Physical Security 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 physical security around payment card processing. 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 Physical Security 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):

Any physical location that is part of the Cardholder Data Environment (CDE) must have the following security controls:

- Access is controlled with badge readers or other devices including authorized badges and lock and key.
- Surveillance monitoring equipment and/or access control mechanisms must be in place to monitor the entry/exit points to sensitive areas.
- Surveillance monitoring equipment and/or access control mechanisms must be protected from tampering or disabling.
- Surveillance monitoring equipment and/or access control mechanisms must be monitored and data from equipment or other mechanisms must be stored for at least three (3) months.
- Physical and/or logical controls must be in place to restrict access to publicly accessible network jacks.
- Physical access to wireless access points, gateways, handheld devices, networking/communications hardware and telecommunication lines (i.e., "critical infrastructure hardware") must be appropriately restricted.

Any physical location that is part of the Cardholder Data Environment (CDE) must have the following security for personnel and visitor access:

- Processes and procedures must be in place for assigning badges to onsite personnel (i.e., employees) and visitors, which consist of granting new badges, changing access requirements and revoking access.
- Processes and procedures must be in place for distinguishing between onsite personnel and visitors, with a mechanism to clearly identify visitors.
- Access to the identification process (such as the badge system) must be limited to authorized personnel.
- Appropriate authorization procedures must be followed before authorizing personnel to access the CDE.
- Any terminated employee must have their access authorization removed immediately.
- Visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.
- A visitor log must be in place to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. The log should record key information:
    - The visitor's name
    - The firm represented
    - The onsite personnel authorizing physical access
- The visitor log must be retained for at least three months.
- Visitor identification (such as badges) must expire.
- Visitors must surrender their badge or other authorization identification upon departure or expiration.

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