POLICIES AND PROCEDURES

| | |
|---|---|
| Department: | Human Resources and Information Technology Services |
| Subject: | Information Security Training Policy |
| Date Issued: | December 14, 2022 |
| Updated and Review By: | Information Security Council – October 24, 2022 |
| Approved By: | President's Cabinet – December 14, 2022 |

## I. Policy

This policy sets forth the guidelines for information security training required for compliance with 16 Code of Federal Regulations (CFR) Part 314, which stems from the Gramm-Leach-Bliley Act (GLBA), and is in compliance with guidelines set forth by the Luther College Information Security Council.

## II. Purpose

The purpose of this policy is to educate the Luther community on our shared responsibility to help protect the confidentiality, availability, and integrity of Luther College's information assets and to ensure that all employees are trained on relevant rules, regulations, and best practices for cybersecurity.

## III. Scope

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

## IV. Procedures and Guidelines

A. Information Security Training Program

- Information Technology Services (ITS) and Human Resources (HR) will coordinate the campus-wide information security training program which provides appropriate training to Luther employees.
- The information security training program will be updated regularly by ITS and HR to align with organizational policies and procedures, and will:
  - Be built on lessons learned from both established and emerging threats.
  - Ensure that all principles, policies, procedures, and training materials are accessible by Luther employees as appropriate.

B. New Hire Information Security Training

- All newly hired employees must complete an initial information security training course within 30 days of start date.

C. Annual Information Security Training

- All Luther College employees, including student workers who have work study accounts, will be required to complete annual information security training that will:
  - Explain acceptable use of information technology.

    - Inform employees about relevant policies, regulations, and risks to information systems and services that house Luther College data assets.
    - Educate employees on cybersecurity topics, including but not limited to:
        - Malware
        - Information safeguarding
        - Phishing
        - Social engineering
        - Application / operating system vulnerabilities
- Annual training must be completed within 90 days of initial notification.
- Completion rates will be tracked and reported.

D. Additional Training

- Employees with financial or accounting responsibilities may need additional security training as required by cyber liability insurance.
- Additional security training may be required by employees at other intervals.

E. Enforcement

- Failure to comply with this policy may result in loss of access to systems and services.