Anti-Virus 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 anti-virus. 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 Anti-Virus 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):

- For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
- A licensed anti-virus software must be utilized for all computer and system components (any network component, server or application included in or connected to the cardholder data environment) within the cardholder environment and for all computers not directly associated with the cardholder environment.
- The licensed anti-virus software utilized must be the most current version available.
- All computers and system components within the cardholder environment must have standard, supported anti-virus software installed.
- The anti-virus software must be active, must be scheduled to perform virus checks at regular intervals and must have its virus definition and all other associated software files kept current.

- The anti-virus software must be enabled for automatic updates and periodic scans.
- All computers not directly associated with the cardholder environment must have standard, supported anti-virus software installed.
- The anti-virus software for all computers not directly associated with the cardholder environment must also be active, scheduled to perform virus checks at regular intervals and must have its virus definitions and all other associated software files kept current.
- No user shall disable or tamper with the configuration of anti-virus software installed on their respective computer.
- Employees who allow non-company employees to attach workstations (desktops or laptops) to the company network are responsible for ensuring that those workstations are running anti-virus software and that a current virus signature is installed.
- Employees who attach workstations to the company network are responsible for ensuring that those workstations are running anti-virus software and that a current virus signature is installed.
- Never open any emails that are from an unknown or suspicious source.
- Never open any email attachments from an unknown or suspicious source.

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