Firewall Requirements 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 for having a firewall at each Internet connection, between any demilitarized zone (DMZ), and the internal network zone. 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 ensure that the firewall configuration standards adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.0):

- Firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.
- The network diagrams for the associated cardholder data environment (CDE) are to be consistent with the firewall configuration standards, which requires an illustrative drawing on the diagrams of the logical and/or physical positioning of the firewalls within the network topology.
- Authorized personnel are to regularly review network configuration documentation for the purposes of verifying that firewalls are in place at each Internet connection and between any DMZ and the internal network zone.

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