PCI Information Security Policy

Policy Number: ECOMM-P-002
Version Number: 1.0
Classification: Business, Finance, and Technology
Responsible University Office: E-Commerce Committee

Effective Date: December, 14, 2016
Date Last Reviewed: December, 19, 2017
Date of Next Review: December, 19, 2018

Table of Contents

Purpose

The primary purpose of this policy is to establish rules to ensure the protection of confidential or sensitive information and to ensure protection of Elon University's information technology resources.

The policy assigns responsibility and provides guidelines to protect Elon University's systems and data against misuse or loss.

Scope

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorized to connect to Elon University's data network. It may apply to users of information services operated or administered by Elon University (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with Elon University are subject to these same definitions and rules when they are using Elon University's information technology resources.

This security policy has been written to specifically address the security of data used by the Payment Card Industry. Credit card data stored, processed or transmitted with Elon University's Merchant ID must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS).

Definitions

Cardholder Data - The Primary Account Number (PAN), Card Validation Code (CVC, CVV2, and CVC2), Credit Card PIN, and any form of magnetic stripe data from the card (Track 1, Track 2).

CVV- Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features.

PAN- Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

PCI- Acronym for "Payment Card Industry."

PCI DSS- Acronym for "Payment Card Industry Data Security Standard."

Payment Cards- For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard, or Visa, Inc.

Policy- Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures

Procedure- Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.

Protocol- Agreed-upon method of communication used within networks. Specification describing rules and procedures that computer products should follow to perform activities on a network.

Policy Statement

Do Not Use Vendor Supplied Defaults for System Passwords and other Security Parameters

System components used in sensitive networks often will come with default vendor settings (usernames, passwords, configuration settings, etc.). Elon University's general policy is to always change

vendor-supplied defaults for system passwords or other security parameters before systems are installed in the secure network environment (cardholder data network).

Individuals with malicious intent (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Change Vendor Supplied Defaults

- All vendor-supplied defaults must be changed on all system components before being used in the cardholder data network. (e.g., passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts, etc.). (PCI DSS Requirement 2.1, 2.2.d)
- All unnecessary default accounts must be removed or disabled before installing a system on the cardholder data network (PCI DSS Requirement 2.1.b)

Implement Strong Access Control Measures

Access to system components and software within the sensitive data environment (cardholder data network) must be controlled and restricted to those with a business need for that access. This is achieved through the use of active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

Protect Stored Cardholder Data

Paper documents containing cardholder data (e.g., PAN and sensitive authentication data) must be protected when stored.

Protect Stored Data

Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc.

The following policies address the treatment of credit card data.

Retention and Disposal of *Sensitive Credit Card Account Data*

- Create Elon University data storage standards and procedures[1]. This document must detail how and where hardcopies of documents containing sensitive cardholder data are allowed to be stored within the organization. For each storage location, the document must define how long data is allowed to be kept (retention period) and contain a justification for its storage. (PCI DSS Requirement 3.1).
- Elon University data storage standards and procedures must document any legal, regulatory, or business requirements for cardholder data retention. (PCI DSS Requirement 3.1)

[1] See the *Data Retention and Storage Procedures* document.

- All cardholder data older than the stated retention period(s) must be removed from storage locations. Document all data storage locations and see that they are covered under the data disposal requirements. (PCI DSS Requirement 3.1)
- A scheduled procedural process must be conducted at least quarterly to identify and remove cardholder data that exceeds retention requirements. (PCI DSS Requirement 3.1)

Storage of Sensitive Credit Card Authentication Data

- Never store the Card Validation Code (CVC) data (3 or 4-digit number located on the back or front of the credit card) in any paper document after any type of card authorization event. (PCI DSS Requirement 3.2.2).

Security Policies and Operational Procedures Documentation

- Ensure that security policies and operational procedures for protecting stored cardholder data is documented, in use, and known to all affected parties. (PCI DSS Requirement 3.7)

Implement Strong Access Control Measures

Access to system components and software within the sensitive data environment (cardholder data network) must be controlled and restricted to those with a business need for that access. This is achieved through the use of active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

Identify and Authenticate Access to System Components

It is critical to assign a unique identification (ID) to each person with access to critical systems or software. This ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Restrict Physical Access to Cardholder Data

Any physical access to hardcopies containing cardholder data should be appropriately restricted.

Physically Secure All Media

- Elon University will define specific procedures[2] to physically secure all paper documents, including but not limited to paper receipts, paper reports and faxes that contain cardholder data. (PCI DSS Requirement 9.5)

Media Destruction Policies and Procedures

- Media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. (PCI DSS Requirement 9.8)
- It is the policy of Elon University that cardholder data that has been processed must be properly destroyed. Techniques for data destruction vary depending on type of media and are defined as follows: (PCI-DSS Requirement 9.8.1.a)
    - Hardcopy media (faxes, printed documents and reports, etc.) must be cross-cut shredded, pulped, or incinerated according to industry-accepted standards.

[2] See the *Physical Security Procedures* document.

    - If electronic cardholder data is discovered, it must be destroyed using an industry-accepted secure wipe program.

- If applicable, all containers used to store media containing cardholder data to be destroyed must be locked and in a secure area at all times. Such containers are only to be given to authorized personnel or third parties for the purpose of destruction. (PCI DSS Requirement 9.8.1.b)

Protection from Tampering and Substitution

- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. (PCI DSS Requirement 9.9)
- Maintain an up to date list of devices including the following: (PCI DSS Requirement 9.9.1)
    - Make and model of the device.
    - Location of the device.
    - Device serial number or other method of unique identification.
- Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been replaced with a fraudulent device). (PCI DSS Requirement 9.9.2)
- Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI DSS Requirement 9.9.3)
    - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
    - Do not install, replace, or return devices without verification.
    - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
    - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

Security Policies and Operational Procedures Documentation

- Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. (PCI DSS Requirement 9.10)

Maintain a PCI Information Security Policy

Without strong security policies and procedures, many of the layers of security controls become ineffective at preventing data breach. Unless consistent policy and practices are adopted and followed at all times, security controls break down due to inattention and poor maintenance. The following documentation policies address maintaining the Elon University security policies described in this document.

Maintain a Security Policy that Addresses PCI Information Security for All Personnel

A strong security policy sets the security tone for Elon University and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it.

> **Note:** "Employees" refers to full-time and part-time employees; student employees; temporary personnel; contractors and consultants; or anyone who is acting on behalf of the university who are "resident" on the University's site.

Publish, Distribute, and Update the Information Security Policy

- Elon University requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI DSS Requirement 12.1)
- The Elon University information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. (PCI DSS Requirement 12.1.1)

Assign Information Security Responsibilities and Train Employees

- The Elon University's information security policy and procedures apply to all employees (full, part-time, or work study employees), contractors, and individuals providing services for Elon University and could affect security of cardholder information. (PCI DSS Requirement 12.4)

Assign Information Security Management

- The overall responsibility of information security at *Elon University* falls under the office of Information Security Director. (PCI DSS Requirement 12.5)

- Specifically, the following responsibilities must be assigned: (see form in Appendix A)
    - Establish detailed documentation of security incident response and escalation procedures and formally assign the responsibility of creating and distributing these procedures to a specific role, position, or team. (PCI DSS Requirement 12.5.3)

Security Awareness Program

- A formal security awareness program[3] must exist and participation is required for all employees working within the cardholder data environment. (PCI DSS Requirement 12.6.a)

Policies for Sharing Data with Service Providers

In order to conform to industry best practices, it is required that due diligence be performed before engaging with new service providers and is monitored for current service providers that store, process, or transmit cardholder data on Elon University's behalf. Service providers, which could affect the security of sensitive cardholder data, are also in-scope of this policy. Specific procedures for the following policies can be found in the above referenced PCI Service Provider Compliance Validation Procedures document in table 1.

---

[3] See the *Security Awareness Training Process* document.

- Elon University shall maintain a documented list[4] of all applicable service providers in use. (PCI DSS Requirement 12.8.1)
- A written agreement with all applicable service providers is required and must include an acknowledgement of the service providers' responsibility for securing all cardholder data they receive from or on behalf of Elon University, or to the extent that they could affect the security of a cardholder data environment (PCI DSS Requirement 12.8.2). In addition, the service provider must agree to provide compliance validation evidence on an annual basis. (PCI DSS Requirement 12.8.4). Prior to engaging with an applicable service provider, a thorough due diligence process[5] should be followed. (PCI DSS Requirement 12.8.3)
- Elon University shall annually review evidence provided by applicable service providers demonstrating their continuing PCI DSS compliance. (PCI DSS Requirement 12.8.4)
- Elon University shall maintain a list[6] of which PCI DSS requirements are managed by each service provider, and which are managed by Elon University. (PCI DSS Requirement 12.8.5)

Incident Response Plan Policies

Incidents or suspected incidents regarding the security of the cardholder data network or cardholder data itself must be handled quickly and in a controlled, coordinated and specific manner. An incident response plan (IRP) must be developed and followed in the event of a breach or suspected breach. The following policies specifically address the Elon University IRP[7]:

- Elon University must maintain a documented IRP and be prepared to respond immediately to a system breach. (PCI DSS Requirement 12.10)
- The IRP must clearly define roles and responsibilities for response team members. (PCI DSS Requirement 12.10.1)
- The IRP must define communication strategies to be used in the event of a compromise including notification of payment brands. (PCI DSS Requirement 12.10.1)
- The IRP must define specific incident response procedures to be followed. (PCI DSS Requirement 12.10.1)
- The IRP must document business recovery and continuity procedures. (PCI DSS Requirement 12.10.1)
- The IRP must detail all data back-up processes. (PCI DSS Requirement 12.10.1)
- The IRP must contain an analysis of all legal requirements for reporting compromises of sensitive data (for example, California Bill 1386 which requires notification of affected

[4] See the *Service Provider Compliance Validation Process* document.

[5] See the *Service Provider Compliance Validation Process* document.

[6] See the *Service Provider Compliance Validation Process* document.

[7] See the *Incident Response Plan* document.

consumers in the event of an actual or suspected compromise of California resident's data). (PCI DSS Requirement 12.10.1)

- The IRP must address coverage and responses for all critical system components. (PCI DSS Requirement 12.10.1)
- The IRP must include or reference the specific incident response procedures from the payment brands. (PCI DSS Requirement 12.10.1)

References

Internal

Policies

Elon University E-Commerce Committee Policy

Procedures

- PCI Data Retention and Storage Procedures
- PCI Physical Security Procedures
- PCI Security Awareness Training Process
- PCI Service Provider Compliance Validation Process
- PCI Incident Response Plan

Appendix A – Management Roles and Responsibilities

Assignment of Management Roles and Responsibilities for Security

As required by policy in Section 12.5 of this security policy, the following table contains the assignment of management roles for security processes.

Table A1 - Management Security Responsibilities

Name of Role, Group, or Department	Date Assigned	Description of Responsibility
Elon E-Commerce Committee		Establish, document, and distribute security policies
Elon E-Commerce Committee		Monitor, analyze, and distribute security alerts and information
Elon E-Commerce Committee		Establish, document, and distribute security incident response and escalation policies
N/A		Administration of user accounts on systems in the cardholder data network*
Elon E-Commerce Committee		Monitor and control all access to cardholder data

*Elon University does not use a separate cardholder data network.

Appendix B – Agreement to Comply

Agreement to Comply with PCI Information Security Policies

All employees working with cardholder data must submit a signed paper copy of this form. Elon University management will not accept modifications to the terms and conditions of this agreement.

_____

Employee's Printed Name

_____

Employee's Department

_____

Employee's Telephone Number

_____

Employee's Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that Elon University internal information, or information that has been entrusted to Elon University by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with Elon University, I agree to return to Elon University all information to which I have had access as a result of my position with Elon University. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal Elon University manager who is the designated information owner.

I have access to a copy of the Elon University Information Security Policies Manual, I have read and understand the manual, and I understand how it affects my job. As a condition of continued employment at Elon University, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from Elon University.

I agree to choose a difficult-to-guess password as described in the Elon University Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to Information Security Director at security@elon.edu.

_____ _____

Employee's Signature Date