Linfield College

Credit Card (PCI) Security Policy

Revised:

Approved: 4/18/2018

Overview

This policy has been created to assist employees in understanding the importance of protecting cardholder data and informing employees about the rules surrounding safeguarding information. The Payment Card Industry (PCI) was formed by the five major card brands (Visa, MasterCard, American Express, Discover and JBC International). This group established a standard set for guidelines around the handling of cardholder data by merchants. These guidelines make up the Payment Card Industry Data Security Standard (PCI DSS) and provide merchants with rules of physical, application and network security, as well as security policy management, which merchants are required to implement and follow. Merchant account holders who fail to comply are subject to fines, any additional monetary cost associated with remediation, assessment, forensic analysis or legal fees and suspension of merchant account(s).

Purpose of Policy

Linfield College handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the institution.

Linfield College commits to respecting the privacy of all its customers and to protecting any customer data from outside parties. To this end, the College will maintain a secure environment in which to process cardholder information so that we can meet these promises.

Scope

All employees or other designated individuals who collect maintain or have access to credit card information or credit card terminals must comply with the PCI policy. Others who do not have access but accidently gain access must immediately report that information to his or her supervisor immediately.

Policy

Protect Stored Data:

1. All third party vendors (see Appendix C) approved to collect payments on behalf of the College must provide a PCIDSS Certificate of Compliance.
2. All sensitive cardholder data stored and handled by Linfield College and its employees must be securely protected against unauthorized use at all times. Any sensitive card data that is no longer required by Linfield College for business reasons must be discarded in a secure and irrecoverable manner.
3. If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.

4. PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger, etc.
5. It is strictly prohibited to store:
   - The contents of the payment card magnetic stripe (track data) on any media whatsoever.
   - The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
   - The PIN or the encrypted PIN Block under any circumstance.

Access to the Sensitive cardholder Data:

1. All Access to sensitive cardholder data should be controlled and authorized. Any job functions that require access to cardholder data should be clearly defined.
2. Any display of the cardholder data should be restricted at a minimum to the first 6 and the last 4 digits of the cardholder data.
3. Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
4. No other employees should have access to this confidential data unless they have a genuine business need.
5. If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained by the Controller's Office as detailed in Appendix C.
6. Service Providers with access to cardholder data will acknowledge in a written agreement that they are responsible for any cardholder data they possess. This agreement will be maintained by the Controller's Office.

Physical Security:

1. Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data. Media is defined as any printed or handwritten paper, received faxes, back-up tapes, computer hard drive, etc.
2. Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
3. Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
4. A list of devices that accept payment card data should be maintained by the Controller's Office. (See Appendix B)
   - The list should include make, model and location of the device.
   - The list should have the serial number or a unique identifier of the device
   - The list should be updated when devices are added, removed or relocated
5. The Controller's Office will coordinate the inspection of POS devices surfaces semi-annually to detect tampering or substitution.
6. Personnel using the devices should be trained and aware of handling the POS devices.

7. Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
8. Personnel using the devices should be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel.
9. The external or internal distribution of any media containing cardholder data and must be approved by the Controller.
10. All computer that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorized use.

Network Security:

1. A high-level network diagram of the network is maintained by the ITS Department and reviewed on a yearly basis.
2. The network diagram provides a high-level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE.
3. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable should also be illustrated.
4. A network scan should be performed and completed by a PCI SSC Approved Scanning Vendor, where applicable. Evidence of these scans should be maintained by the ITS Department for a period of 18 months.

Protect Data in Transit:

1. All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.
2. Cardholder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
3. If there is a business justification to send cardholder data via email or by any other mode then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, etc.).
4. The transportation of media containing sensitive cardholder data to another location must be authorized by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

Disposal of Stored Data:

1. All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. The Controller's Office will perform a semi-annual review to confirm that all non-electronic cardholder data is being appropriately disposed of in a timely manner.

2. Linfield College will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials be crosscut shredded, incinerated or pulped so they cannot be reconstructed.

3. The Data Governance Team Linfield College will maintain documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
    - All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

Security Awareness and Procedures:

1. The policies and procedures outlined in this policy must be incorporated into College practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.
    - Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day practice.
    - Distribute this security policy document to all College employees. It is required that all employees that handle cardholder data must confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
2. All employees that handle sensitive cardholder information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they are allowed to work with cardholder data. It is the responsibility of each department to insure that any employee being assigned to handle cardholder data has had a background check.
3. All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
4. College security policies will be reviewed annually by the Information Security Governance Team.

Credit Card (PCI) Security Incident Response Plan:

1. All employees are responsible to report any incident of theft, damage, fraud, etc. If you believe that an incident has occurred, please notify your immediate supervisor, College Public Safety and the Controller. If you are unable to contact the Controller, you may notify the Vice President for Finance and Administration. Any questions to this policy may be addressed to the Controller.
2. In response to a systems compromise, the following steps will be taken:
    - Ensure compromised system/s is isolated on/from the network.
    - Gather, review and analyze the logs and related information from various central and local safeguards and security controls
    - Conduct appropriate forensic analysis of compromised system.
    - Contact internal and external departments and entities as appropriate.
    - Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.

   - Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.
3. The credit card companies have individually specific requirements that must address in reporting suspected or confirmed breaches of cardholder data. See Appendix D for these requirements. This requirement will be reviewed annually by the Controller's Office.

Transfer of Sensitive Information

1. All third-party companies that have access to cardholder information must adhere to the PCI DSS security requirements and
   - Acknowledge their responsibility for securing the cardholder data.
   - Acknowledge that the cardholder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
   - Provide full cooperation and access to conduct a thorough security review after a security intrusion by a Payment Card industry representative, or a Payment Card industry approved third party.

Policy Compliance

Linfield College will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and community feedback to the policy owner. This policy will be reviewed annually by the Controller's Office and the Chief Technology Officer.

All users must comply with the College's policies. When a member of the College community is found to be in violation of this policy, the College's disciplinary process will be followed. If the matter involves illegal action, law enforcement agencies may also become involved, as would occur for matters that do not involve information technologies or the Internet.

Approved by:

MDRodriquez Date: 5-1-18

Mary Ann Rodriguez
VP for Finance and Administration

Appendix A – Agreement to Comply Form

Linfield College Credit Card Payment Acceptance Guidelines

The purpose of this document is to describe the responsibilities inherent with the collection, processing, storage, or dissemination of credit card data while using the wireless credit card terminal.

- Cardholder information must **not** be accepted through an e-mail. If an e-mail is received, do not process the payment. A reply should be sent to the sender letting them know that their payment cannot be processed via e-mail and give them instructions on the proper procedures for submitting the information; however, the reply e-mail should not include the cardholder information. The Information Technology Services (ITS) Help Line should be contacted for assistance in deleting the original e-mail.
- No cardholder information is allowed to be stored electronically on any device (e.g. computer hard drives, CDs, disks, smart phones and other external storage media).
- The PIN and CVV2 or card verification code (on the back of the card) is NEVER allowed to be stored.
- Access to cardholder information must be limited to those individuals whose job requires access.
- Any media, including paper copies that contain cardholder information, must be treated as confidential.
- Any paper copies of cardholder information & the terminal must be securely stored in a locked location when not in use.
- Do not publicly display cardholder information or leave it unattended and do not disclose cardholder information to others.
- When paper copies of cardholder information are no longer necessary, they must be shredded using a crosscut shredder.
- **Employees and students handling cardholder information must complete terminal training, PCI compliance training and must acknowledge understanding of these Linfield College Credit Card Processing Guidelines**

I, ___________________________________ have read, acknowledge and agree to the Credit Card Processing Guidelines.

____ Date: __________________________

(Signature)

Appendix B – List of Devices

Asset/Device Name	Description	Owner/Approved User	Location

Appendix C - List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date

Appendix D – Credit Card Companies Incident Response Requirements

VISA Steps:

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level(High, Medium, Low)
   c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures
   a. Include forensic tools used during investigation

V. Findings
   a. Number of accounts at risk, identify those stores and compromised
   b. Type of account information at risk
   c. Identify ALL systems analyzed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)
   d. Identify ALL compromised systems. Include the following:
      - DNS names
      - IP addresses

- OS version
- Function of System(s)

e. Timeframe of compromise
f. Any data exported by intruder
g. Establish how and source of compromise
h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

- Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
- Distribute the account number data to its respective issuers.

- Employees of Linfield College will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within Linfield College and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers
4. Obtain additional specific requirements from Discover Card

American Express Steps

1. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
3. Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express