Change Control 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 change control for security patches and software modifications. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

Change control has become a critical issue due in large part to regulatory compliance purposes and the need to fully document the change control process for accountability and tracking changes. As a result, all system components directly associated with the cardholder data environment and other IT resources that undergo changes must be documented accordingly. The Office of Information Security will ensure that Change Control policy and procedures adhere 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):

- Establishment of change control initiation, implementation and authorization directives.
- Establishment of a change control lifecycle.
- Establishment of minimum reporting criteria for change control documentation.
- Separation of duties, roles and responsibilities exist between the development/test environment(s) and production environment(s), complete with access controls in place.
- Production data with live Primary Account Numbers (PAN) are not to be used for testing or development.
- Test data and all associated accounts are removed before a production system becomes active.
- Documentation of impact is included in the change control documentation.

- Management approval by appropriate parties, along with approval for all stages of the change control lifecycle, is required for each change.
- Operational functionality testing is performed and must be documented for each change, where applicable so as to verify that the change does not adversely impact the security of the custom code changes.
- For custom code changes made, all updates and releases are tested for compliance with Requirement 6.5 before being released to production.
- Additionally, change controls policies, procedures, and supporting initiatives are to properly document the following:
    - Documentation of impact is included in the change control documentation for each sampled.
    - Documented approval by authorized parties is present for each sampled change.

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