Policy 5.18
Cardholder Data Environment Administrative and 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: July 17, 2017

Policy Sections:

Overview

This policy defines how non-console administrative access and remote access is controlled in the Cardholder Data Environment (CDE).

Applicability

This policy applies to the people, processes, and technology included in the CDE.

Policy Details

PCI DSS version 3.2 control standard 8.2 requires multi-factor authentication for any user who is accessing the CDE remotely. Multi-factor authentication is also required for all non-console administrative access to devices included in the CDE.

All use of computing devices, such as 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.

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 - The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment (CDE), they must be protected in accordance with applicable PCI DSS requirements. 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.

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

Non-console Administrative Access – Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks.

PCI DSS – Acronym for "Payment Card Industry Data Security Standards" The data security standards established to govern the security of payment card data. The current version of the standards are available at https://www.pcisecuritystandards.org/

Related Links

- Current Version of This Policy: http://policies.emory.edu/5.18
- Enterprise Information Security Incident Response Policy (https://policies.emory.edu/5.17)
- Payment Card Information Security Policy (https://policies.emory.edu/5.19)
- 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)
- Emory PCI Policies and Procedures Manual (https://www.finance.emory.edu/home/cash_debt/daily_cash_needs/Payment%20Card%20Processing%20and%20Compliance%20Policy%20and%20Procedures%20Manual.pdf)

Revision History

- Version Published on: May 15, 2015 *(Updated definitions and related links. Other minor modifications.)*
- 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.