Policy 5.19
Payment Card Information Security Policy

Responsible Official:  Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship
Administering Division/Department:  Payment Card (PCI) Policies
Effective Date:  April 29, 2015
Last Revision:  July 17, 2017

Policy Sections:

I. Overview
II. Applicability
III. Policy Details
IV. Definitions
V. Related Links
VI. Revision History

Overview

This policy establishes information security requirements and guidelines for technologies and individuals involved in the storage, processing, and/or transmission of credit/debit cardholder data.

Applicability

This policy applies to all people, processes, and technology involved with the storage, processing, or transmission of credit/debit cardholder data, including those that may not be directly involved in processing cardholder data but still have a potential to impact the security of the cardholder data environment.

Policy Details

General Requirements

- Due to Emory’s contractual agreement with our acquiring bank, all credit/debit payment card processing at Emory must be conducted in a manner that fully complies with the requirements set forth in the Payment Card Industry Data Security Requirements (PCI DSS). The current version of the requirements can be found here [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org) Although all merchants are required to adhere to every PCI DSS requirement, some merchants with specific business models may find that some of the requirements do not apply.

Technology Usage Requirements

- Remote access to cardholder data and/or the cardholder data environment must utilize Emory’s multi-factor authentication technology. Any users who access the cardholder data environment are required to use multi-factor authentication including but not limited to administrators, end users, and Emory approved vendors.
- Only technologies explicitly authorized by Emory’s Associate Vice President for Treasury and Debt Management may be used for payment card processing activities. Utilization of unauthorized technologies is prohibited. Examples of prohibited technologies include but are not limited to the following: all end user messaging technologies such as email (including Emory Exchange) and/or instant messaging technologies (including Lync), web based file sharing / collaboration tools (including Emory Box), wireless networks (including Emory Unplugged and EHC), wired networks (other than Emory’s PCI and PCI DMZ networks), and personally owned devices (laptops, tablets, smartphones, etc.)
- All technologies used for payment card processing must be Emory owned / Emory managed devices.
All technologies used for payment card processing must reside within an approved PCI network zone (e.g. PCI zone, PCI DMZ), unless that technology utilizes and Emory approved point to point or end to end encryption technology.

All technologies used for payment card processing must require user authentication (e.g. user ID and password, token, or other authentication mechanism)

Only devices that have been explicitly authorized and inventoried may be utilized for payment processing.

Individuals are prohibited from copying, moving, and/or storing cardholder data on local hard drives or removable electronic media, unless explicitly authorized for a defined business need by Emory’s Associate Vice President for Treasury and Debt Management. Any authorized storage of cardholder data on local hard drives or removable electronic media must be conducted in a manner that fully complies with the data protection requirements contained within the Payment Card Industry Data Security Standard.

Remote access technologies and/or access methods (e.g. user accounts and passwords) utilized by Emory approved vendors and business partners to access cardholder data or the cardholder data environment must only be activated when explicitly needed and must be immediately deactivated after use.

All non-console administrative access to the cardholder data environment must utilize Emory’s multi-factor authentication technology. This does not include access to the system at a locally accessed console session.

Personnel Security Responsibilities

Merchant Business Owners are responsible for the following within their respective areas of responsibility:

- Ensuring ongoing compliance with Emory Policies related to payment processing
- Ensuring ongoing compliance with the Payment Card Industry Data Security Standard
- Creation and management of remediation plans to address any compliance gaps
- Developing daily operational security procedures that are consistent with the aforementioned policies (for example, user account maintenance procedures, log review procedures, etc.)
- Creating and assigning defined roles and responsibilities for all personnel who have access to cardholder data and the cardholder data environment
- Ensuring the prompt removal of user access privileges for all users who have been terminated or who’s job duties no longer require access to cardholder data and/or the cardholder data environment
- Creating and maintaining an accurate and up-to-date inventory of all devices involved in payment card processing activities
- Ensuring the prompt remediation of identified vulnerabilities within prescribed timelines
- Ensuring the full and accurate completion of all required annual PCI DSS assessment activities (e.g. inventories, environmental surveys, self-assessment questionnaires, remediation, etc.)
- Administration of user access to payment card processing systems and applications, including the addition, deletion, and modification of user access privileges
- Ensuring that employees understand their roles and responsibilities and have been properly trained on departmental business processes for handling cardholder data.
- Ensuring that employees are trained upon hire and at least annually using the approved PCI security awareness training
- Monitoring and controlling all access to cardholder data in any form

The Office of Treasury and Debt Management is responsible for:

- Authorizing the use of specific technologies for use in payment processing activities at Emory
- Defining responsibilities related to payment card processing for various Emory constituents
- Initiating and overseeing an annual PCI DSS self-assessment for all Emory merchants
- Providing annual security awareness and training
- Ensuring that all merchant business owners are aware of Emory’s PCI Policies and Procedures Manual and that all personnel acknowledge in writing that they have reviewed the Emory PCI Policies and Procedures Manual

LITS Enterprise Security Personnel are responsible for:

- Enterprise threat monitoring, including the monitoring of security alerts and the communication of information regarding threats to appropriate IT and/or business unit management personnel
- Coordinating and managing required vulnerability assessment activities for the Enterprise and for systems involved in payment card processing
- Assisting and supporting the Office of Treasury and Debt Management in the completion of technical portions of the annual PCI self-assessment
- Making the final determination as to which PCI requirements apply to individual merchants

Emory’s Chief Information Security Officer is responsible for:

- Establishing, publishing, communicating, and maintaining Information Security Policies for payment card processing
- Establishing, publishing, communicating, and maintaining security incident response and escalation policies and procedures

Sanctions:
Failure to comply with this policy may have legal consequences and may result in:

- Suspension or termination of access;
- Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

Definitions

**Cardholder Data** - At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

**Cardholder Data Environment (CDE)** - The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.

Related Links

- Current Version of This Policy: [http://policies.emory.edu/5.19](http://policies.emory.edu/5.19)
- Enterprise Information Security Incident Response Policy ([https://policies.emory.edu/5.17](https://policies.emory.edu/5.17))
- Cardholder Data Environment Remote Access Policy ([https://policies.emory.edu/5.18](https://policies.emory.edu/5.18))
- PCI Risk Assessment Policy ([https://policies.emory.edu/5.20](https://policies.emory.edu/5.20))
- Payment Card Processing and Compliance Policy ([https://policies.emory.edu/2.2](https://policies.emory.edu/2.2))
- Retention and Disposal ([http://records.emory.edu/retention-schedules/index.html](http://records.emory.edu/retention-schedules/index.html))

Revision History

- Version Published on: May 15, 2015 *(Updated to align with PCI DSS v3.2 requirements)*
- Version Published on: May 15, 2015 *(Original Publication)*

*Emory University policies are subject to change at any time. If you are reading this policy in paper or PDF format, you are strongly encouraged to visit policies.emory.edu to ensure that you are relying on the current version.*