Requirement 6.1 to 6.2

Security Patch Management Installation Policy and Procedures

6.1 to 6.2 Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, *[company name]* has established a formal policy and supporting procedures concerning security patch management. This policy is to be implemented immediately. It will be evaluated on a(n) *[annual, semi-annual, quarterly]* basis for ensuring its adequacy and relevancy regarding *[company name]*'s needs and goals.

6.1 to 6.2 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. 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 database 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

6.1 TO 6.2 PROCEDURE

[Company name] has developed and implemented a comprehensive program regarding security patch management, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by *[company name]* for ensuring the Security Patch Management Program (SPMP) initiatives are executed in a formal manner and on a consistent

basis for all system components within the cardholder data environment and all other IT resources.

Security Patch Management Program Employee

This individual will be responsible for coordinating, facilitating and undertaking all necessary activities regarding security patch management policies and procedures. Additionally, this individual will have the necessary information technology and security expertise to successfully execute all steps as required. Specifically, this individual will have a strong working knowledge of vulnerability and patch management, as well as system administration, intrusion detection and firewall management.

Table 6.1.a

Security Patch Management Program Employee

Name	Title	Contact Information
Jason Smith	*Senior Network Engineer*	*smith@company.com*
Mike Larson	*Backup Network Engineer*	*Mlarson@company.com*
?	*?*	*?*
?	*?*	*?*
?	*?*	*?*

Comprehensive Inventory of All System Components Directly Associated with Cardholder Environment

The following table includes all system components that are directly associated with the cardholder environment. These system components are to be listed by network devices, operating systems, applications and any other system components as needed.

Table 6.1.b

System Components	Host Name	Physical Location	Owner of System Components	Primary Use in Cardholder Data Environment
?	*?*	*?*	*?*	*?*
?	*?*	*?*	*?*	*?*
?	*?*	*?*	*?*	*?*
?	*?*	*?*	*?*	*?*

?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?

Comprehensive Inventory of all other IT Resources Not Directly Associated with Cardholder Environment

The following table includes all other IT resources not directly associated with the cardholder environment. These IT resources, however, are still considered critical to the daily operations of *[company name]*.

Table 6.1.c

IT Resources	Host Name	Physical Location	Owner of IT Resources	Primary Use within Organization
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?
?	?	?	?	?

?	*?*	*?*	*?*	*?*
?	*?*	*?*	*?*	*?*
?	*?*	*?*	*?*	*?*

Industry-Leading Security Sources and Additional Supporting Resources

Various external security sources and resources are utilized to ensure that *[company name]* maintains awareness of security threats, vulnerabilities and what respective patches, security upgrades and protocols are available.

Currently, *[company name]* subscribes to the following types of security sources and resources (NIST, n.d.):

- Vendor websites and email alerts
- Vendor mailing lists, newsletters and additional support channels for patches and security
- Third-party websites and email alerts
- Third-party mailing lists
- Online forums and discussion panels
- Conferences, seminars and trade shows

Listed below are the specific security resources and sources to which *[company name]* subscribes for patch management, alerts, security and support as applicable:

Table 6.1.d

Online Resources for Patch Management, Alerts, Security and Support, As Applicable

Vendor/Provider and Type of System	Website	Other
CISCO	http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml	*Security Advisory Alert Board*
IBM AIX	http://www-03.ibm.com/systems/power/software/aix/service.html	*AIX support and alert website*
Microsoft	http://technet.microsoft.com/en-us/wsus/default.aspx	*Windows Server*

		Update Services (WSUS)
Oracle	http://www.oracle.com/technology/deploy/security/alerts.htm	*Critical Patch Updates and Security Alerts*
Apache	http://www.apache.org/dist/httpd/patches	*Official Patches for Apache*
?	*?*	*?*
?	*?*	*?*
?	*?*	*?*
?	*?*	*?*

Please note: This is just a sample used to illustrate how this section should be completed. For an in-depth listing of all vendors, providers, their products and respective websites, please view Appendix D from the following URL: http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf. *Additionally, please add any other vendors that you use.*

Risk Ranking for Security Patch Management

A Risk Ranking matrix will be established regarding security patch management. Specifically, system components and other associated IT resources will be given a risk ranking pertaining to the importance of security patch management activities to be undertaken.

In accordance with NIST SP 800-30, *[company name]* will adhere to the following definitions regarding risks that are related to all system components within the cardholder environment and any other IT resources.

- **High:** The threat source is highly motivated and sufficiently capable; controls to prevent the vulnerability from being exercised are ineffective.
- **Medium:** The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
- **Low:** The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

TABLE 6.1.E

RISK RANKING TABLE

Critical Security Threats	Response Mechanisms to Initiate	Priority Level 1 (High)	Priority Level 2 (Medium)	Priority Level 3 (Low)
Vendor Patches and security updates defined as "high," "critical" or "urgent" for all system components and other IT resources affected by threat	*Please discuss your response mechanisms for these types of security threats.*	*X*		
Vendor Patches and security updates defined as "medium," "moderate" or "important" for all system components and other IT resources affected by threat	*Please discuss your response mechanisms for these types of security threats.*		*X*	
Vendor Patches and security updates defined as "low," "non-essential" or "non-urgent" for all system components and other IT resources affected by threat	*Please discuss your response mechanisms for these types of security threats.*			*X*
Security alerts from SANS, CERT, NIST, CIS and all other industry-leading associations	*Assign risk accordingly based on each individual threat.*			
Recommendations from all other industry-leading security sources (online forums, email subscriptions to security forums, etc.) regarding threats	*Assign risk accordingly based on each individual threat.*			

Additionally, the Security Patch Management Program employee will also be responsible for the following critical activities:

- Being aware of all known threats or vulnerabilities that could significantly impact system components within the cardholder data environment and any other IT resources. This requires consistent oversight and management of all online resources used for security patch management as previously described.
- Having a strong technical and business understanding of all critical systems within the organization's IT infrastructure, as well as knowing which systems are essential for day-to-day operations
- Having response mechanisms and procedures in place to immediately report the scope of the exploitation (systems affected), the impact to the IT infrastructure as a whole and which remediation activities and plan of action initiatives are already available to the management in the event of network exploitation.

Database of Remediation Activities that Need to be Applied

The database for remediation activities will consist of listing the relevant Uniform Resource Locators (URL) for each patch and specific advice and any other comments deemed critical to the patch itself. Additionally, the Security Patch Management Program employee will be responsible for keeping the database accurate and relevant.

Table 6.1.f

System Components within Cardholder Data Environment and other IT Resources	Uniform Resource Locator (URL) for Patch	Notes/Comments
Oracle	http://www.oracle.com/technology/deploy/security/alerts.htm#CriticalPatchUpdates	*Online board and listing for Oracle products and their respective patches*
Microsoft	http://www.microsoft.com/security/updates/bulletins/default.aspx	*Online board and listing for Microsoft products and their respective patches*
?	*?*	*?*
?	*?*	*?*
?	*?*	*?*

Test Procedures for Testing Patches Regarding Remediation

Security patch management testing procedures must be observed to ensure the authenticity of the patch or any other security upgrades before they are released to day-to-day operations. The following testing procedures are to be adhered to (NIST, n.d.):

- An acceptable test environment (non-production systems) will be determined and utilized, if necessary, for each and every patch and security upgrade implemented by the SPMP employee.

- For vendors providing patches, the authenticity of the downloaded patch will need to be verified. This verification process will be determined as needed for patches and security upgrades.
- A virus scan is to be run on all patches before installation.
- Determine *patch dependency* or any other issues that may result in the installation of the patch. Would the installation of the new patch disable another? Are other patches uninstalled when the new patch is installed?

Procedures for the Distribution, Deployment and Implementation of Patches and other Related Security-Hardening Procedures

All patches and security updates are to be pushed out in a formalized and secure manner, with all critical patches installed within one (1) month of release from a vendor or other approved third party. This includes using the following:

- Enterprise Patch Management software
- Secured email lists sent to authorized personnel
- Secure internal web source for retrieving patches sent out by the SPMP employee

[Listed above are three common examples of deploying patches. Please modify according to your specific environment.]

Procedures for Verifying Successful Implementation of Patches and other Related Security-Hardening Procedures

It is the responsibility of the SPMP employee to verify the successful implementation of all patches and security upgrades to *[company name]*'s IT infrastructure. These activities will consist of, but are not limited to, the following:

- Verifying that the files have been changed as stated in the vendor's documentation to reflect the updates as needed
- Verifying whether the recommended patches and security updates were installed properly by reviewing patch logs

[Listed above are two common examples of verifying the successful implementation of patches and security updates. Please modify according to your specific environment.]

6.1 to 6.2 Responsibility for Policy Maintenance

The *[title of responsible party]* 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.