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 as mandated (PCI DSS Requirements and Security Assessment Procedures, Version 3.0).

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.
- 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).

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.

Requirement 8.7

Database Access & Configuration Settings Policy and Procedures

8.7 Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, [company name] has established a formal policy and supporting procedures concerning database access & configuration settings. 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.

8.7 Policy

[Company name] will ensure that the Database Access & Configuration settings 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, Version 3.0):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all users are authenticated prior to access.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that user direct access to or queries of databases are restricted to database administrators.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that application IDs can only be used by the applications (and not by individual users or other processes).

8.7 Procedures

[Company name] has developed and implemented a comprehensive policy regarding database access and configuration, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by [company name] to ensure that the database authentication and configuration 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 deemed critical by [company name].

Database Authentication Procedures

Authentication procedures to databases allow users to perform a wide variety of work-related tasks such as read and write privileges, the execution of queries, making structural changes to the database itself and numerous other critical functions. As such, *[Company name]* utilizes the following authentication procedures for verifying the identity of a user or tool that is requesting database access to use data, resources or applications. Validating the authentication process to databases establishes a trust relationship while also enabling accountability by linking access and actions to specific identities.

Table 8.7

Database Authentication Methods

Database System	**MySQL 5.5.8**
Hostname(s)	**DB001PROD, DB002PROD and DB003PROD, which are three (3) production database servers, each residing on the internal host on separate, physical stand-alone Dell servers**
Application or platform for which Database Supports	**DB001PROD, DB002PROD and DB003PROD all support the internally developed Software as a Service Platform (SaaS), which grants clients access to all necessary financial data for their respective accounts.**
Authentication by the Operating Systems	**Yes, authentication to the database is allowed in the following manner: [please describe if this is allowed, as various operating systems allow for the database to use information they obtain to authenticate users.]**
Authentication by the Application	**Yes, authentication to the database is allowed in the following manner: [please describe if this is allowed, as many end-users can actually have access to databases when they perform searches or queries within the application, resulting in the database being called.]**
Authentication by the Network	**Yes, authentication to the database is allowed in the following manner: [please describe network protocols used to allow database authentication, such as Kerberos, LDPA and remote network authentication (Radius, SSL, etc.)]**
Authentication by the Database	**Yes, authentication to the database is allowed in the following manner: [please describe direct database authentication procedures that are utilized, such as storing users' passwords in the data dictionary, allowing for direct access.]**
Authentication for Database Administrators (DBA)	**Database administrators authenticate in the following manner: [please describe how they authenticate, both with local and remote authentication.]**

Database Access Rights and Stored Procedures

Database access rights, and access rights to the related applications for which they support, are defined in a manner that ensures all user access, user queries and user actions are done so through programmatic methods such as stored procedures. Stored procedures allow greater flexibility in offering capabilities such as conditional logic and also help to reduce bandwidth and execution time. As such, the following access rights have been defined for the different classes of users along with a listing of general programmatic methods/stored procedures that are in place for each class of users (i.e., end-users, system administrators, database administrators [DBA]).

TABLE 8.7.B

DATABASE ACCESS RIGHTS AND STORED PROCEDURES

	General Access Rights and Privileges	Programmatic Methods/Stored Procedures for users
Access Rights for End-Users	End-users are generally restricted to read-only rights and specific queries of the database for their given role, which have been established through programmatic methods and stored procedures via SLQ Statements.	[Please provide a general list of programmatic methods and stored procedures that are in place for end-users.]
Access Rights for System Administrators	System Administrators have all rights associated with end-users, along with having elevated access rights to database content within various tables.	[Please provide a general list of programmatic methods and stored procedures that System Administrators use themselves, or have implemented for others to use.]
Access Rights for Database Administrators (DBA)	Database Administrators (DBA) have super-user rights, allowing access to the entire database, along with the ability to perform any function desired.	[Please provide a general list of programmatic methods and stored procedures that Database Administrators use themselves, or have implemented for others to use.]

DATABASE ADMINISTRATORS

The database administrator (DBA) is responsible for the design, implementation, maintenance and repair of all databases within the organization. As such, DBAs are granted direct access to all databases and may perform all necessary functions to facilitate proper operations of the databases and all supporting systems. DBA functions include but are not limited to the following:

- transferring data
- replicating data
- maintaining database and ensuring its availability to users
- controlling privileges and permissions to database users
- monitoring database performance
- database backup and recovery
- database security

Database Applications and Related Application IDs

For database applications and the related application IDs, application IDs can only be used by the applications, not by individual users or other processes. As such, the following procedures are in place for ensuring this function: [Please discuss what functions you have in place for ensuring this is being implemented. For example, somebody other than the actual employee associated with the application(s) calling the database should set the application IDs.]

Database Tools

The following tools are utilized to facilitate all daily operational processes and procedures concerning the administration of *[Company name]* databases.

Table 8.7.c

Database Tools and Uses

Tool	General Description and Use
Navicat	Series of graphical database management and development software that supports multiple database connections for local and remote databases
SQL Workbench	SQL Workbench/J is a free, DBMS-independent, cross-platform SQL query tool whose main focus is running SQL scripts (either interactively or as a batch) and export/import features.
SQL Plus	Oracle command-line utility program that can run SQL and PL/SQL commands interactively or from a script
Toad	Database tools built for analysts, developers and database administrators
?	?
?	?
?	?

8.7 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)

EMPLOYEE SEPARATION FORM

General Information for Terminated User

User Name and Contact Information			Type Of User (Circle one):			
			Employee	Guest	Vendor	Other
Last Name	First Name	Middle Name	Social Security Number, Internal Employee ID Number, or other type of Unique Identifier			
Date of Termination			Type of Termination (Circle one):			
Month:	Day:	Year:	Voluntary		Involuntary	

If user was involuntary terminated, please provide a brief overview as to the nature and reason for this:

Physical Office Address Where User Resided				
Street Address	City	State	ZIP	Country

Administrative Actions (Financial and Legal) to Initiate for Terminated User

Item Number	Task or Action to be Performed		Date Performed	General Notes and/or Comments
1.	Determine financial amount ("wages") that are owed to terminated user, which must include any vacation, bonuses. or any other type of compensation issue that must be factored into consideration.			
	(a).			
	(b).			
	(c).			
	(d).			

2.	Determine what deductions are necessary from final amount owed to terminated user.			
	(a).			
	(b).			
	(c).			
	(d).			
3.	Determine if company has any obligations to terminated user regarding stock options or any other type of other securities and/or instruments.			
	(a).			
	(b).			
	(c).			
	(d).			
4.	Determine if any legal actions (i.e., civil, criminal, other) are pending or are being considered against terminated user.			
	(a).			
	(b).			
	(c).			
	(d).			
5.	Determine if any non-compete, confidentiality, trade secret rights are in place and enforceable, if necessary.			
	(a).			
	(b).			
	(c).			
	(d).			
6.	Determine if any final expense reports are outstanding and need to be paid to terminated user.			
	(a).			
	(b).			

	(c).			
	(d).			
7.	Determine if any other Financial and Legal issues require resolution regarding terminated user.			
	(a).			
	(b).			
	(c).			
	(d).			

Administrative Actions (Health and Benefits) to Initiate for Terminated User

Item Number	Task or Action to be Performed		Date Performed	General Notes and/or Comments
1.	Coordinate COBRA benefits or other state equivalent coverage as required by law and confirm that coverage is guaranteed for a minimum of [x] days.			
	(a).			
	(b).			
	(c).			
	(d).			
2.	Determine 401K responsibilities for company (such as rollover, etc.) and notify 401k provider of termination of user.			
	(a).			
	(b).			
	(c).			
	(d).			
3.	Notify all applicable Health and Benefits provides regarding terminated user, this includes, but is not limited to the following: (1). Medical. (2). Dental (3). Life. (4). Disability.			
	(a).			
	(b).			

	(c).			
	(d).			
4.	Determine if any other Health and Benefits issues require resolution regarding terminated user.			
	(a).			
	(b).			
	(c).			
	(d).			

Administrative Actions (Internal Controls) to Initiate for Terminated User

Item Number		Task or Action to be Performed	Date Performed	General Notes and/or Comments
1.	Determine if terminated user had any of the following financial privileges:			
	(a).	Signature Authority		
	(b).	Access to company financial accounts (i.e., bank accounts, brokerage accounts, investment accounts, etc.).		
	(c).	Access to employee administered financial accounts.		
2.	Determine if the terminated user was effectively removed from access from the following company-wide system resources:			
	(a).			
	(b).			
	(c).			
	(d).			
	(e).			
	(f).			
3.	Determine if any other Internal Controls and/or operational issues require resolution regarding terminated user.			
	(a).			

	(b).			
	(c).			
	(d).			
	(e).			
	(f).			
	(g).			
	(h).			
	(i).			

Company Assets and Property Checklist

Item	Asset | Property	Serial Number	Date of Return	General Notes and/or Comments
1.	Computer (Laptop)			
2.	Printer, Scanner, Fax			
3.	Cell Phone, Pager			
4.	Portable Digital Assistant (PDA)			
5.	USB Drives, External hard Drives, etc			
6.	Company Credit Card			
7.	Access Devices-Keys			
8.	Access Devices-Electronic Badges | Swipe Cards			
9.	Furniture			
10.	Pictures			
11.	Uniforms			
12.	Parking Permits			
13.				
14.				
15.				

Comments or any Special Requests or Instructions:	
Approval	
Name and Title of Personnel approving Employee Separation form	**Notes/Comments**
Date of Approval	**Signature**

Incident Response Plan Form

Incident Response Form	
Date and Time of Notification:	
Date and Time of Detection:	
Name:	
Title:	
Phone:	
Email:	
Signature:	

Summary of Incident	
Type of Incident:	**Description of Incident:**
Names and Contact Information of Other Parties Involved:	

Incident Notification			
Names of Personnel Contacted:			
1.		**6.**	
2.		**7.**	
3.		**8.**	
4.		**9.**	
5.		**10.**	

Response and Resolution Measures
Initial Response:
Evidence Collection and Investigation:
Security Analysis | Recovery and Repair
Communication
Lessons Learned