Data Security Policy - Change and Configuration Management

PURPOSE

To provide principles and guidelines for managing changes and configurations at **Organization**, including code changes and infrastructure configurations.

SCOPE

The Change and Configuration Management Policy and Procedure will cover **Organization's:**

- Change management process, including code changes
- Configuration management process, including infrastructure configurations
- Separation of environments
- Unauthorized changes
- Roles and Responsibilities
- Related Forms, Plans, and Documents
- Related Policies
- Relevant Regulations, Standards, and Criteria

POLICY

Organization has and follows policies and procedures that govern how changes are made at Organization.

Change Management

These change management processes apply to all code and configuration changes made to production systems that contain or process sensitive or protected information, including *ePHI.*

Changes must be requested and authorized prior to being worked on.

Change Review and Approval

Before changes can be migrated to production, they must be reviewed and approved by an appropriate workforce member, such as a supervisor or peer. Change developers cannot approve their own changes or migrate them to production. As a result, only authorized changes should be present in production.

Configuration Management

Organization documents configuration standards for systems that contain or process sensitive or protected information, including *ePHI.* These configurations are periodically reviewed and updated based on Organization's needs, security best practices, and other changes that occur. These standards also serve as baselines for Organization.

Configuration Changes

Changes to configurations in production environments must follow Organization's change management process.

Separation of Environments

Organization must maintain separate environments for production and development, at minimum. Maintaining separate environments limits the possibility of unauthorized changes being made to production.

Secure Development Training

Organization provides secure development training and resources for developers and coders.

PROCEDURES

The Change and Configuration Management policy and procedure should be reviewed at least annually and updated to reflect changes as needed.

The Change and Configuration Management process should be initiated whenever a change or configuration change is required.

Change Management

Changes must be initiated and requested through a change ticket or form.

Workforce members who work on change requests follow their team's process for designing and developing changes. Organization allows the workforce to use both traditional and agile project management methods to meet objectives.

Changes are documented in a ticketing system or similar repository. Change ticket documentation includes:

- Change ID
- Change Requestor
- Title or Short Description of the Change
- Long Description of the Change
- Change Testing Evidence (i.e., descriptions, screenshots, and testing reports)
- Approver(s) and their Signoffs
- Approver or Reviewer Notes

Changes are tracked throughout the change management process.

Change Testing

Changes are manually and automatically tested whenever possible prior to changes being made to production. Tests may include User Acceptance Testing (UAT), automated code scanning, and other methods used to verify that the change meets the requirements in the documented request.

Evidence of change testing should be attached to the change ticket and must demonstrate that the change was developed successfully. Descriptions of tests, reports, and screenshots are all acceptable for evidence of change testing.

Testing is not performed in production environments.

Change Review and Approval for Migration

After changes are developed and tested, an appropriate workforce member, such as a supervisor, peer, or change manager, reviews all change documentation and ensures that the change process has been followed.

If the change is appropriate, meets the requirements of the change request, and does not pose other risks or security threats, the change will be approved and migrated to production in the next release cycle.

If the change does not meet the requirements of the change request, testing is insufficient, or the change poses additional risks or security threats that are not addressed, the change will be rejected. Rejected changes may be re-worked and re-submitted for approval once additional development and testing has occurred.

Only authorized workforce members may initiate a change release cycle. Developers are prohibited from migrating their own changes to production. Any changes migrated to production without sufficient testing or approval is an unauthorized change.

Configuration Management

Organization uses a configuration management toolset when possible, to orchestrate and manage configurations across Organization.

Configuration standards for all types of production infrastructure, applications, and devices are developed and maintained by system owners. These standards are kept in a repository that only authorized users can access.

Configuration standards are reviewed at least annually, and updated when changes occur, or as needed.

Configuration Changes

Configuration changes must be requested through a change request and follow the change management process. Configuration changes must also be tested, reviewed, and approved by appropriate and skilled workforce members prior to being implemented in production.

Configuration changes are not tested in production.

Emergency Changes

Emergency changes must be requested through the change request process. An authorized workforce member determines if the situation is truly an emergency. If the workforce member concludes that the situation warrants an emergency change, the change will be developed and implemented, possibly without obtaining approval beforehand.

Emergency changes must be reviewed within 5 business days, and approved within that timeframe, otherwise the emergency change will be reverted.

Unauthorized Changes

Organization has set up detection tools and mechanisms to detect unauthorized changes to systems, applications, or configurations. If unauthorized changes are detected, they must be reported as soon as possible through the Incident Response and Reporting process.

Separation of Environments

Organization has set up separate environments for development (Dev), testing and quality assurance (Test/QA), and production (Prod). Only a limited subset of users have access to make changes to production.

ROLES AND RESPONSIBILITIES

System Owner(s): Develop and maintain configuration standards for the systems, infrastructure, and applications they own. Review changes. May serve as a delegate to approve changes for migration to production.

FORMS/PLANS/DOCUMENTS

- Change Ticket or Form (Can Be Electronic)
- Configuration Standard(s)

RELATED POLICY

- Data Security Policy - Security Management
- Data Security Policy - Incident Response and Reporting

RELEVANT SOC 2 CRITERIA

- CC 8.1.1 *Manages changes throughout the system lifecycle*
- CC 8.1.2 *Authorizes changes*
- CC 8.1.3 *Designs and develops changes*
- CC 8.1.4 *Documents changes*
- CC 8.1.5 *Tracks system changes*
- CC 8.1.6 *Configures software*
- CC 8.1.7 *Tests system changes*
- CC 8.1.8 *Approves system changes*
- CC 8.1.9 *Deploys system changes*
- CC 8.1.10 *Identifies and evaluates system changes*
- CC 8.1.12 *Identifies changes in infrastructure, data, software, and procedures required to remediate incidents*
- CC 8.1.13 *Provides for changes necessary in emergency situations*
- CC 8.1.14 *Protects confidential information*
- CC 8.1.15 *Protects personal information*