Non-Console Administrative Access Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established a formal policy and supporting procedures regarding non-console administrative access. This process will be conducted by authorized personnel with the appropriate technical knowledge and skill sets needed to undertake this activity. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

The Office of Information Security will encrypt all non-console administrative access using strong cryptography for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. Many system components within the cardholder data environment are accessed through a non-console administrative function; thus, they must ensure that strong cryptography and other secure transmission methods are utilized at all times. The following is a list of protocols, secure data transmission elements, and tools that are used for accessing various system components:

- Secure Shell (SSH)
- Virtual Private Network (VPN)
- Secure Socket Layer (SSL) I Transport Layer Security (TLS)
- Secure File Transfer Protocol (sFTP)
- Remote Desktop Protocol (RDP)

Additionally, regarding non-console administrative access, the following conditions must apply in order to ensure further compliance with the Payment Card Industry (PCI) Data

Security Standards (DSS) Initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that a strong encryption method is invoked before the administrator's password is requested.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that Telnet and other insecure remote-login commands are not available for non-console access.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that administrator access to any web-based management interface is encrypted with strong cryptography.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.

Responsibility for Policy Maintenance

The Office of Information Security is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019