Media Device Protection 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 concerning media device protection. 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 Media Device Protection policy adheres 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):

- Authorized personnel are to conduct the following:
    - Maintain a list of all devices that capture payment card data, for which the list is to include the following:
        - Make, model of device
        - Location of device (for example, the address of the site or facility where the device is located)
        - Device serial number or other method of unique identification.
    - Periodically inspect all devices to ensure that they have not been tampered with or substituted.
    - Adequately train personnel to be aware of suspicious behavior and to report tampering or substitution of devices.
    - Ensure that the list of devices is updated when devices are added, relocated, decommissioned.

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