<COMPANY>

PR11 - Log Review Procedure

Document Reference	PR11 - Log Review Procedure
Date	30th September 2014
Document Status	Final
Version	3.0
Revision History	1.0 12 January 2010 - Initial release. 1.1 14 September 2010 - Formatting changes. 1.2 18 January 2011 - Process for restoring historical logs. 1.3 15 June 2011 - Changes to include FIM. 2.0 03 January 2012 - Update to reflect PCI DSS v2.0 changes. 3.0 30 September 2014 - Update to reflect PCI DSS v3.0 changes.

Table of Contents

1. Purpose

This document details the steps required to review the security logs of all system components within the cardholder data environment at least daily, and following a security incident. Any exceptions identified are followed up and reported to Management. Employees of **<COMPANY>** or any other third party authorised to monitor / handle / access the logs should familiarise themselves with this procedure. Questions related to log review should be addressed to the **<COMPANY> [ROLE NAME]**.

2. Scope

This procedure covers all logs generated for systems within the cardholder data environment, based on the flow of cardholder data over the **<COMPANY>** network, including the following components:

- Operating System Logs (Event Logs and su logs).
- Database Audit Logs.
- Firewalls & Network Switch Logs.
- IDS Logs.
- Antivirus Logs.
- CCTV Video Recordings.
- File integrity monitoring system logs.
- All system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- All servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

3. Roles and Responsibilities

<COMPANY> [RESPONSIBLE TEAM] - Responsible for executing and implementing this procedure.

<COMPANY> [ROLE NAME] - Responsible for monitoring the implementation of this procedure.

See P01 – Information Security Policy for team contacts.

4. Procedure

4.1. Review of Logs

Review of logs is to be carried out by means of **<COMPANY>**'s network monitoring system (**<COMPANY>** to define hostname), which is controlled from the **<COMPANY>** console (**<COMPANY>** to define hostname). The console is installed on the server (**<COMPANY>** to define hostname / IP address), located within the **<COMPANY>** data centre environment.

The following personnel are the only people permitted to access log files (**<COMPANY>** to define which individuals have a job-related need to view audit trails and access log files).

The network monitoring system software (**<COMPANY>** to define) is configured to alert **<COMPANY> [RESPONSIBLE TEAM]** to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to:

- A dashboard browser-based interface, monitored by **<COMPANY> [RESPONSIBLE TEAM]**.
- Email / SMS alerts to the **<COMPANY> [RESPONSIBLE TEAM]** mailbox with a summary of the incident. The **<COMPANY> [ROLE NAME]** also receives details of email alerts for informational purposes.

4.2. Review of Server Operating System Logs

The following Operating System Events are configured for logging, and are monitored by the console **(<COMPANY>** to define hostname):

- Any additions, modifications or deletions of user accounts.
- Any failed or unauthorised attempt at user logon.
- Any modification to system files.
- Any access to the server, or application running on the server, including files that hold cardholder data.
- Actions taken by any individual with Administrative privileges.
- Any user access to audit trails.
- Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

The process for restoring historical logs for analysis is **(<COMPANY>** to document the process for restoring historical logs for analysis).

4.3. Review of Oracle Database Audit Logs

The following Database System Events are configured for logging, and are monitored by the network monitoring system **(<COMPANY>** to define software and hostname):

- Any failed user access attempts to log in to the Oracle database.
- Any login that has been added or removed as a database user to a database.
- Any login that has been added or removed from a role.
- Any database role that has been added or removed from a database.
- Any password that has been changed for an application role.
- Any database that has been created, altered, or dropped.
- Any database object, such as a schema, that has been connected to.
- Actions taken by any individual with DBA privileges.

The process for restoring historical logs for analysis is **(<COMPANY>** to document the process for restoring historical logs for analysis).

4.4. Review of Firewall Logs

The following Firewall Events are configured for logging, and are monitored by the network monitoring system **(<COMPANY>** to define software and hostname):

- ACL violations.
- Invalid user authentication attempts.
- Logon and actions taken by any individual using privileged accounts.
- Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified).

The process for restoring historical logs for analysis is **(<COMPANY>** to document the process for restoring historical logs for analysis).

4.5. Review of Switches Logs

The following Switch Events are to be configured for logging and monitored by the network monitoring system **(<COMPANY>** to define software and hostname):

- Invalid user authentication attempts.
- Logon and actions taken by any individual using privileged accounts.
- Configuration changes made to the switch (e.g. configuration disabled, added, deleted, or modified).

The process for restoring historical logs for analysis is **(<COMPANY>** to document the process for restoring historical logs for analysis).

4.6. Review of Intrusion Detection Systems Alerts

The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system **(<COMPANY>** to define software and hostname):

- Any vulnerabilities listed in the Common Vulnerability Entry (CVE) database.
- Any generic attack(s) not listed in CVE.
- Any known denial of service attack(s).
- Any traffic patterns that indicated pre-attack reconnaissance occurred.
- Any attempts to exploit security-related configuration errors.
- Any authentication failure(s) that might indicate an attack.
- Any traffic to or from a back-door program.
- Any traffic typical of known stealth attacks.

The process for restoring historical logs for analysis is **(<COMPANY>** to document the process for restoring historical logs for analysis).

4.7. Review of File Integrity Monitoring System Logs

The following File Integrity Events are to be configured for logging and monitored by **(<COMPANY>** to define software and hostname):

- Any modification to system files.
- Actions taken by any individual with Administrative privileges.
- Any user access to audit trails.
- Any Creation / Deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

The process for restoring historical logs for analysis is **(<COMPANY>** to document the process for restoring historical logs for analysis).

4.8. Action to be Taken on Detection of Suspicious Events

For any suspicious event confirmed, the following must be recorded on F17 - Log Review Form, and the **<COMPANY> [ROLE NAME]** informed:

- User Identification.
- Event Type.
- Date & Time.
- Success or Failure indication.

- Event Origination (e.g. IP address).
- Reference to the data, system component or resource affected.

The process for restoring historical logs for analysis is **(<COMPANY>** to document the process for restoring historical logs for analysis).

4.9. Log Retention

Logs are recorded for a minimum period of 1 year, as defined in PR02 - Log Retention Procedure.

5. Enforcement

Any employee found to have violated this procedure will be subject to **<COMPANY>** disciplinary procedures, as detailed in the **<COMPANY>** Staff Handbook.

6. Glossary and References

6.1. Glossary

- **See "P99 - Glossary"**

6.2. References

- P01 - Information Security Policy
- PR02 - Log Retention Procedure
- F17 - Log Review Form