Access Controls and Logs
Version 3.2

Implementation Notes

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

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.

Access Controls and Logs
Version 3.2

1. Purpose

1.1. The purpose of this policy is to define the requirements for logging access to credit card data and the systems that store, process and transmit such data.

1.2. These requirements are designed to minimize company exposure to loss of credit card information and comply with the Payment Card Industry Data Security Standard (PCI).

2. Scope and Responsibility

2.1. This policy is implemented by the Information Department.

3. Policy

3.1. Access Controls

3.1.1. Access to system components and cardholder data shall be limited to only those individuals whose jobs require such access, as follows:

3.1.1.1. Access rights for privileged user IDs shall be restricted to least privileges necessary to perform job responsibilities.
3.1.1.2. Privileges assigned to individuals shall be based on job classification and function (also called "role-based access control" or RBAC).
3.1.1.3. Approval by authorized parties is required by documentation (in writing or electronically) that specifies required privileges.
3.1.1.4. Access controls may be implemented via an automated access control system.

3.1.2. An access control system shall be in place for systems with multiple users to restrict access based on a user's need

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.

to know, and is it set to "deny all" unless specifically allowed, as follows:

3.1.2.1. Access control systems shall be in place on all system components.
3.1.2.2. Access control systems shall be configured to enforce privileges assigned to individuals based on job classification and function.
3.1.2.3. Access control systems shall have a default "deny-all" setting.

***Note**: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*

3.2. Network Monitoring

3.2.1. A process shall be in place to link all access to system components (especially access done with administrative privileges, such as root) to each individual user.

3.2.1.1. Automated audit trails shall be implemented for all system components to reconstruct the following events:
3.2.1.1.1. All individual user accesses to cardholder data.
3.2.1.1.2. All actions taken by any individual with root or administrative privileges.
3.2.1.1.3. Access to all audit trails.
3.2.1.1.4. Invalid logical access attempts.
3.2.1.1.5. Use of and changes to identification and authentication mechanisms–including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges.
3.2.1.1.6. Initialization, stopping or pausing of the audit logs.
3.2.1.1.7. Creation and deletion of system-level object.
3.2.1.2. Audit trail entries shall be recorded for all 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.

components for each event:

3.2.1.2.1. User identification
3.2.1.2.2. Type of event
3.2.1.2.3. Date and time
3.2.1.2.4. Success or failure indication
3.2.1.2.5. Origination of event
3.2.1.2.6. Identity or name of affected data, system component, or resource

3.3. Time Synchronization

3.3.1. All critical system clocks and times shall be synchronized through use of current time synchronization technology. Time synchronization technology shall be updated as the technology changes.
Note*: One example of time synchronization technology is Network Time Protocol (NTP).*

3.3.1.1. The following controls shall be implemented for acquiring, distributing and storing time:

3.3.1.1.1. Only designated central time servers shall receive time signals from external sources to ensure all critical systems have the correct and consistent time, based on International Atomic Time or UTC.
3.3.1.1.2. Designated central time servers shall peer with each other to keep accurate time, and ensure other internal servers only receive time from the central time servers.

3.3.1.2. Time data shall be protected as follows:

3.3.1.2.1. Access to time data is restricted to only personnel with a business need to access time data.
3.3.1.2.2. Changes to time settings on critical systems shall be logged, monitored and reviewed.
3.3.1.2.3. Time settings shall be received from specific, industry-accepted time sources. (This is to prevent a malicious individual from changing the clock.) Optionally, those updates can be encrypted with a

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.

symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).

3.4. Audit Trails

3.4.1. Audit trails shall be secured so they cannot be altered, as follows:

3.4.1.1. Viewing of audit trails shall be limited to those with a job-related need.

3.4.1.2. Audit trail files shall be protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.

3.4.1.3. Audit trail files shall be promptly backed up to a centralized log server or media that is difficult to alter.

3.4.1.4. Logs for external-facing technologies (for example, wireless, firewalls, DNS, email) shall be offloaded or copied onto a secure, centralized log server or media on the internal LAN.

3.4.1.5. File-integrity monitoring or change-detection software shall be used on logs to ensure existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

3.5. Logs for all system components shall be reviewed at least daily, and follow-ups to exceptions are required.
Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).
Note: *Log harvesting, parsing, and alerting tools may be used to achieve compliance with PCI DSS Requirement 10.6.*

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.

3.6. Log Retention

3.6.1. Audit log retention policies and procedures shall be in place and shall require audit trail history is retained for at least one year.

3.6.2. Audit logs shall be available for at least one year with processes in place to immediately restore at least the last three months' logs for analysis.

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.

4.2. External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

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.