# Configuration Management Policy

| | |
|---|---|
| **Document Classification:** | |
| **Document Ref.** | |
| **Version:** | **1** |
| **Date:** | |
| **Document Author:** | |
| **Document Owner:** | |

## Revision History

| Version | Date | Revision Author | Summary of Changes |
|---|---|---|---|
| | | | |
| | | | |

## Distribution

| Name | Title |
|---|---|
| | |
| | |
| | |

## Approval

| Name | Position | Signature | Date |
|---|---|---|---|
| | | | |

## Purpose

This policy establishes the $COMPANY$ Configuration Management Policy, for managing risks from system changes impacting baseline configuration settings, system configuration and security. The configuration management program helps document, authorize, manage and control system changes impacting Information Systems.

## Scope

The scope of this policy is applicable to all Information Technology (IT) resources within the boundaries of the $COMPANY$ Cardholder Data Environment. All users $COMPANY$ (Corporation employees, contractors, vendors or others) of the $COMPANY$ are responsible for adhering to this policy.

## Intent

The $COMPANY$ Corporation Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a configuration management capability throughout the $COMPANY$ for documenting, authorizing, managing, and controlling configuration changes which may occur across the enterprise environment.

## Change Control Board

The System Owner is responsible for oversight of the asset management policy and standards. The System Owner is responsible of assembling a Configuration Control Board (CCB) that represents the appropriate stakeholders. The $COMPANY$ CCB meets weekly. The System Owner or delegated official serves as the Authorizing Official (AO) to approve/reject the change. Approval of the change is to accept the risk of the change.

The Configuration Manager implements configuration management policy and standards. The configuration manager facilitates weekly Change Control Board meetings. The Information Security Officer will review changes to evaluate the security implications of the proposed changed. The Configuration Analyst facilitates impact assessments of proposed changes. The

Configuration Administrator provides information on the status of the configuration. The Configuration Administrators are responsible for providing details of baseline configuration. They will also review baseline configurations for accuracy.

The Configuration Control Board defines the configuration baselines, application information, infrastructure ensuring that they meet requirements. The CCB also reviews all changes for compliance with standards, contractual, and internal requirements. The CCB will track the minutes of the meeting and document the results of the vote for each configuration item. CCB decisions and minutes will be retained for a minimum of a year in the $COMPANY$ portal.

## $COMPANY$ Baseline

The objective of establishing a baseline is to define a basis to allow reference to, control of, and traceability among configuration items and requirements. It serves as a common reference point that all system development is built on. The $COMPANY$ Baseline configuration will be be stored in the $COMPANY$ portal. Access will be restricted to the configuration based on role.

The baseline configuration will be reviewed and updated after every change has been approved by the CCB and implemented by the change administrator. The Change administrator will update the baseline configuration. The $COMPANY$ tracks the revision history of the baseline up to 10 versions. The revision history is necessary for potential need to roll back to a last known good configuration baseline. The $COMPANY$ leverages an automated auditing tool to monitor the configuration items of the system to detect any unauthorized changes to the baseline. Where configuration items cannot be managed via automated tools, a repository of changes must be updated by the change administrator.

## Configuration Items

Configuration Items (CI) are defined as any system components necessary to deliver the $COMPANY$ service. Throughout the System Development Lifecycle, configuration items will be tracked in the $COMPANY$ Portal. System owners are responsible for insuring that CIs are up to date and documented. CIs are to be identified using the standard referenced in this document. CIs will be tracked using the configuration management process. The CI repository may only be accessed by authorized personnel.

## Software Use Restriction

Only approved software may be used within the $COMPANY$. Any software requiring licenses will be strictly regulated leveraging automated tools. Software may only be installed by authorized personnel.

## Software Configurable Items

Software Configurable Items consist of third party providers, custom developed applications, and open source software. Third party providers consist of $SERVICE PROVIDER$. Software consists of $SOFTWARE$. Each software configuration item for each product has an identifier assigned to it. The naming scheme is as follows:

<SystemID>_<ProductID>_<name/module>_<version> example
firewall1_V_DNS_2.0

## Hardware Configurable Items

The majority of the $COMPANY$ consists of hardware operated by third party vendors. There are few instances of support services that are managed by $COMPANY$ provided hardware. Hardware configurable items consist of type (server, network device), component (RAM, Power supply, CPU, etc), and location (HQ, Appleton, etc). Each hardware configuration item has an identifier assigned to it. The naming scheme is as follows:

<SystemID>_<Hardware type>_<component>_<location>
device_Svr_PSU_HQ

## Standard Changes

A standard change are changes that have been pre-approved by the CCB. These types of changes are routine and common. They do not require that the CCB convene to discuss the implication of the change every time they must be made. A list of standard changes will be managed in the $COMPANY$ portal.

## Emergency Changes

Emergency changes occur when security and/or availability of a service is impacted. The designated members of the Emergency Change Control Board (ECCB) are on call and available for convening 24 hours a day. They consist of the $ROLE$. They will review and authorize the change and submit to the CCB for further review.

## Change Access Restrictions

The $COMPANY$ deploys a Roles based access control policy. Changes may only be made by those authorized to conduct the change and/or manage the system. Access may be restricted on physical and/or logical level as necessary. System changes are audited as defined by the $COMPANY$ Audit and Accountability policy.

## Configuration Settings

All $COMPANY$ system components must be configured with a baseline security configuration. These configurations may be found in the $COMPANY$ Portal. These checklists insure a secure operating environment. The checklist implements systems in the most restrictive mode possible for the service operation. Systems may only perform functions essential for its operation (ie no unauthorized/unnecessary software). Deviations from the baseline must first undergo the configuration management process and obtain approval before implementation. The automated auditing process will monitor systems for unauthorized deviations from standard.

Software configuration settings are managed by a centralized system that deploys configuration changes and tracks revision history. The system will verify that configuration item change was successful.

## Operational Procedures

At a minimum the change control process will include documenting the following to present to the CCB:

- Formal written change request
- Identification, prioritization of change
- Requirements analysis
- Inter-dependency analysis
- Impact assessment

- Change approach
- Change test
- User acceptance testing/approval
- Implementation planning
- Documentation
- Change Monitoring
- Defined roles and responsibilities of the change
- Notification Plan

All change requests will be logged whether approved or rejected and stored in $COMPANY$ portal.

# Appendix A: Standard Changes

Below is a list of standard changes that do not need to be reviewed by the CCB. In order to add to this list, the CCB must review and approve it.

- System Patches
- Modifications to user accounts
- Modifications to e-mail addresses
- New Server builds
- Add RAM
- Add CPU
- Add Storage
- change Virtual machine Host/Storage
- Failover processes

# Appendix B: Roles and Responsibilities

| Name | Role | Description |
|---|---|---|
| | CM Process Owner/Manager | Responsible for process design, promote CM communication, update documentation, train staff on process, Responsible for process execution |
| | CM Process Sponsor | Authorizes CM policies and procedures |
| | CM Implementer | Implements changes |
| | Security Engineer | Assesses security implications of changes. |