Policy 5.18
Cardholder Data Environment Remote Access 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 restricts remote access to the Cardholder Data Environment (CDE).

Applicability

This policy applies to the people, process, and technology involved with accessing and/or governing remote access to the Cardholder Data Environment (CDE).

Policy Details

All use of portable computing devices, such as remote computers, laptops, workstations, or mobile devices, regardless of whether they are employee owned or company owned are prohibited from remotely connecting directly to the Cardholder Data Environment (CDE) at all times. Any remote access to the Cardholder Data Environment (CDE) must go through an Emory-approved “jump-box” with specific standards that will meet or exceed PCI DSS requirements.

User/Jump-Box Requirements:

- User must be a part of the PCI Core VPN Group
- User must utilize two factor authentication (such as a secure ID token) to access the jump-box
- User must use an Emory-owned Computer
- Jump-box must be managed by LITS, Libraries and Information Technology Services
- Jump-box must be configured and managed in a manner that complies with all PCI Data Security Standard requirements, and must receive explicit approval from LITS Enterprise Security prior to use.
- Physical and Logical location of Jump-box within the Emory environment must be approved by LITS Enterprise Security prior to use.

Definitions
**Cardholder Data** - At a minimum, cardholder data should consist 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.

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

**Related Links**

- Current Version of This Policy: [http://policies.emory.edu/5.18](http://policies.emory.edu/5.18)
- Enterprise Information Security Incident Response Policy ([https://policies.emory.edu/5.17](https://policies.emory.edu/5.17))
- Payment Card Information Security Policy ([https://policies.emory.edu/5.19](https://policies.emory.edu/5.19))
- 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 ([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.*