Administrative Data Security
Version 3.2

Implementation Notes

This document is a package of 3 policies including, Administrative Data Security, Control of Computers and Software and Electronic Data Security. You must implement all 3 of these policies plus any additional policies or procedures that you may write to control your particular business.

These policies contain the minimum requirements that must be met to comply with specific requirements of the PCI DSS. Your controls may be more complex and require additional security measures. You must document additional controls you may be using in policies and/or procedures.

This policy contains appendices that must be completed and maintained.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Administrative Data Security
Version 3.2

1. Purpose

1.1. The purpose of this policy is to define the requirements for customer personal information, particularly credit card account numbers (PAN), when retained on paper.

2. Scope and Responsibility

2.1. All employees who handle or use paper records containing credit card primary account numbers as part of their job responsibilities.

3. Policy

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. Security Codes

3.2.1. Under no circumstances shall the security code, which is sometimes called the CVV or CVC value, be written down or collected on paper. This number is found printed on the signature block of the card on MasterCard, JCB, Visa and Discover and printed on the front of American Express cards.

3.2.2. Employees may collect this value directly from a card or verbally from the cardholder over the phone. It may be entered into a terminal or computer where it is erased after authorization.

3.3. Paper records of credit card account numbers (PAN) shall be stored in locked files when not in use.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.4. PAN data shall not be left unattended when in use. Employees who must leave the work area while PAN records are outside of the locked file shall secure them in a drawer, a locked room or return them to the file.

3.5. If PAN are part of a data entry or order form they may be destroyed by shredding after data entry and verification.

3.6. PAN received by fax shall be subject to the following:

3.6.1. The fax machine shall be secured or attended while receiving PAN data.

3.6.2. Faxes shall be treated the same as paper records.

3.7. Record retention and destruction

3.7.1. Records should be retained for no more than 2 years.

3.7.2. Orders may be destroyed immediately after the transaction is completed unless they are the only transaction record. In that case, they must be retained for 2 years. The PAN may be obliterated leaving no more than the last 4 digits of the card number to increase security.

3.7.3. Records sent to long-term storage shall be shipped in a sealed and locked container and inventoried as to their location and destruction date. See Appendix A: Inventory of Storage Locations.

3.7.4. Records shall be reviewed quarterly to identify records that exceed the destruction period by one or both of the following methods:

3.7.4.1. A management review shall determine the cardholder data or paper records that have exceeded the destruction period.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.7.4.2. An automated or manual programmatic process shall delete cardholder data that has exceeded the destruction period.

3.7.4.3. All cardholder data records and data shall be identified on Appendix B of this policy.

3.7.5. Destruction shall be performed securely by either an employee or a secure destruction service.

3.7.5.1. Destruction must be through shredding, incinerating or pulping. In the case of electronic media degaussing may be used.

3.8. Each employee who handles or uses credit card information or PAN data shall be screened appropriately (background check) before being granted access to this data.

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

4. References and Cites

4.1. PCI Data Security Standard v3.2

5. Records

5.1. Appendix A: Inventory of Storage Locations

5.2. Appendix B: Retention Schedule for Cardholder Data

6. Definitions

6.1. *PAN* – Credit Card Primary Account Number.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

6.2. *Credit Card Primary Account Number* – The number embossed on the face of a credit card. This number is sometimes printed on the back of the card across the signature block.

Copyright 2008-2016 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: Inventory of Storage Locations

Location – Address or Room	Destruction Date

Copyright 2008-2016 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: Retention Schedule for Cardholder Data

Name and Type of Record or Media	Retention Period	Authorized By

Copyright 2008-2016 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 3.2

1.0 Purpose

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:

1.2 Computers are physically secured

1.3 Access is controlled

1.4 Virus protection is in place and configured correctly

1.5 Operating systems are up to date

1.6 Configuration management is in place

2.0 Scope and Responsibility

2.1 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.

3.0 Procedure

Copyright 2008-2016 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

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

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

- 3.4.1 Badges shall be assigned by authorized personnel including:
- 3.4.2 Visitor badges shall be clearly distinguishable from employee ID badges and shall expire.
- 3.4.3 Access to any badge system or process.
- 3.4.4 Granting badges to visitors before they are allowed access.
- 3.4.5 Changing access requirements or levels.
- 3.4.6 Revoking or terminating badges when access is no longer needed or allowed.
- 3.4.7 Visitor access shall be logged.
  - 3.4.7.1 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.
- 3.4.8 Badges shall be surrendered any time the visitor leaves the premises.
- 3.4.9 Appropriate access controls, such as videos, shall be applied to sensitive areas including data centers, server rooms, gateways and access points.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

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

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

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

3.4.13 Network jacks

3.4.13.1 Publicly accessible jacks shall be:

3.4.13.2 Physically secured or;

3.4.13.3 Disconnected.

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

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

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

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

3.8 Anti-Virus

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

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

3.9.2 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.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.9.3 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.

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

3.9.5 Automatic scanning shall be enabled.

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

3.9.7 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.

3.10 Operating Systems

3.11 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.

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

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

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

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

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.16 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.

3.17 Software

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

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

3.20 Configuration Management – Configuration standards shall be implemented that include:

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

3.22 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.

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

3.24 The following restrictions shall apply:

3.24.1 There shall be only one primary function per server.

3.24.2 If virtualization is used there shall be only one primary function per system.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.24.3 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.

3.24.4 Insecure services, protocols, daemons, etc. shall be justified and documented security features shall be implemented (SSH, IpSec VPN, etc.).

3.25 Configuration standards shall include:

3.25.1 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.

3.25.2 Common system security parameter settings shall be set appropriately.

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

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

3.25.5 Only documented functionality shall be present on system components.

3.26 Network

3.27 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.

3.28 Servers

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

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

4.0 References and Cites

4.1 PCI Data Security Standard v3.2

5.0 Records

5.1 Appendix A: Computer Inventory

5.2 Appendix B: Personnel Responsible for Information Security

6.0 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 *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

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

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 2008-2016 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 3.2

Appendix A: Computer Inventory

Computer Name	IP Address	Location

Copyright 2008-2016 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 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

Electronic Data Security
Version 3.2

1.0 Purpose

1.1 This policy is intended to ensure customer personal information, particularly credit card information and primary account numbers (PAN), are securely stored.

2.0 Scope and Responsibility

2.1 The Information Department or information personnel shall be responsible for implementing this procedure.

2.2 Vendors who provide software or hardware services, for example; hosting companies and hosted software that store, process or transmit credit card data or PAN data are bound by this policy.

3.0 Policy

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 Security Codes

3.3 Under no circumstances shall the security code, which is sometimes called the CVV or CVC value, be stored – EVEN IF ENCRYPTED. This number is found printed on the signature block of the card on MasterCard, JCB, Visa and Discover and printed on the front of American Express cards.

3.4 Employees may collect this value directly from a card or verbally from the cardholder over the phone. It may be entered into a terminal or computer where it is erased after authorization.

Copyright 2008-2016 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 PAN Data

3.6 PAN data shall be stored on network file servers only. No storage on workstations, laptops or personal computers is permitted, even for brief periods of time.

3.7 Under no circumstances are the full contents of the magnetic stripe to be recorded or stored.

3.7.1 The PAN data obtained from the magnetic stripe is limited to card number, expiration date and card holder name and this data shall be encrypted when stored.

3.8 PAN data is to be encrypted or truncated to the last four digits at all times when stored.

3.8.1 When data is displayed in reports or on user screens the PAN shall be masked so only the last four (4) digits of the number are printed of displayed.

3.9 When credit card data is sent over public networks, such as the internet, it must be encrypted.

3.10 SSL and early versions of TLS shall not be used unless there is a written plan to secure their use that includes a migration plan that discontinues them by 6/30/2018, as follows:

3.10.1 The name of the policy <Company Name> Network Security Policy.
3.10.2 The date, before 6/30/2018, the migration will by complete.
3.10.3 A confirmation that this is the formal policy.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.11 Access control to PAN data shall be on a strict need-to-know basis only. All other traffic is to be denied unless specifically authorized.

3.12 Modems are to be set to automatically disconnect from the host when not in use.

3.13 Wireless networks are to be secured according to the company's requirements for wireless networks.

3.14 Media Storage

3.15 Strict control shall be maintained over all media including computers, drives, etc. as follows:

- 3.15.1 Media shall be classified so sensitive data can be readily identified.
- 3.15.2 Any movement of media shall be explicitly approved by management.
- 3.15.3 Media shall be sent by secure delivery method and shall be accurately tracked.
- 3.15.4 Tracking logs shall be maintained.
- 3.15.5 Media shall be inventoried and reviewed annually.
- 3.15.6 When no longer needed for business back up, data shall be destroyed by degaussing or the media itself shall be shredded.
- 3.15.7 Media held for destruction:
  - 3.15.7.1 Shall be labeled "to be destroyed."
  - 3.15.7.2 Shall be in locked containers.

3.16 Back up media shall be securely stored and transported as follows:

- 3.16.1 Back up media shall be stored in a secure location, preferably remote.
- 3.16.2 The storage location security shall be reviewed annually.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.

3.16.3 When no longer needed for business back up, data shall be destroyed by securely erasing, degaussing or the media itself shall be shredded.

4.0 References and Cites

4.1 PCI Data Security Standard v3.2

5.0 Definitions

5.1 *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.

5.2 *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.

Copyright 2008-2016 CSRSI, all rights reserved, reproduction in any form, by anyone other than the licensed user, is strictly prohibited unless authorized in writing by CSRSI.