Insert Logo Here

Organization Name

Security Procedure

Configuration Management

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published CM Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68600484)

[2 Purpose 1](#_Toc68600485)

[3 Scope 1](#_Toc68600486)

[4 Roles and Responsibilities 1](#_Toc68600487)

[5 Management Commitment 2](#_Toc68600488)

[6 Authority 3](#_Toc68600489)

[7 Compliance 3](#_Toc68600490)

[8 Procedural Requirements 4](#_Toc68600491)

[8.1 CONFIGURATION MANAGEMENT PLAN 4](#_Toc68600492)

[8.2 BASELINE CONFIGURATION 4](#_Toc68600493)

[8.3 SOFTWARE 4](#_Toc68600494)

[8.4 HARDWARE 4](#_Toc68600495)

[8.5 CONFIGURATION CHANGE CONTROL 5](#_Toc68600496)

[8.6 CONFIGURATION SETTINGS AND LEAST FUNCTIONALITY 6](#_Toc68600497)

[8.7 INFORMATION SYSTEM COMPONENT INVENTORY 7](#_Toc68600498)

[8.8 SECURITY IMPACT ANALYSIS 8](#_Toc68600499)

[8.9 ACCESS AND SOFTWARE USAGE RESTRICTONS 8](#_Toc68600500)

# Introduction

Organization Name has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by Organization Name management and in compliance with the Configuration Management family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

This document defines the information configuration management procedures. These procedures are in place to facilitate the implementation of the configuration management policy and associated controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems

# Scope

The provisions of these policies pertain to all Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **Individual or Group** | **Role** | **Responsibility** |
| --- | --- | --- |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for Organization Name information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Manager | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
|  | System Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization Name and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization Name Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these procedures is mandatory. It is Organization Name policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed annually by an external vendor to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Procedural Requirements

The following configuration management requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the Organization Name systems.

## CONFIGURATION MANAGEMENT PLAN

The *Configuration Management Plan* describes all roles, responsibilities, activities required to establish configuration requirements, identifies configuration items, establishes and controls configuration items, and manages configuration item baselines including configuration item status, reporting, and auditing.

Organization Name ensures the protection of the *Configuration Management Plan* from unauthorized disclosure and modification by implementing access permission restriction, role-based access and need to know permissions.

## BASELINE CONFIGURATION

Organization Name maintains configuration information for baseline software configurations to ensure consistency and reproducibility. Procedures involve the use {Tools} to harden systems and to establish configuration baselines. CIS benchmark compliance is verified using {Tool} Compliance scanning. Deviations from baselines are kept in the Organization Name {Repository} and reviewed annually or upon a request for change to a baseline setting.

## SOFTWARE

All software is documented in the StateRAMP inventory workbook that includes the software name and version information. Software baselines are captured by {Tool} and are checked in to the {Tool} as they become available. The following tasks are performed by the {Role} with oversight from the {Role/Team}:

* Receive, verify, and process the receipt of approved software licenses and license keys
* Establish a media library with restricted access
* Store vendor shipments of software media in the media library
* Store downloaded software from Vendor website in the software media library
* Establish software license tracking method
* Assign licenses and keys appropriately
* Track and report software license allocation
* Ensure that the configuration records are established when software moves to production
* Maintain software images for refresh or installation
* Conduct audits and reviews/updates of configuration item records for all software monthly

The {Role/Team} maintains the StateRAMP inventory workbook for standard software configurations and installations and ensures that updating the baseline configuration is integrated into these related functions.

## HARDWARE

Hardware configuration is inherited from {Insert SSP Information}

## CONFIGURATION CHANGE CONTROL

Organization Name controls change to the information system and infrastructure with logical access restrictions to ensure approved changes are only made by system administrators and/or system owners with appropriate permissions.

Access restrictions are enforced via role-based access control (RBAC) through security groups within Active Directory and assigned permissions to users. The system supports audits related to how access to the associated privileges is approved using the {Tool}.

Organization Name prevents installation of software components that are not approved for the environment by using {Tool}. New software installed on systems in the environment must be authorized by {Tool}. Methods of approving new software include update mode, checksum, digital signature, trusted path, updaters, or trusted user. The change management process is followed to install software on systems in the environment.

Organization Name will maintain a list of authorized software contained in the StateRAMP inventory workbook to be updated monthly. The list of authorized software is reviewed by {Role/Team} at least monthly or when there is a change. Organization Name employs a deny-all, permit-by-exception software execution policy by enforcing software restriction policy that prevents the execution of any unauthorized software.

The privilege to change information system components and information is limited to specific users. Organization Name follows an account request and approval process and account permissions are reviewed quarterly to ensure appropriate permissions are assigned to personnel by RBAC.

Configuration change control for the information system involves systematic proposal, justification, implementation, test and evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, and firewalls), emergency changes, and changes to remediate flaws.

The {Role/Team} will approve configuration-controlled changes to information systems with explicit consideration for security impact analyses. Before any approval for changes to the operational network, the {Role/Team} in coordination with the {Role/Team} will test, validate, and document those changes in accordance with the test plan in the change request. In the event of an emergency or expedited change, testing may not be completed prior to implementing the change.

The Change Management system documents approved configuration changes to the system. All proposed changes to the information system are reviewed by a peer post implementation and completed changes are reviewed again during change management meetings.

Organization Name coordinates and provides oversight for configuration change control activities through the Configuration Management Board that convenes weekly. Expedited changes, which are changes that need to be implemented to prevent an issue that cannot wait for the next Configuration Management Board meeting, are reviewed by the change management approvers through {Tool}. Emergency changes, which are changes to resolve a production issue, are automatically approved and communicated through the Change Management system to the change management approvers.

## CONFIGURATION SETTINGS AND LEAST FUNCTIONALITY

Organization Name maintains alignment with the information system settings defined by the Center for Internet Security Guidelines Level 1 Benchmark establishing a restrictive configuration of the information system. These configurations are:

* Documented in the Information System Baseline documentation
* Verified through {Tool} policy compliance scanning performed by {Tool} or the {Tool} Scanner Appliance

Various levels of automated configuration management tools have been implemented to maintain configuration compliance for information system components based on operational requirements. The {Role/Team} shall ensure that any exceptions are:

* Identified
* Documented in the Organization Name {Repository}
* Approved via a change record
* Explicitly Required

The following deviations are contained in separate systems:

* {Tool} deviations will be contained within the {Tool} system
* {Tool}

Organization Name employs the settings to centrally manage and apply the configuration settings. CIS Level 1 Benchmark compliance verification is performed through {Tool} Policy Compliance scanning.

The {Role/Team} conduct quarterly reviews to identify and disable or remove unnecessary functions, ports, protocols, and services. Any changes resulting from that review are identified, documented, and approved through the Organization Name Change Management process. Updates to the ports, protocols, and services are documented in the SSP.

Information systems are configured to prevent program execution in accordance with the Configuration Management Policy and regarding software program usage and restrictions as well as rules authorizing the terms and conditions of software program usage.

{Tool} Application Control is used to prevent program execution. {Tool} application Control has modes as documented below:

* **Enabled Mode:** systems in enabled mode will block the execution of new software
* **Update Mode:** systems in update mode will allow and automatically whitelist any applications that are running on the system while in update mode unless the application has previously been blacklisted
* **Observe Mode:** observe mode is used upon initial installation of {Tool} Application Control and is used to inventory and whitelist software initially installed on a system

{Tool} Application Control has a few methods of whitelisting software as described below:

* **Updaters:** can install new software and update existing software based on a file name
* **Approved Certificates:** can be configured to allow specific certificates to be whitelisted
* **Approved Installers:** can execute and update software on the endpoint and is approved based on the SHA-1 or SHA-256 checksum of the installer.
* **Approved (trusted) Directories:** allow software within a trusted directory path to run
* **Approved (trusted) Users:** accounts trusted to install or update any software
* **Approved executable files:** added manually based off file name, SHA-1 checksum or SHA-256 checksum

Organization Name monitors and controls change to the configuration settings to limit risk of deviation from approved system configuration. The following list of tools are used to control and monitor configuration changes:

* {Tool} **Configuration Manager:** used to deploy required software and apply security updates
* **Terraform:** used to deploy standardized build of servers in the environment
* **Desired State Configuration (DSC):** used to monitor and configure operating system settings compliance and avoid drift from the baseline configuration
* **Group Policy Objects (GPO):** used to control CIS benchmark compliance
* {Tool} **Policy Compliance:** used to monitor CIS benchmark compliance

## INFORMATION SYSTEM COMPONENT INVENTORY

Organization Name is responsible for developing, documenting, and maintaining an inventory of information system components that is consistent with the authorization boundary of the information system. All components within the authorization boundary of the information system are inventoried via {Tool} Asset View (software inventory, ports, protocols, services, and virtual machine system components). Results are compiled in the StateRAMP inventory workbook and are reviewed monthly.

Organization Name implements automated mechanisms to continuously monitor for the presence of unauthorized software components within the Organization Name SaaS authorization boundary. {Tool} Application Control is used to detect unauthorized software and alert the {Role/Team}. {Tool} Application Control blocks all new software on a system unless the software has been authorized through Application Control to run. Upon detection, the {Role/Team} will coordinate efforts with the {Role/Team} to decide what action should be taken on the new software. If the new malware is determined to be malicious in nature, the Incident Response Plan will be executed. Organization Name inventory workbook contains the following information:

* Unique Asset Identifier
* IPv4 or IPv6 Address
* Virtual
* Public
* DNS Name or URL
* NetBIOS Name
* MAC Address
* Authenticated Scan
* Baseline Configuration Name
* OS Name and Version
* Location
* Asset Type
* Hardware Make/Model
* In Latest Scan
* Software/ Database Vendor
* Software/ Database Name & Version
* Patch Level
* Function
* Comments
* Serial #/Asset Tag#
* VLAN/Network ID
* System Administrator/ Owner
* Application Administrator/ Owner

## SECURITY IMPACT ANALYSIS

The {Role/Team} analyzes new software before implementing in the production environment. Changes to the information system are all assessed to determine how security is impacted. This is done by reviewing information system documentation to understand how security controls are implemented and how the changes might affect the controls.

The security impact analysis includes a risk assessment to understand the impact of changes to determine if additional security controls are required.

## ACCESS AND SOFTWARE USAGE RESTRICTONS

Any changes to the software of the information system can potentially have significant effects on the overall security of the system. The {Role/Team} defines and documents logical access restrictions associated with changes to the information system. The Change Management Review Board approves changes to logical access restrictions for backend administration accounts and changes to account permissions are conducted through the account request process.

Organization Name takes steps to ensure software and associated documentation are used in accordance with contract agreements and copyright laws. These steps include tracking the use of software and associated documentation protected by quantity licenses to control copying and distribution via {Tool}.

The use of open-source software is restricted unless explicitly reviewed and approved by the Change Management Board.