Policy 2.2
Payment Card Processing and PCI Compliance Policy

Responsible Official: Vice President for Finance/Chief Finance Officer
Administering Division/Department: Treasury Operations
Effective Date: January 28, 2013
Last Revision: December 14, 2015

Policy Sections:

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

Overview

Emory University and Emory Healthcare, hereinafter referred to as “Emory”, have a fiduciary responsibility to their customers and payment card processors to comply with the Payment Card Industry Data Security Standard (PCI DSS) when handling payment card transactions. Non-compliance can result in serious consequences for Emory, including reputational damage, loss of customers, litigation, and financial costs. The objective of this policy is to:

- ensure compliance with PCI DSS and other applicable policies and standards,
- establish the governance structure for payment card processing and compliance activities at Emory,
- define responsibilities for payment card services to various Emory constituents, and
- provide general guidelines regarding the handling of cardholder data.

Applicability

This policy applies to all University and Healthcare departments & employees as well as non-employees acting as agents of Emory who handle or support the handling of cardholder data.

Policy Details

a. Background Information

In an effort to enhance the security of payment card data, the credit card industry has formed a council called the Payment Card Industry Security Standards Council comprised of the five

founding global payment brands: Visa Inc., MasterCard Worldwide, American Express, Discover Financial Services, and JCB International. The Council has developed the PCI Data Security Standard (PCI DSS), an actionable framework for developing a robust payment card data security process which includes prevention, detection and appropriate reaction to security incidents. This standard is mandated by the industry in order for a merchant to accept credit/debit card payments, and failure to abide by it may result in reputation risk as well as financial penalties.

Emory accepts credit/debit card payments as a convenience to its customers. To protect our customers' payment card information, Emory's reputation, and to reduce the financial risk or impact associated with a breach of payment card information, this policy addresses Emory's responsibilities to abide by PCI DSS and other applicable policies and standards.

In order for a department, or any other entity at Emory, to process credit/debit card transactions, it must be established as a merchant. Departments may accept VISA, MasterCard, Discover, American Express, and debit cards with a VISA or MasterCard logo. All merchants at Emory are required to use First Data Merchant Services to process credit/debit card transactions, with an exception for The Emory Clinic which uses Sage Payment Solutions.

b. Authority and Delegation

The University Vice President for Finance/Chief Financial Officer has overall authority to ensure PCI DSS compliance for Emory University and Emory Healthcare. The University Vice President for Finance/Chief Financial Officer has delegated authority to the Associate Vice President for Treasury and Debt Management to define responsibilities for payment card services and modify this policy as necessary, provided that all modifications are consistent with PCI DSS then in effect.

c. Applicable Policies and Standards

In addition to the directives and procedures set forth in this policy, any employee, contractor, or agent who, in the course of doing business on behalf of Emory, is involved in the handling of credit card payments must adhere to the following applicable policies and standards:

Emory Policy 5.1 – Information Technology Conditions of Use

"Computers, networks, and software applications are powerful tools that can facilitate Emory's core missions in teaching, learning, research, and service. Access and utilization of these tools is a privilege to which all University faculty, staff, students, and authorized guests are entitled. This policy documents the responsibilities that accompany this privilege. Campuses, schools, colleges, departments, and other administrative units have considerable latitude in developing complementary information technology conditions of use policies, as long as they are consistent with this Emory policy and any other applicable policies of the University. Such policies may be more restrictive than the Emory policy, but must not be more permissive."

Payment Card Industry Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. It consists of common sense steps that mirror security best practices. Below is a high-level overview of PCI DSS. The complete standard is accessible at the web address listed in Related Links below.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks. _

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs.

Requirement 6: Develop and maintain secure systems and applications._

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data. _

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes. _

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

Credit Card Brand Standards

Each card brand has its own program for compliance validation levels and enforcement. Departmental merchants should be familiar with all of the individual credit card brand standards (American Express, Discover Financial Services, MasterCard Worldwide, and Visa Inc.) and refer to them periodically. More information about compliance with specific credit card brands can be found at the web addresses listed in Related Links below.

d. Core Responsibilities

The University Vice President for Finance/Chief Financial Officer has overall authority to ensure PCI DSS compliance for Emory University and Emory Healthcare. The University Vice President for Finance/Chief Financial Officer has delegated authority to the Associate Vice President for Treasury and Debt Management to define responsibilities for payment card services to various Emory constituents. Core responsibilities for each constituent are listed below.

- The Office of Treasury and Debt Management is responsible for initiating and overseeing an annual PCI DSS self-assessment, making appropriate revisions to this policy as needed and coordinating any remediation activities as required by PCI DSS or other applicable policies and standards. The annual self-assessment will include oversight by the Ways and Means Committee and the Enterprise Risk Management Program, in coordination with Emory Healthcare and Library and Information Technology Services (LITS). Other responsibilities include providing annual security awareness & training programs and contracting with third-party credit card processing vendors and service providers.

- LITS Enterprise Security is responsible for maintaining and disseminating security policies and procedures that address PCI DSS requirements, testing Emory's infrastructure and network environment, and assisting the Office of Treasury and Debt Management in completing the technical sections of the annual PCI DSS self-assessment.

- The University Treasury Operations Office is responsible for initial setup and ongoing administration of all University and Emory Hospital merchant accounts. Key responsibilities

include approval of merchant applications, procurement of credit card terminals and other equipment, and operations liaison to Emory's third-party credit card processing vendor, First Data.

• The Emory Clinic Finance Office is responsible for initial setup and ongoing administration of all Emory Clinic merchant accounts. Key responsibilities include approval of merchant applications, procurement of credit card terminals and other equipment, and operations liaison to The Emory Clinic's third-party credit card processing vendors, First Data and Sage Payment Solutions.

• Local IT Services Departments, including LITS sub-departments, are responsible for configuring and managing all computer systems and other IT resources in compliance with PCI DSS and Emory security requirements, limiting access to IT resources and cardholder data, and assisting the Office of Treasury and Debt Management in completing the technical sections of the annual PCI DSS self-assessment.

• Departmental Merchants are responsible for ensuring that all business processes for accepting, processing, retaining, and disposing of cardholder data comply with PCI DSS and all other applicable policies and standards. Departmental merchants are also responsible for performing an annual PCI DSS self-assessment in partnership with the Office of Treasury and Debt Management. Departmental employees who handle cardholder data must attend a security awareness & training program and sign the Payment Card Merchant Compliance Statement.

e. Consequences of Non-Compliance

Non-compliance can result in serious consequences for Emory, including reputational damage, loss of customers, litigation, and financial costs. Failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences which may include:

- loss of the ability to process payment card transactions,
- departmental repayment of financial costs imposed on Emory, and
- employee disciplinary action, which can include termination of employment

The Associate Vice President for Treasury and Debt Management has the authority to restrict and/or terminate merchant account status for non-compliance.

Definitions

Cardholder data is any personally-identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, and Card Validation Code – a three-digit or four-digit value printed on the front or back of a payment card referred to as CAV, CVC, CVV, or CSC depending on the payment card brand. The term cardholder data is interchangeable with payment card data throughout this policy.

Merchant refers to an Emory department or operating unit that has applied for and been approved to accept credit/debit card payments for goods and/or services. A merchant is assigned a specific merchant account, which is used to process all credit/debit card transactions via an Emory-approved payment card processer.

Payment card refers to both credit and debit cards. Payment card processing is defined as using any application or device to process a credit/debit card transaction as payment for goods or services from an Emory merchant. This policy does not apply to the EmoryCard, P-card, and Corporate card programs.

Related Links

- Current Version of This Policy: http://policies.emory.edu/2.2
- Emory Policy 5.1 Information Technology Conditions of Use (http://policies.emory.edu/5.1)
- Payment Card Industry Data Security Standard (PCI DSS) (http://www.pcisecuritystandards.org)
- American Express (http://www.americanexpress.com/datasecurity)
- Discover Financial Services (http://www.discovernetwork.com/fraudsecurity/disc.html)
- MasterCard Worldwide (http://www.mastercard.com/sdp)
- Visa Inc. (http://usa.visa.com/merchants/operations/op_regulations.html)
- Emory Payment Card Processing and Compliance Procedures Manual (https://www.finance.emory.edu/home/cash_debt/daily_cash_needs/cash_operations.html)
- Enterprise Information Security Incident Response Policy (https://policies.emory.edu/policy/index.cfm?policy_id=11281)
- Cardholder Data Environment Remote Access Policy (https://policies.emory.edu/policy/index.cfm?policy_id=11282)
- Payment Card Information Security Policy (https://policies.emory.edu/policy/index.cfm?policy_id=11283)
- PCI Risk Assessment Policy (https://policies.emory.edu/policy/index.cfm?policy_id=11284)
- Retention and Disposal (http://records.emory.edu/documents/pci-data-security.pdf)

Contact Information

Subject	Contact	Phone	Email
Credit Card Merchant Accounts	Treasury and Debt Management		paymentcardservices@emory.edu

Revision History

- Version Published on: Jul 17, 2015 *(Updated link)*
- Version Published on: Jul 17, 2015 *(Updated names and links)*
- Version Published on: Mar 14, 2013
- Version Published on: Jan 28, 2013
- Version Published on: Feb 06, 2009 *(Sub-sections 2.2.3, 2.2.4 and 2.2.5 were added to the current policy.)*
- Version Published on: Mar 28, 2007 *(Original Publication)*