Firewall and Router Configurations 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 firewall and router configurations. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

Office of Information Security will ensure that firewall and router rules sets reviews 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):

- Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
- Appropriately configure, examine and confirm all firewalls and router settings for ensuring that all inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.
- Appropriately configure, examine and confirm all firewalls and router settings for ensuring that all other inbound and outbound traffic is specifically denied by using various configuration settings (i.e., deny all).
- Secure and synchronize router configuration files.
- Appropriately configure, examine, and confirm that router configuration files are secured from unauthorized access.

- Appropriately configure, examine, and confirm that router configurations are synchronized, for example, the running (or active) configuration matches the start-up configuration.
- Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
- Appropriately configure, examine and confirm examine firewall and router configurations for ensuring that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.
- Appropriately configure, examine and confirm that firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

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