Policy 5.20
PCI Risk Assessment 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: May 15, 2015

Policy Sections:

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

Overview

This policy explains Emory's official position on how the organization formalizes a Risk Assessment as required by PCI DSS v2.0.

Applicability

This policy applies to all people, processes, and technology involved with the storage, processing, or transmitting of 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 (CDE).

Policy Details

As part of the annual PCI compliance process, Emory University will assess all card processing activities in order to identify threats and vulnerabilities that could negatively impact the security of cardholder data and will be documented in a formal risk assessment. The PCI Risk Assessment shall include:

- Current and Future Merchant processing activities
- Current and Future Service Provider processing activities
- Current and Future Acquirer processing activities
- Results of all Merchant Self-Assessment Questionnaires (SAQ) Compliance
- Results of all Approved Scanning Vendor (ASV) Compliance
- Results of all Acquirer Attestations and Project Plans
- Current and Future Transaction Volume
- Introductions/Changes of Product Lines or Service Offerings
- Introductions/Changes to Software Applications in the Cardholder Data Environment (CDE)
- Introductions/Changes to Third Party relationships
- Changes to Network Topology impacting the Cardholder Data Environment (CDE)
- Any other substantial payment processes deemed appropriate for inclusion to this evaluation

The Library and Information Technology Services, Enterprise Security team uses an adaptive version of the NIST Risk Assessment framework and the documented risk assessment is a result of an annual Enterprise Risk Assessment performed by the staff. This Enterprise Risk Assessment takes into consideration other Information Technology regulatory requirements, systems, threats, and vulnerabilities outside of the scope of PCI DSS.

**Sanctions:**
Failure to comply with Emory’s PCI Risk Assessment policy may result in:
- Suspension or termination of merchant account, suspension of access;
- Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy;
- Civil or criminal prosecution.

**Definitions**

**Acquirer** - Also referred to as “merchant bank,” “acquiring bank,” or “acquiring financial institution.” Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

**ASV** - Acronym for “Approved Scanning Vendor.” Company approved by the PCI SSC to conduct external vulnerability scanning services.

**CDE** - Acronym for “cardholder data environment.” The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

**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.

**Merchant** - For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers.

**Risk Assessment** - Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

**SAQ** - Acronym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.

**Service Provider** - Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data

**Related Links**
- Current Version of This Policy: [http://policies.emory.edu/5.20](http://policies.emory.edu/5.20)
- Payment Card Information Security Policy ([https://policies.emory.edu/5.19](https://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))
- Payment Card Processing and Compliance Policy ([https://policies.emory.edu/2.2](https://policies.emory.edu/2.2))
- Retention and Disposal ([https://records.emory.edu/content/records-management-guides](https://records.emory.edu/content/records-management-guides))

**Revision History**
No previous versions of this policy were found.

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.