Northeastern ILLINOIS UNIVERSITY

University Policy

Volume I1: Information Technology	**I1.02.7** **Electronic Data Erasure** **Interim Policy** **Effective Date:** 06/30/2022 **Last Revised:** mm/dd/yy	**Responsible Office:** University Technology Services
Chapter 02: Data Security		**Responsible Officer:** Information Security Officer

POLICY STATEMENT

The safety of data must always be maintained from the time of creation to disposal. Appropriate disposal of data when it is no longer needed or when it has reached the end of life will protect it against activities that could compromise the confidentiality of its content.

PURPOSE OF THE POLICY

The purpose of this policy is to set out the requirements for maintaining the confidentiality of data on computer devices when the data or the computer device that holds such data is no longer required.

WHO IS AFFECTED BY THIS POLICY

All University employees and third parties who handle and/or manage data on behalf of the University.

DEFINITIONS

Computer Equipment or Device: any device that stores data temporarily or permanently including but not limited to computer hard disks (internal and external disks), CDs/DVDs, USB flash drives, backup tapes, smart cards, tablets, etc.

Data Erasure: Complete purging of data from a computer device.

Equipment Destruction: Physical destruction of a device.

REGULATIONS

5 ILCS 160/1 Illinois State Records Act

Data Erasure for Equipment Transfer or Disposal

- Users must delete data stored on a computer device before it is dropped off or picked up by University Technology Services (UTS) Helpdesk.
- The UTS Helpdesk must ensure that the device is completely purged of any data or applications (for example, the computer is reimaged) before it is transferred to another user.
- The UTS Helpdesk must ensure that the device is completely purged of any data or applications before the device is disposed of following the university's procedure outlined in the section below.

Data Erasure on Removable Devices

- Users must delete data on removable computer devices such as external hard disks, CDs/DVDs, USB flash drives, backup tapes, smart cards, etc. before it is transferred to other users or dispose of. For assistance with this, users can notify University Technology Services Helpdesk to arrange data erasure and/or device disposal.
- Smartphones and tablets that are no longer required, obsolete or damaged must be returned to the UTS Helpdesk. Users must ensure they remove the pincode from these devices and reset them to factory settings before returning them to the UTS Helpdesk.

Data Erasure on Lost or Stolen Devices

- Employees are to notify IT Helpdesk via email after a university device is reported lost or stolen to the police. The email must include:
  - The name of the device owner and department
  - Make of the device
  - Where the device was last seen or used
  - The date the device was lost or stolen
  - What type of information was stored on the device
  - The police report number

- IT Helpdesk should report the incident to Property Control immediately to carry out a search of the device around the university premises to determine if the device can be located.

- Helpdesk must notify the device management vendor as soon as possible to initiate the relevant investigatory process upon receiving a notification of a lost or stolen laptop. If the device cannot be located, the vendor will initiate wiping data off the device when it connects online.

- When the investigation of the lost or stolen device is complete, the status of the device must be updated in the inventory system by Property Control.

Employees must not transfer or dispose of any electronic data or computer device outside of the requirements stated in this policy.

All paper records must be disposed of according to the Record Destruction Process.

Responsibility

- It is the responsibility of the computer device user to delete data from a computer device when it is no longer needed.
- It is the responsibility of Property Control, Facilities and the UTS Helpdesk to ensure that computer devices in their care after receipt, during transportation, or disposal are secured to protect against unauthorized access to the data or applications that may be held on these devices.
- It is the responsibility of the UTS Helpdesk to ensure that data is completely wiped from a computer device before it is transferred to other users or disposed of.

PROCEDURES

- Employees are to back up work data stored on a computer device onto the university's network file storage or Google Drive when the device is no longer needed.
- As a temporary safety measure, employees are to delete data from a computer device before it is dropped off or picked up for transfer or disposal. See the guidelines below for more information on data deletion.
- For a small computer device drop off such as a laptop, contact the UTS Helpdesk at helpdesk@neiu.edu.
- To transport big computer devices or a large number of computer devices to the UTS Helpdesk, contact Property Control at property-control@neiu.edu.
- Upon receiving computer devices:
    - For device transfer, the UTS will reimage the device and maintain a record of the device. The status of a computer device will be updated when the device is transferred to another user.
    - For device disposal, the UTS will crush the hard disks and transfer the computer devices and hard disks to Property Control. The UTS will ensure computer devices and crushed hard disks are labeled appropriately before they are picked up by Property Control.
- Property Control will arrange to dispose and transfer the surplus equipment to the State or recycling service provider.

GUIDELINES

- Equipment storage: Employees are to store equipment pending pick up or drop off in a locked office or drawer.
- Data deletion: In addition to using the Delete function, also use "Empty Trash" to delete files stored in the computer trash area.

Note: Using "Delete", "Empty Trash", or formatting a hard disk will not delete data permanently from the computer. These methods only prevent accessing deleted files easily and directly on the computer, but data can be retrieved using recovery tools. Computer device users are to notify the UTS Helpdesk to erase data from the hard disk before it is repurposed or disposed of.

HISTORY

Updated August 29, 2023 to include property control directives and updated links
Draft created June 2022

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Property Control
Records Retention

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	Email
Office of VP, Finance and Admin	(773) 442-5100	vpfinance-admin@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.