Insert Logo Here

Organization Name

Security Policy

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 Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc60977237)

[2 Purpose 1](#_Toc60977238)

[3 Scope 1](#_Toc60977239)

[4 Roles and Responsibilities 1](#_Toc60977240)

[5 Management Commitment 2](#_Toc60977241)

[6 Authority 3](#_Toc60977242)

[7 Compliance 3](#_Toc60977243)

[8 Policy Requirements 4](#_Toc60977244)

[8.1 Configuration Management Policies and Procedures 4](#_Toc60977245)

[8.2 Baseline Configuration 4](#_Toc60977246)

[8.3 Configuration Change ControL 4](#_Toc60977247)

[8.4 Security Impact Analysis 5](#_Toc60977248)

[8.5 Access Restrictions for Change 5](#_Toc60977249)

[8.6 Configuration SettingS 6](#_Toc60977250)

[8.7 Least Functionality 6](#_Toc60977251)

[8.8 Information System Component Inventory 6](#_Toc60977252)

[8.9 Configuration Management Plan 7](#_Toc60977253)

[8.10 Software Usage Restrictions 7](#_Toc60977254)

[8.11 User Installed Software 7](#_Toc60977255)

# Introduction

has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by 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

The purpose of these policies is to establish configuration management requirements to ensure the confidentiality, integrity, and availability of systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

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

# Roles and Responsibilities

These policies apply to all employees, contractors, business partners, third parties, and others who need or have access to 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 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

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 system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the 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 policies is mandatory. It is 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.

# Policy 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 systems.

## Configuration Management Policies and Procedures

Every three (3) years, must develop, disseminate, review, and update the formal, documented *Configuration Management Policy* that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Likewise, the *Configuration Management Procedure* must be reviewed and updated at least annually or any time there is a significant change in software or security.

Updates must be made in accordance with overall business goals and risk position. The document(s) will be reviewed by the Information Owner. Any updates, improvements, or suggestions related to the policy and/or procedure should be sent to the Information Owner.

## Baseline Configuration

Organization Name has developed, documented, and maintained under configuration and control, a current baseline configuration of the information system. A review and update of the baseline configuration occur at the following times:

* At least annually or when a significant change occurs
* When required by the ISM, system owner, or when directed by the StateRAMP PMO.
* As an integral part of information system component installations and upgrades

Organization Name has also employed automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. Additionally, previous versions of baseline configurations of the information system are retained to support rollback.

For those individuals traveling to locations that the organization deems to be of a significant risk, information systems will be issued with a special configuration and security safeguards will be applied to the device(s) when the individual returns.

## Configuration Change ControL

Organization Name has implemented the requirements outlined below to manage the configuration change control process and related activities. In the event of a configuration change, the designated team of individuals will complete the following actions:

* Determine the types of changes to the information system that are configuration-controlled
* Review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses
* Document configuration change decisions associated with the information system
* Implement approved configuration-controlled changes to the information system

In addition, the following measures have been put in place to manage, track, communicate, and audit configuration change activities:

* Records of configuration-controlled changes to the information system are retained for at least one year
* Activities associated with configuration-controlled changes to the information system are audited and reviewed weekly.
* Oversight is coordinated for configuration change control activities through a Change Approval Board (CAB) that convenes at least bi-weekly to review and authorize configuration changes when change requests are pending
* All major changes are communicated to the authorizing official (AO)
* A central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the government and associated service consumers (e.g., RSS feed, web status page) has been established

## Security Impact Analysis

analyzes all changes to the information system to determine potential security impacts prior to change implementation.

## Access Restrictions for Change

Pertaining to user access and access restrictions in relation to changes, will:

* Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system
* Ensure that the information system enforces access restrictions and supports auditing of the enforcement actions
* Ensure that the information system prevents the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization (if digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used)
* Limit privileges to change information system components and system-related information within a production or operational environment
* Review and reevaluate privileges at least quarterly

## Configuration SettingS

has established and documented configuration setting for information technology products employed within the information system using the FedRAMP Requirements and Guidance that reflect the most restrictive mode consistent with operational requirements, including:

* The use of Center for Internet Security (CIS) guidelines and Level 1 Benchmarks to establish configuration setting or establish its own configuration setting if CIS setting are not available
* Ensuring checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible if the validated checklists are not available

has implemented configuration settings based on the aforementioned requirements and will execute the following activities on an ongoing basis:

* Identify, document, and approve any deviations from established configuration settings for components based on operational requirements
* Monitor and control changes to the configuration settings in accordance with organizational policies and procedures
* Employ automated mechanisms to centrally manage, apply, and verify configuration settings for components

## Least Functionality

must maintain an information system configuration that allows only essential capabilities. The use of the functions, ports, protocols, and/or services identified in the CIS Level 1 Benchmark are prohibited or restricted.

The information system must be reviewed at least monthly to identify unnecessary and/or nonsecure functions, ports, protocols, and services. Ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure will be disabled.

The information system must prevent program execution in accordance with policies regarding software program usage and restrictions or rules authorizing the terms and conditions of software program usage.

employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system. The list of authorized software programs must be reviewed and updated at least quarterly or when there is a change.

## Information System Component Inventory

has developed and documented an inventory of information system components that:

* Accurately reflects the current information system
* Include all components within the authorization boundary of the information system
* Is at the level of granularity deemed necessary for tracking and reporting
* Include information deemed necessary to achieve effective information system component accountability

Additionally, the InfoSec and IT team will complete the following activities on a monthly basis to ensure an accurate and secure system component inventory:

* Review and update the information system component inventory at least monthly or when there is a change
* Update the inventory of information system components as an integral part of component installations, removals, and information system updates
* Employ automated mechanisms with a maximum five-minute delay in detection running on a continuous basis to detect the presence of unauthorized hardware, software, and firmware components within the information system
* When unauthorized components are detected, either disable network access by such components or isolate the components and notify appropriate personnel or roles
* Verify that all components within the authorization boundary of information system are not duplicated in other information system inventories

## Configuration Management Plan

has developed, implemented, and maintains a configuration management plan for information systems that:

* Addresses roles, responsibilities, and configuration management processes and procedures
* Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items
* Defines the configuration items for the information system and places the configuration items under configuration management
* Protects the configuration management plan for unauthorized disclosure and modification

## Software Usage Restrictions

must use software and associated documentation in accordance with contract agreements and copyright laws. The use of software must be tracked, and associated documentation protected by quantity licenses to control copying and distribution.

controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Additional restrictions have been placed on the use of open source software as applicable.

## User Installed Software

has established restrictions on unauthorized software usage by users and has enforced software installation policies through whitelisting. Policy compliance is monitored continuously.