POLICIES AND PROCEDURES

Department: Financial Services
Subject: Information Safeguarding
Date Issued: April, 2009
Date Revised: July, 2011
Approved By:

I. Policy

This policy sets forth the guidelines for information safeguarding required for compliance with 16 CFR Part 314, which stems from the Gramm-Leach-Bliley Act.

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, 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 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, students, and contracted workers
V. Procedures and Guidelines

A. Information Technology Safeguards
   • Network Security
     o Access to Luther networks is password protected
     o A computer must have a fully patched operating system and up-to-date antivirus software to access a Luther network
     o A network firewall ensures that workstations are not directly accessible by people on the internet
     o Network switches are installed in locked closets
     o Software management access to network switches is restricted to a small number of IP addresses within the Information Technology department
   • Password Security
     o Passwords must be changed every 180 days
     o Passwords must be at least 8 characters with at least one number and at least one letter
   • Physical Security of Servers
     o The door to the room containing all of Luther’s servers is always locked and has hinges that are inaccessible unless the door is open
     o The server room has no windows
     o All storage media is wiped clean prior to disposal
   • Software and Operating System Security
     o Security patches are applied to applications and operating systems as they become available
     o Server side firewalls are turned on and configured to allow only necessary access
   • Data Backup Security
     o Daily and weekly backups are stored in the locked server room for four weeks before they are overwritten
     o Monthly backup tapes are stored in a locked, fireproof safe for one year and then are overwritten.
     o Yearly backup tapes are stored in a locked, fireproof safe for ten years and then are destroyed.
     o Old backup media that is no longer needed is physically destroyed so that the data is no longer readable

B. Physical Records Safeguards
   • Records to be Destroyed
     o Records containing customer information must be confidentially destroyed according to the records retention schedule created by the Luther College Archivist (See Appendix A)
     o Until records are ready for destruction, they are stored in locked offices or storage facilities
     o 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
     o Some records that cannot ever be destroyed are maintained by individual departments in locked storage facilities
     o 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, 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
    - Sign off of a workstation when leaving the immediate work area for an extended period of time
    - 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 attacks, intrusions, or other system failures

- The following steps are to be followed whenever the security of a server is found to be compromised
  - Regain control of the system
    - The compromised system is completely disconnected from the network to ensure that the intruder has no control of the system
  - Perform necessary notifications of the security breach
Network and systems staff will notify the Executive Director of Library Information Services.

The Executive Director of Library Information Services will determine which additional staff members need to be notified and send them notification.

- Analyze the intrusion
  - Determine the level of access the intruder was able to obtain
  - Look for modifications made to system software and configuration files
  - Look for modifications made to data
  - Look for tools and/or data left behind by the intruder
  - Look for programs the intruder may be running on the system
  - Look for jobs the intruder may have scheduled to run at a certain date and time
  - Review log files

- Recover from the intrusion
  - The operating system and software running on the server are completely reinstalled
  - When restoring data, care is taken not to restore anything which could allow unauthorized access
  - The new system is improved to ensure that the previous vulnerability no longer exists
  - Once the system is fully recovered, it is reconnected to the network

E. Management of information security program

- Employee Training
  - New employees, 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.
  - Employees who will be responsible for taking an active role in Luther’s information security system will be trained by their department supervisor.

- Program Oversight
  - The following Luther employees will be responsible for the annual review and assessment of Luther College information security policies and practices:
    - Director of Network & Systems – policies regarding information technology safeguards and the response to an unauthorized intrusion of a Luther server.
    - Director of Software Development – the sections of the statement of responsibility dealing with information technology.
    - College Archivist – policies regarding physical records safeguards.
    - Registrar – policies regarding FERPA compliance.
  - Updates to the comprehensive information security policy that result from the annual review and assessment of information security policies and practices will be enacted by the Grants & Special Projects Accountant.

Appendix A – Record Retention Schedule located at:
https://www.luther.edu/archives/records/schedule/

Appendix B – Luther College Records Transfer Form located at:
https://www.luther.edu/archives/records/recordstransferform/