Policy 5.19
Payment Card Information Security Policy

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

- 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. 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

- 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).

- 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 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.

### 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 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 proscribed 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

- 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

**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

- Makes 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 Emory’s Payment Card Information Security Policy may result in:

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

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

Revision History

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.