LUTHER COLLEGE

POLICIES AND PROCEDURES

Department:	Information Technology Services and Financial Services
Subject:	Information Safeguarding
Date Issued:	April, 2009
Updated and Reviewed By:	Information Security Council - April 20, 2023
Approved By:	President's Cabinet – September 13, 2023

I. Policy

This policy sets forth the guidelines for information safeguarding required for compliance with 16 Code of Federal Regulations (CFR) Part 314, which stems from the Gramm-Leach-Bliley Act (GLBA).

II. Purpose

The purpose of this policy is to create a system of information security which ensures the security and confidentiality of customer information, protects against any threats to the security or integrity of such information, and guards against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. The information security system set forth in this policy will be maintained in perpetuity through the use of employee training and management, periodic assessment of the risk of a security breach, and regular system updates.

III. Scope

This policy applies to all faculty, staff, volunteers, students, and contracted workers with access to Luther College data or data networks.

IV. Terms and Definitions

- Information Technology – computer-based information systems and the data contained within
- IP Address – a numerical identification assigned to a specific device participating in a computer network
- Physical Records – all material on which information is recorded or preserved, regardless of form or characteristics, which is created or maintained by any agency, officer, or employee of Luther College in the transaction of its business
- Customer Information – any personally identifying information (PII) such as names, addresses, account and credit information, and social security numbers
- FERPA – The Family Educational Rights & Privacy Act of 1974 covers the legal accessibility of confidential student information
- Directory Information – student data that is considered generally available to the public and not kept private by Luther unless a student specifically requests otherwise

- Statement of Responsibility – an agreement to uphold certain requirements for information security and confidentiality signed by all Luther employees, volunteers, students, and contracted workers
- Payment Card Industry Data Security Standards (PCI) - standards and requirements designed to ensure that companies who process, store, or transmit credit card information maintain a secure environment Information Security Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

V. Procedures and Guidelines

A. Information Technology Safeguards

- Network Security
  - Access to Luther networks is password protected
  - A device should have a fully patched operating system and up-to-date anti-malware software to access the Luther network
  - A network firewall ensures that devices are not directly accessible from the Internet
  - Network switches are installed in locked closets
  - Software management access to network switches is restricted to a small number of IP addresses within the Information Technology Services (ITS) department
  - All Network access is protected by a Domain Name Service (DNS) filtering service.
- Server Security
  - Physical Security
    - The server room is always locked. Primary staff access to the server room is through an electronic lock which logs access that is reviewed periodically
    - The server room has no windows
    - All storage media is wiped clean or destroyed prior to disposal in accordance with the college's Electronic Media Disposal Policy
    - The server room door is monitored by a security camera
  - Server Data Backup Security
    - Incremental backups are done daily to the off-site disk based backup system
    - Backups of Virtual Machine (VM) disk images are done daily to the offsite disk based backup system
    - Backups are retained on offsite storage for up to 60 days before being moved to cloud storage for preservation for up to 10 years.
    - Backup media that is no longer needed is physically destroyed so that the data is no longer readable
    - Random restorations of backed up files is conducted on a periodic basis
  - Server Software and Operating System Security
    - Approved security patches are applied to applications and operating systems as they become available
    - Server side firewalls are turned on and configured to allow only necessary access
    - Servers are protected by anti-malware/endpoint protection software. On Windows servers, the anti-malware software is run in lock-down mode which prevents execution of unauthorized executables.
    - Only software necessary for the function of each server should be installed on the server
    - Administrator access to servers requires Multi-factor authentication
  - Remote access to servers

        - Remote Desktop access to Windows servers and secure shell (ssh) access to linux servers for administrators is allowed only via a virtual private network (vpn) connection, and via the wired ITS user network.
- Workstation Security
    - Access to Luther networks is password protected
    - Physical Security
        - All labs and classrooms are locked outside of normal usage hours. Hours vary by building/room.
        - Doors should be locked when offices are empty; computers should be locked when individuals are away from their desks.
        - Hard Disk Drives (HDD) and Solid State Drives (SSD) are wiped in compliance with DoD standards prior to disposal.
        - Workstations in inventory are stored in locked spaces.
    - Data Security
        - The use of network drives and Google Drive is recommended for files that need to be backed up.
        - Faculty/Staff workstations are backed up prior to being re-imaged and the data is retained for over a year. All backups are stored in a locked cabinet.
        - Local accounts operate under standard user rights. Temporary administrator rights can be granted upon request.
        - Remote assistance to workstations requires password and client approval.
        - Employees may not access their workstations remotely.
    - Software and Operating System Security
        - Approved security patches are applied to applications and operating systems as they become available
        - Windows/macOS workstations are protected by anti-malware/endpoint protection
        - All faculty/staff and student employee workstations have their local HDD/SSD encrypted
        - All faculty/staff and student employee workstations have their screens locked after 25 minutes of inactivity
        - Temporary files are cleared via an automated schedule on Windows workstations
        - All workstations have software installed that performs Web/Domain Name Service (DNS) filtering
        - Workstations running unsupported operating systems are not allowed on the internal network
    - User Credential Security
        - All Windows Faculty/Staff workstations have a unique local administrator password that is changed every 30 days.
        - All workstation logins are synced with a user's Active Directory (AD) credentials.
        - AD / Norse Key Password Security
            - Passwords must be changed every 180 days
            - Minimum requirements for new Norse Key passwords:
                - must not be blank
                - must not contain any spaces
                - must not contain these special characters (\ * : , < >)
                - must not be in your password history
                - must be at least 12 characters long
                - must be less than 24 characters long
                - must contain at least one number
                - must contain at least one special character

        - must contain at least one uppercase character

    - All Norse Apps accounts are required to use Google 2-Step verification.
    - Enterprise password manager software is available for all Luther college employees.
- Remote Work Security
    - Employees will review and abide by the "Remote Work Policy" located on the policies page at www.luther.edu/policies.
- PCI Data Security
    - Annual review of campus areas that accept payment card transactions
    - Additional guidance is located in the Payment Card Industry Compliance and Incident Response policy located on the policies page at www.luther.edu/policies.

B. Physical Records Safeguards
- Records to be Transferred
    - The Records Transfer Form is required for all transfers to the Luther College Archives for retention or confidential destruction, per the Records Retention Schedule located at www2.luther.edu/archives/records/schedule. The full Records Management and Confidential Destruction Policy is located on the policies page at www.luther.edu/policies.
- Records to be Destroyed
    - Records containing customer information must be confidentially destroyed according to the Records Retention Schedule created by the Luther College Archivist (See www2.luther.edu/archives/records/schedule)
    - Until records are ready for destruction, they are stored in locked offices or storage facilities
    - Records that have been delivered to archives for destruction but have not yet been destroyed are kept in a locked cage in the library basement
- Records Maintained in Perpetuity
    - Some records that cannot ever be destroyed are maintained by individual departments in locked storage facilities
    - Records containing customer information that the Luther College Archivist maintains in perpetuity are accessible only to appropriate Luther employees

C. Safeguards over the Dissemination of Customer Information
- Luther College controls access to student records in accordance with the regulations set forth by FERPA
    - Luther College will not release student information to anyone other than those prescribed by law, with the following exceptions:
        - The student gives consent for the release of information
        - There is legal compulsion to release the information
        - The immediate security of persons or Luther College property depends on the release of information
    - Students will be informed of their privacy rights with respect to their educational records on an annual basis
    - Student directory information is not considered to be confidential unless specified by a student
    - Students have the right to inspect and review any of their official records
- Statement of Responsibility
    - At the start of a relationship with Luther and every 180 days thereafter, every Luther College employee, volunteer, student, and contracted worker is required to read a

statement of responsibility for the security and confidentiality of data and data networks and agree to:
    - Keep personal passwords private; passwords are not to be written down or shared with others
    - Use Google 2-Step Verification
    - Use Multi-Factor Authentication (MFA)
    - Sign off or lock a workstation when leaving the immediate work area
    - Assume responsibility and be held accountable for all data modifications made using his/her ID and password
    - Not allow unauthorized use of any information in files or databases
    - Not provide or permit access to Luther College data infrastructure or networks by any unauthorized individuals
    - Not seek personal benefit or permit others to benefit personally through the use of any confidential information which has come to him/her through his/her work assignment
    - Not exhibit or divulge the contents of any record or report to any person except in the conduct of his/her regular work assignment
    - Not use any official record or report (or a copy) for purposes other than college business
    - Not operate or request another to operate any Luther College computer equipment for purely personal business
    - Not aid, abet, or act in conspiracy with any person to violate any part of the statement of responsibility
    - Report any violation of the statement of responsibility to his/her supervisor immediately
  - The statement of responsibility for the security and confidentiality of data and data networks also contains the requirements for compliance with FERPA

D. Response to information security incident(s)

- If an information security incident is detected, steps should be followed as outlined in Luther College's Incident Response Plan and corresponding playbooks.

E. Management of information security program

- Employee Training
  - New employees, volunteers, students, and contracted workers are required to read and agree to the statement of responsibility for the security and confidentiality of data and data networks when they set up the password which will give them access to secure information on Luther networks
  - Faculty, staff, volunteers, contracted workers, and student employees with access to Luther College data or data networks are required to complete training as outlined in Luther's Information Security Training Policy located on the policies page at www.luther.edu/policies.
- Program Oversight
  - The Information Security Council will be responsible for the annual review and assessment of Luther College information security policies and practices.

  - Updates to the Information Safeguarding policy that result from the annual review and assessment of information security policies and practices will be reviewed and adopted, as deemed appropriate, by the Information Security Council.