Change Management
Version 3.0

Implementation Notes

This is a package of 3 policies covering change management, control of computers and software and antivirus protection. These policies contain the minimum information needed to comply with the PCI DSS requirements in the subject areas.

These policies contain appendices that you must complete when implementing this policy.

You may need to write additional policies and/or procedures to accommodate your specific organization's practices.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Change Management
Version 3.0

1. Purpose

1.1. The purpose of this policy is to ensure changes affecting computers and devices that store, process or transmit credit card information are well controlled, properly approved and conform to the Payment Card Industry Data Security Standard (PCI DSS).

1.2. Companies having a single proprietor may not be able to meet the letter of the above section. It is strongly recommended that those who do not have qualified employees or sole proprietorships obtain an expert to sit on a Change Management and Control Committee (CMaCC) and provide an independent review.

2. Scope and Responsibility

2.1. This Policy applies to all computers and devices that store, process or transmit credit card information or Primary Account Numbers (PAN).

2.2. The CMaCC shall appoint an Incident Response Team. The CMaCC may sit as the Incident Response Team, if it chooses.

2.3. The CMaCC is responsible for compliance with the Payment Card Industry Data Security Standard.

2.4. The CMaCC is responsible for ensuring each employee who handles or uses credit card information or PAN data is screened appropriately (background check) before being granted access to these data.

2.4.1. Employees who handle one card at a time, in the customer's presence, may be exempted from this requirement at the discretion of the CMaCC.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

2.5. The CMaCC is responsible for the overall implementation of this policy and all policies, procedures and activities that have ANY affect on the storage, processing and transmission of credit card information or PAN.

2.6. The Information department is responsible for administering policies and procedures associated with this policy.

2.7. All employees are required to comply with applicable portions of the Policy and Procedure Manual.

3. Policy

3.1. Change Management and Control Committee (CMaCC).

3.1.1. The CMaCC shall consist of at least 2 members, 3 or more are recommended, as per Appendix A.

3.1.2. Managers and persons from a minimum of the following disciplines make up the CMaCC:

3.1.2.1. Operations
3.1.2.2. Information and technology (this may be a contractor or vendor)
3.1.2.3. Human Resources

3.1.3. A meeting quorum shall consist of a simple majority of the CMaCC membership (half plus one).

3.1.4. A record of each CMaCC meeting shall be made per Appendix B. This record shall include attendees, a synopsis of discussions, a detail of all decisions reached and the meeting date.

3.1.5. The CMaCC shall review system configurations annually to assess data risk.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.2. General Configuration Policy

All equipment and systems must comply with the following configuration policy:

3.2.1. Prior to deployment, hardware, operating systems, services and applications shall be approved by the CMaCC.

3.2.1.1. Approvals shall be signed by appropriate management.

3.2.2. New computer code:

3.2.2.1. Prior to deployment, new computer code shall be approved by the CMaCC.

3.2.2.2. Back-out plans shall be in place in case of an implementation failure.

3.2.3. Operating system configuration must conform to implementing procedures.

3.2.4. The CMaCC shall approve configuration changes.

3.3. Equipment outsourced to External Service Providers such as hosting companies.

3.3.1. Under the PCI DSS the responsibility for the security of the equipment deployed by other companies must be PCI DSS compliant. This is to be documented in the contract.

3.3.2. Departments or persons that engage contractors are responsible for third party compliance with this policy.

3.3.3. External vendors shall be required to comply with the portions of the PCI DSS that apply to them.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.3.4. Contracts shall allow the company to verify that the vendor is compliant with the PCI DSS.

4. References and Cites

4.1. PCI Data Security Standard v3.0

5. Records

5.1. Appendix A – Change Management Committee Members

5.2. Appendix B - Change Management and Review Committee Minutes

6. Definitions

6.1. *Credit Card Information* – This is made up of 4 elements, the Primary Account Number (PAN), Cardholder Name, Service Code and Expiration Date. When these elements are found in association with each other they must be protected.

6.2. *PAN* – An acronym for the Primary Account Number, which is the number embossed on the face of a credit or debit card. The PAN is always protected, either by encryption, masking or if stored on paper, placing in secure storage.

6.3. *Service Code* – A three-digit code encoded on the magnetic stripe of a credit card that controls the circumstances where the card may be used (international transactions, types of purchases, etc.).

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Appendix A: Change Management and Review Committee Members

CMaCC Membership

Job Title	Name	Date Appointed

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Appendix B: Change Management and Review Committee Minutes

Date of Meeting:_____

Attendance:

_____
_____
_____
_____
_____
_____
_____

Minutes:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Control of Computers and Software
Version 3.0

1. Purpose

1.1.1. The purpose of this procedure is to provide guidance so computers that store, process or transmit credit card information have software and hardware managed in such a way that conforms to the Payment Card Industry Data Security Standard. Including:

1.1.2. Computers are physically secured

1.1.3. Access is controlled

1.1.4. Virus protection is in place and configured correctly

1.1.5. Operating systems are up to date

1.1.6. Configuration management is in place

2. Scope and Responsibility

2.1.1. Information personnel are responsible for implementing this policy. Roles and security responsibilities shall be documented in Appendix B.

2.2. This policy is applicable to all computers and other devices that store, process or transmit credit card information or PAN or are connected to credit card information.

2.3. The physical security requirements of this policy are applicable to all equipment such as routers and switches connected to computers that store, process or transmit credit card information.

3. Procedure

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.1. For all hardware and software the password shall be changed from the original vendor default password to a strong password in accordance with the company's requirements for administrative passwords.

3.2. Physical security

3.2.1. Computers that store credit card data must be kept in a locked room or cabinet.

3.2.2. Visitor access to computer rooms, data centers and cabinets, including contractors and vendors, must be controlled.

3.2.2.1. Badges shall be assigned by authorized personnel including:

3.2.2.1.1. Visitor badges shall be clearly distinguishable from employee ID badges and shall expire.

3.2.2.1.2. Access to any badge system or process.

3.2.2.1.3. Granting badges to visitors before they are allowed access.

3.2.2.1.4. Changing access requirements or levels.

3.2.2.1.5. Revoking or terminating badges when access is no longer needed or allowed.

3.2.2.1.6. Visitor access shall be logged.

3.2.2.1.6.1. Logs shall contain, at a minimum, the visitor's name, company affiliation, the employee authorizing and the employee responsible for the visit if different from the authorizer.

3.2.2.1.7. Badges shall be surrendered any time the visitor leaves the premises.

3.2.2.2. Appropriate access controls, such as videos, shall be applied to sensitive areas including data centers, server rooms, gateways and access points.

3.2.2.2.1. Monitoring equipment and records/recordings shall be protected from tampering.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.2.2.2.2. Data gathered shall be correlated with other controls (access logs, etc.).

3.2.2.2.3. Data gathered shall be retained for at least 3 months.

3.2.2.2.4. Network jacks

3.2.2.2.4.1. Publicly accessible jacks shall be:

3.2.2.2.4.1.1. Physically secured or;

3.2.2.2.4.1.2. Disconnected.

3.2.2.2.4.2. Visitors in areas with "live" network jacks shall be escorted.

3.2.3. Routine access shall only be given to those employees with a business need to access or service.

3.2.4. Computers shall be inventoried on Appendix A: Computer Inventory.

3.2.5. Computers shall be labeled with their names, IP addresses and locations.

3.3. Anti-Virus

3.3.1. Anti-virus software shall be installed on all company owned computers.

3.3.1.1. Administrative default accounts and passwords shall be changed according to the company requirements for administrative user names and passwords.

3.3.1.2. Anti-virus software capable of detecting, removing and protecting against all known types of malicious software shall be deployed on all systems that are vulnerable.

3.3.1.2.1. The master installation of anti-virus software shall be set to automatically update. This feature is to be set so the user cannot bypass the updates.

3.3.1.2.2. Regardless of automated updates personnel shall ensure anti-virus definitions are up to date.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.3.1.2.3. Automatic scanning shall be enabled.

3.3.1.2.4. Anti-virus software shall generate audit logs and shall be retained in accordance with the Access Control Log Policy.

3.3.1.3. If software testing conflicts with anti-virus software, run the anti-virus utility to ensure the machine is virus free, disable the software, then run the test. After the test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email, browsers or file sharing.

3.4. Operating Systems

3.4.1. All patches/hot-fixes recommended by the equipment vendor and Company must be installed as soon as practical after testing and/or review, but no longer than 30 days from release.

3.4.2. This applies to all services installed, even though those services may be temporarily or permanently disabled.

3.4.3. There must be processes in place to keep appropriate patches/hot fixes current, such as auto update.

3.4.4. Services and applications not serving business requirements must be disabled in accordance with the company's requirements for firewall security.

3.4.5. Access to services and applications not for general access must be restricted.

3.4.6. Remote administration must be performed over secure channels via VPN connections or console access independent from the DMZ networks. In other words, you can use a console from a machine that is INSIDE the firewall or on the server being administered.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.5. Software

3.5.1. New software shall be tested for security vulnerabilities prior to deployment.

3.5.2. No software shall be deployed without written approval by management.

3.6. Configuration Management – Configuration standards shall be implemented that include:

3.6.1. Configurations developed for all system components shall be consistent with industry accepted hardening standards (see definition in section 6).

3.6.2. Configuration standards shall be updated as new vulnerabilities are identified according to Vulnerabilities scoring 4.0 or above on the Common Vulnerability Scoring system (CVSS), found at http://nvd.nist.gov.

3.6.3. Configuration standards shall be applied when new systems are configured.

3.6.4. The following restrictions shall apply:

3.6.4.1. There shall be only one primary function per server.
3.6.4.2. If virtualization is used there shall be only one primary function per system.
3.6.4.3. Only necessary services, protocols, daemons, etc. directly necessary for the function of the system may be enabled. All unnecessary services, protocols, daemons, etc. shall be disabled.
3.6.4.4. Insecure services, protocols, daemons, etc. shall be justified and documented security features shall be implemented (SSH, SSL, IpSec VPN, etc.).

3.6.5. Configuration standards shall include:

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.6.5.1. Knowledgeable system administrators and personnel shall configure the system in accordance with company policies and procedures. Personnel must be knowledgeable in common system security parameter settings for the components they configure.

3.6.5.2. Common system security parameter settings shall be set appropriately.

3.6.5.3. Documentation shall be maintained that enables functions to support secure configuration.

3.6.5.4. All unnecessary functions – such as scripts, drivers, features, subsystems, file systems and unnecessary web servers shall be removed.

3.6.5.5. Only documented functionality shall be present on system components.

3.7. Network

3.7.1. The Information Department shall maintain a diagram, in accordance with the Firewall Policy, showing all computers that store credit card information or primary account numbers (PAN). The diagram shall include all computer, networks and equipment that are connected to computers containing PAN data.

3.8. Servers

3.8.1. Only one primary function shall be implemented per server (for example, web servers, database servers and DNS shall be implemented on separate servers.)

4. References and Cites

4.1. PCI Data Security Standard v3.0

5. Records

5.1. Appendix A: Computer Inventory

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

5.2. Appendix B: Personnel Responsible for Information Security

6. Definitions

6.1.1. *Credit Card Information* – This is made up of 4 elements, the Primary Account Number (PAN), Cardholder Name, Service Code and Expiration Date. When these elements are found in association with each other they must be protected.

6.2. *Hardening Standards* - Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).

6.3. *PAN* – An acronym for the Primary Account Number, which is the number embossed on the face of a credit or debit card. The PAN is always protected, either by encryption, masking or if stored on paper, placing in secure storage.

6.4. *Malicious Software* – Viruses, Trojans, Worms, Spyware, Adware, Rootkits and other harmful programs that are capable of damaging computers and equipment or searching for and stealing data.

6.5. *Service Code* – A three-digit code encoded on the magnetic stripe of a credit card that controls the circumstances where the card may be used (international transactions, types of purchases, etc.).

6.6. *VPN* – Virtual Private Network a secure connection, sometimes called a tunnel, which allows data to transit the Internet securely.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Appendix A: Computer Inventory

Computer Name	IP Address	Location

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Appendix B: Personnel Responsible for Information Security

Name	Title	Responsibilities

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

User Anti-Virus
Version 3.0

1.0 Purpose

1.1 This policy is intended to guide employees to protect company computers from viruses, malicious code, spam and attacks.

2.0 Scope and Responsibility

2.1 Information Personnel shall ensure anti-virus software is installed on all company computers and managed in accordance with this policy.

2.2 All employees are required to observe Section 3 of this policy when using the company computers.

3.0 Policy

3.1 All employees shall observe the following:

3.2 NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments then immediately empty your Trash Folder.

3.3 Delete spam, chain, and other junk email without forwarding.

3.4 Never download files from unknown or suspicious sources.

3.5 Avoid direct disk sharing with read/write access unless there is a business requirement to do so.

3.6 Never use a portable disk (thumb drive or other), CD, DVD or floppy diskette from an unknown source.

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.7 Always scan a portable disk (thumb drive or other), CD, DVD or floppy diskette from any source for viruses before using it.

3.8 Employees are forbidden from using a computer that does not have updated anti-virus software installed.

3.9 Employees are forbidden from disabling anti-virus software in any way.

3.10 Anti-virus software shall be set so that users do not have access to settings or the ability to disable the software.

4.0 References and Cites

4.1 PCI Data Security Standard v3.0

Copyright 2008-2015 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.