Security Logs & Events 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 security logs & events. 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 Security Logs & Events 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):

- Authorized personnel are to review logs and security events on a daily basis for all system components for the purposes of identifying anomalies or suspicious activity.
- As such, the following items are to be reviewed by authorized personnel:
    - All security events
    - Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
    - Logs of all critical system components
    - Logs of all servers and system components that perform security functions.
- Additionally, authorized personnel are to perform the following:
    - Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.

  - Follow up on any exceptions and anomalies identified during the review process.

- Furthermore, all audit trail history files are to be retained for at least one year, with a minimum of three months immediately available for analysis.

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