Administrative User Names and Passwords

Version 3.2

Implementation Notes

This document contains 2 polices, one for Administrative User Passwords and a second one for User Names and Passwords.

Administrative User Names and Passwords

This policy applies to controlling and managing system, administrative and managing user passwords.

This policy only contains the basic requirements that must be implemented for compliance with the PCI DSS. You must document any procedures that you use to meet these requirements.

There are two appendices at the end of the policy that must be maintained.

User Passwords

This policy contains requirements for users selecting, safeguarding and maintain their passwords.

This policy contains the minimum requirements for passwords, you must document any additional requirements that you place on users of your systems.

Note that Appendix A must be completed and signed by each user acknowledging that they accept the requirements of the 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.

Administrative User Names and Passwords

Version 3.2

1. Purpose

1.1. The purpose of this policy is to define the administrative requirements for user names and passwords.

2. Scope and Responsibility

2.1. This policy is applicable to any computer system or environment that records or stores credit card information including Credit Card Primary Account Numbers (PAN).

2.2. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any company facility or has access to the company network, and stores any PAN Data. This includes employees, contractors and vendors that have been granted access to network.

2.3. Managers responsible for Human Resources and Information Technology are required to implement this policy.

2.4. Responsible position(s) are to be designated in Appendix A.

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. User Accounts

3.2.1. All users shall be authenticated with their own username and password using multi-factor authentication.

3.2.1.1. Each user shall have a unique user name AND;

3.2.1.1.1. A password, and/OR;

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.

3.2.1.1.2. A token or readable card AND/OR;
3.2.1.1.3. A biometric recording that is authenticated.

3.2.1.2. For remote access:

3.2.1.2.1. A password, and;
3.2.1.2.2. A token or readable card OR;
3.2.1.2.3. A biometric recording that is authenticated.

3.2.1.3. Additions, deletions and modifications of user ID and credentials in any form shall be authorized according to job function.

3.2.2. When an employee or contractor leaves the company, the user account and password shall be immediately revoked.

3.2.3. All user accounts shall be reviewed on a regular basis to ensure malicious, out-of-date or unknown accounts do not exist.

3.2.4. All user accounts shall be reviewed at least every 90 days to identify those accounts that have not logged in for over 90 days. Any identified accounts shall be deleted.

3.2.5. No group or shared user accounts and passwords shall be permitted.

3.2.6. All passwords on network and system devices shall be encrypted and rendered unreadable when transmitted.

3.2.7. User identity must be verified before performing password resets.

3.2.7.1. First time and reset passwords shall be set to a unique value and the user must change it after first use.

3.3. Vendor Access

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.

3.3.1. Vendor access to computers storing processing or transmitting credit card information or PAN data shall be restricted to the time period the vendor needs access for repair or maintenance.

3.3.2. Vendor access shall be specifically approved.

3.3.3. Vendor access shall be documented by a trouble ticket or similar means.

3.4. Network and System Device Configuration

3.4.1. All network and system devices requiring passwords shall be configured to only accept strong passwords.

3.4.2. All network and system devices requiring passwords shall be configured to not allow a user to submit a password that has been used during any of the user's last 4 password changes.

3.4.3. All network and system devices requiring passwords shall be configured to require password change at least every 90 days.

3.4.4. User accounts must be locked for a period of no less than 15 minutes after 6 failed login attempts.

3.4.5. Applications used for remote access shall be configured to require unique user name and password.

3.4.6. Applications used for remote access shall be configured to require encryption and two factor authentication.

3.5. System Administrators and Production System Accounts

3.5.1. All production system level passwords shall be recorded in an encrypted password management database or log.

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.

3.5.2. User accounts that have system level privileges granted through group memberships or programs shall have a unique password from all other accounts held by that user.

3.5.3. Vendor supplied or standard default login passwords shall be changed on new network or internet accounts that can access PAN data.

4. Enforcement

4.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. References and Cites

5.1. Payment Card Industry Data Security Standard v3.2

6. Records

6.1. Appendix A: Job Responsibilities (current list of persons responsible for password administration)

7. Definitions

7.1. *Application Administration Account* - Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.2. *Strong Password* – Passwords that are at least 8 Characters long and use a combination of letters and numbers or special characters eg. *^%#. An example of a strong password is: I81@joe_s.

7.3. *Primary Account Number (PAN)* – A primary account number is the number that is embossed on a credit card.

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.

7.4. *Production System Level Password* – A password that can access administrative functions and data on a computer system that is used in the normal course of business by many users. Sometimes called an Administrative Password.

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: Job Responsibilities

The following personnel are responsible for password administration in accordance with this procedure.

Name	Job Title	Comments

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.

User Passwords

Version 3.2

1. Purpose

1.1. The purpose of this policy is to define the requirements for user passwords.

2. Scope and Responsibility

2.1. This policy is applicable to any computer system or environment that records or stores credit card information including Credit Card Primary Account Numbers (PAN).

2.2. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any facility or has access to the network, and stores any PAN Data. This includes employees, contractors and vendors who have been granted access to network.

3. Policy

3.1. Passwords

3.1.1. All user-level and system-level passwords shall conform to the policy guidance described below.

3.1.2. General Password Construction Guidelines

3.1.2.1. Passwords must follow the "strong password" guidelines.

3.1.2.1.1. Be as long as possible (never shorter than 8 characters).
3.1.2.1.2. Include mixed-case letters.
3.1.2.1.3. Include digits and special characters.
3.1.2.1.4. Not be based on any personal information.

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.

3.1.2.1.5. Not be based on any dictionary word, in any language.

3.1.2.2. Passwords shall never be written down or stored online.

3.1.3. Password Protection Standards

3.1.3.1. Do not use the same password for company accounts as for personal accounts and other non-work related accounts such as home internet and email, banking, benefits, etc.

3.1.3.2. Do not share company passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as confidential company information.

3.1.3.3. Do not use the "Remember Password" function in any application.

3.1.3.4. Passwords must not be inserted into email messages or other forms of electronic communication.

3.1.3.5. Change all passwords at least once every 90 days.

3.1.3.6. If you suspect an account or password has been compromised, change the password immediately and then report the incident to your supervisor.

3.1.3.7. Management may conduct password cracking or guessing on a periodic or random basis by itself or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

3.2. Passphrases

3.2.1. Passphrase construction must adhere to the password guidelines described above.

3.3. Enforcement

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.

3.3.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4. References and Cites

4.1. Payment Card Industry Data Security Standard v3.2

5. Records

5.1. Appendix A: Acceptance of Password Responsibilities (the responsible manager (see Section 2. Scope and Responsibility) shall maintain the completed list in a secure location)

5.1.1. All users granted accounts shall read and sign Appendix A to this Password Policy. This document shall be retained in a secure (locked) location for 2 years from termination of the last employee to sign the document.

6. Definitions

6.1. *Application Administration Account* - Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

6.2. *Strong Password* – Passwords that are at least 8 Characters long and use a combination of letters and numbers or special characters eg. *^%#. An example of a strong password is: I81@joe_s.

6.3. *Passphrase* – The same requirements as for a password except that a passphrase is longer (at least 20 characters) and should contain multiple words.

6.4. *Primary Account Number (PAN)* – A primary account number is the number that is embossed on a credit card.

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.

6.5. *Production System Level Password* – A password that can access administrative functions and data on a computer system that is used in the normal course of business by many users. Sometimes called an Administrative Password.

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.

User Passwords

Version 3.2

Appendix A: Acceptance of Password Responsibilities

By signing this document I certify that I have read understand, and agree to follow the User Passwords Policy. I further understand that violation of this policy may lead to disciplinary action up to and including termination of my employment.

Date	Printed Name	Signature

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.