LUTHER COLLEGE

POLICIES AND PROCEDURES

Department:	The Office for Financial Services
Subject:	Payment Card Industry Compliance and Incident Response
Date Issued:	December 1, 2008
Date Revised:	March 7, 2012; October 11, 2018
Approved By:	

I. Policy

This policy sets forth the guidelines for compliance with Payment Card Industry Data Security Standards (PCI DSS) and incident response in case of a breach of cardholder data on or off campus.

II. Purpose

The purpose is to protect cardholder information from being exposed to unauthorized individuals.

III. Scope

This policy applies to all departments and organizations that process payment card transactions or work with 3rd party processors on or off campus.

IV. Terms and Definitions

- Anti-virus Software - Programs capable of detecting, removing, and protecting against various forms of malicious code or malware, including (but not limited to) viruses, worms, Trojan horses, spyware, and adware.
- Due Diligence - Refers to the care a reasonable person should take before entering into an agreement or transaction with another party. This would include the verification of all information given to a reasonable person by any prospective business associate.
- Encrypted – Information that has been converted into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
- Firewall – Hardware, software, or both that protect resources of one network from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.

V. Procedures and Guidelines

A. Approval for Payment Card Processing.

- Any new system/software that can process payment card information is required to be approved by the Controller **prior** to being purchased.
- Technology changes that affect payment card systems are required to be approved by the Controller **prior** to being implemented.
- Credit Card Terminals are to be approved by the Controller **prior** to being purchased.

- Any agreement with a 3rd party processor for online sales needs to be approved by the Controller **prior** to being entered into. The requesting department will need to show proof of due diligence and provide documentation that the 3rd party processor is PCI compliant.

B. Processing Payment Card Transactions.

- All staff and student workers that will have access to cardholder information will be required to read and electronically accept the Statement of Responsibility semi-annually.
- Computer systems that process payment cards must be behind a firewall.
- Computer systems that process payment cards must use and regularly update antivirus software.
- A unique ID should be assigned to each person with computer access.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Change system passwords at least once every six months.
- Point of Sale computer systems that process payment cards must have the ability to monitor and track access to network resources and cardholder data.
- Manual card swipers or imprinters are not authorized for use.

C. Storing Payment Card Information.

- It is against Luther College Policy to store sensitive card information (full account number, type, expiration date, or track data) on any server, computer, flash drive or database.
- Treat payment card receipts like you would cash.
- Keep payment card data secure and confidential.
- Restrict access to card data to “those who need to know”.
- Documents containing cardholder data should be kept in a secure environment (I.E. safe, locked file cabinet, etc.).

D. Transmission of Payment Card Information.

- Cardholder data must be transmitted securely (I.E. encrypted).
- Email is not an approved way to transmit credit card numbers.
- Fax transmittal is not an approved way to transmit credit card numbers.

E. Preventing and Handling a Payment Card Information Security Breach

- The Office for Financial Services will perform periodic audits of each department that processes payment card transactions or works with 3rd party processors to ensure compliance to PCI DSS.
- The Office for Financial Services and Library and Information Services will complete a Self Assessment Questionnaire and Attestation of Compliance for each Luther merchant account on an annual basis.
- The Office for Financial Services and Library Information Services will be available to assist any department achieve PCI DSS Compliance.
- Report all suspected or known security breaches to Campus Security, the Controller and the Executive Director of Library and Information Services.

F. Destruction of Payment Card Information.

- All media containing cardholder data must be destroyed when no longer needed for business or legal reasons.

- Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed.

VI. Incident Response Policy

A. Incident Identification.

- Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures.
- All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility.
- Some examples of incidents that an employee might recognize in their day to day activities include, but are not limited to:
    - Theft, damage or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
    - Fraud – Inaccurate information within databases, logs, files or paper records.

B. Reporting an Incident.

- Contact Campus Safety and Security at ext. 2111 to report any suspected or actual incidents.
    - Campus Safety and Security should contact the Controller immediately of any suspected or real incident involving cardholder data.
    - Campus Safety and Security should contact the Executive Director of Library and Information Services immediately of any suspected or real incident involving cardholder data.
    - No one should communicate with anyone outside of their supervisor(s) or Campus Safety and Security about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by Campus Safety and Security.
    - Document any information you know while waiting for Campus Safety and Security to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

C. Incident Response.

- Incident response should proceed through the following stages:
    - Identification.
    - Severity classification.
    - Containment.
    - Eradication.
    - Recovery.
    - Communication.
    - Root cause analysis resulting in improvements of security controls.
- Notify applicable card associations.

  - VISA: Notify Visa Fraud Investigations and Incident Management group immediately at (650) 432-2978. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com**.**
  - MASTER CARD: Contact the Bank of the West in Decorah at (563) 382-2991 for specific details on what to do following a compromise.
  - DISCOVER CARD: Contact the Discover Network Incident Response Team at (800) 347-1111 Authorization Code 10. Additional guidance can be found at http://www.discovernetwork.com/fraudsecurity/databreach.html
  - AMERICAN EXPRESS: Contact the American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750/U.S. only, or at (602) 537-3021/International, or email at EIRP@aexp.com.

- Alert all necessary parties. Be sure to notify:

  - Campus Safety and Security at ext. 2111 or (563) 387-2111.
  - Executive Director of Information Technology Services at ext. 1007 or (563) 387-1007.
  - Controller at ext. 1015 or (563) 387-1015.
  - Decorah Police (563) 382-3667.
  - Merchant Bank – Bank of the West (563) 382-2991.
  - FBI (report online if applicable – check with local police) – http://www.fbi.gov/

- Perform an analysis of legal requirements for reporting compromises in every state where clients were affected.
- Collect and protect information associated with the intrusion. In the event that forensic investigation is required Campus Safety and Security will work with legal counsel and Luther College management to identify appropriate forensic specialists.
- Eliminate the intruder's means of access and any related vulnerabilities.
- Research potential risks related to or damage caused by intrusion method used.

D. Root Cause Analysis and Lessons learned

- Not more than one week following the incident, members of Campus Safety and Security will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan.
- Review other security controls to determine their appropriateness for the current risks.
- Update any identified areas in the policy or security control that can be made more effective or efficient.

VII. Confidentiality and Record

Each department is responsible for the safe keeping of all cardholder information and to keep it from being exposed to unauthorized individuals, including any monetary loss suffered by the college due to theft or improper use of payment card numbers and associated information.

VIII. Contacts

Campus Safety and Security (563) 387-2111
Controller, Office for Financial Services: (563) 387-1015
Accounting Manager, Office for Financial Services: (563) 387-1526
Executive Director of Information Technology Services: (563) 387-1007