Securing of Audit Trails Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established a formal policy and supporting procedures concerning the securing of audit trails. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

The Office of Information Security will ensure that the time-synchronization technology policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Only individuals with a job-related need can view audit trail files.
- Current audit trail files are to be protected at all times from unauthorized modifications via access control mechanisms, physical segregation and/or network segregation.
- Audit trail files are to be promptly backed up to a centralized log server or media that is difficult to alter.
- Logs for external-facing technologies are to be written onto a secure, centralized, internal log server or media.
- Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the use of file-integrity monitoring or change-detection software on logs.

Responsibility for Policy Maintenance

The Office of Information Security is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019