Custom Application Code Audit 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 custom application code change reviews. 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 Custom Application Code Change Reviews 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):

- Code changes are reviewed by individuals other than the originating code author.
- Code changes are reviewed by individuals who are knowledgeable in code review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines, such as the Open Web Security Project Guide, as stated in Requirement 6.5, titled “Software Development Processes for Secure Coding Guidelines and Techniques”, and for any language-specific platforms utilized to develop internal systems and applications.
- Appropriate corrections are implemented prior to release of code.
- Code review results are reviewed and approved by management prior to release.

Furthermore, these activities relating to code changes may be done manually or automatically by the Office of Information Security.

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