# Security Patch Management Installation 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 security patch management. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

## Policy

Security patch management (patch management) has become a critical security issue due in large part to the exploitation of information technology systems from numerous external and internal sources. Consequently, all system components directly associated with the cardholder data environment must be securely hardened and configured with all necessary and appropriate patches and system updates for preventing the exploitation or disruption of mission-critical services as mandated (PCI DSS Requirements and Security Assessment Procedures).

Similarly, all IT resources not directly associated with the cardholder data environment must also be securely hardened and configured with all necessary and appropriate patches and system updates in order to prevent the exploitation or disruption of mission-critical services.

In accordance with best practices for security patch management, the subsequent three (3) security concerns will be highlighted throughout the Security Patch Management policy. They are as follows (NIST, n.d.):

- **Vulnerabilities**: Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the system components directly associated with the cardholder data environment or any other IT resources.

- **Remediation:** The three (3) primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting and (3) removal of affected software.

- **Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Common examples are scripts, worms, viruses and Trojan horses.

Failure to keep system components and other IT resources patched securely and on a consistent basis can cause unwanted damage to all environments directly associated with the cardholder environment. This includes but is not limited to the following:

- Network devices and all supporting hardware and protocols.

- Operating systems within the development and production environments.

- Applications within the development and production environments.

- Any other mission-critical resources within the cardholder data environment that require patches and security updates for daily operations

Additionally, a Security Patch Management Program (SPMP) is to be implemented, which consists of the following initiatives:

- A formalized Security Patch Management Program employee, complete with his/her roles and responsibilities.

- Comprehensive inventory of all system components directly associated with the cardholder environment.

- Comprehensive inventory of all other IT resources not directly associated with the cardholder environment.

- Subscribing to industry-leading security sources, additional supporting resources for vulnerability announcements and other security patch management alerts and issues.

- Procedures for establishing a risk ranking regarding security patch management. This will include but is not limited to (1) the significance of the threat, (2) the existence and overall threat of the exploitation and (3) the risks involved in

applying security patch management procedures (its effect on other systems, resources available and resource constraints).

- The creation of a log of remediation activities that needs to be applied.
- Test procedures for testing patches regarding remediation.
- Procedures for the deployment, distribution and implementation of patches and other related security-hardening procedures.
- Procedures for verifying successful implementation of patches and other related security-hardening procedures.
- Installation of applicable critical vendor-supplied security patches within one month of release.
- Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

## 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