whole drive secure deletion tool, as listed in the appendix. The ITS technician will then run the program, performing one complete overwrite.

USB drives

When a USB drive containing covered data needs to be discarded, an ITS technician will attach the USB drive to a computer and run an approved granular secure deletion tool, as listed in the appendix. The ITS technician will then run the program, performing one complete overwrite.

Non-electronic removable media

When any form of media, which is inserted into a desktop drive, containing covered data needs to be discarded, the media must be physically destroyed. This is most easily accomplished by using a pair of scissors to cut the media in half. It is also acceptable to send the media through a shredding device. This does not need to be performed by an ITS technician.

Electronic removable media

Electronic removable media (USB drives, memory cards, etc.), which is inserted into a computer, containing covered data needs to be discarded, the media must be physically destroyed. This is most easily accomplished by crushing or shredding. This does not need to be performed by an ITS technician.

Backup tapes

When a backup tape needs to be discarded, the backup tape must be sent through a degaussing device. Because it is difficult to determine which specific files are on which specific tape, all backup tapes are subject to this policy. If an area has backup tapes but does not have a degaussing device, they can provide the backup tapes to ITS. An ITS technician will then degauss the backup tapes. Once the backup tapes are degaussed, they can be discarded.

Broken devices or media

If a device or piece of media is unable to be read, it must be either degaussed or physically destroyed. If an area is unsure of how to do so, or does not have a degaussing device, they can contact ITS. ITS will pick up the device or piece of media. The ITS technician will then either physically destroy the device or degauss it, depending on which is more appropriate.

PCI Lockbox

PCI lockbox images older than 7 days will automatically be deleted from server storage daily. Results of this job will be logged onto a central logging server in accordance with the Log Management Standard and emailed to appropriate ITS staff members.

Devices containing HIPAA Related Information

Devices containing protected health information as outlined by HIPAA require additional steps to ensure no data can be retrieved from the device. All HIPAA related devices will be erased using an approved whole drive secure deletion tool, as listed in the appendix. The ITS technician will then run the program, performing seven complete overwrites. Any device that cannot be erased in this manner must be physically destroyed.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Secure Deletion Procedure at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- ITS Security Policy

Approval Authority:	ITESC	**Approval Date:**	March 12th, 2008
Review Authority:	Jim Pardonek	**Review Date:**	June 14th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu