

GovRAMP

{Insert Company Name}

Security Policy

Configuration Management

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

Table of Contents[Document Revision History 1](#_Toc196396926)

[1 Introduction 3](#_Toc196396927)

[2 Purpose 3](#_Toc196396928)

[3 Scope 3](#_Toc196396929)

[4 Roles and Responsibilities 3](#_Toc196396930)

[5 Management Commitment 4](#_Toc196396931)

[6 Authority 5](#_Toc196396932)

[7 Compliance 5](#_Toc196396933)

[8 Policy Requirements 5](#_Toc196396934)

[8.1 Configuration Management Policies and Procedures [CM-1] 5](#_Toc196396936)

[8.2 Baseline Configuration [CM-2, CM-2 (2,3)] 6](#_Toc196396937)

[8.2.1 Configure Systems and Components for High-Risk Areas [CM-2 (7)] 6](#_Toc196396938)

[8.3 Audit Storage Capacity [CM-3, CM-3 (2,4), {CM-3 (1,6) High Only}] 7](#_Toc196396939)

[8.4 Impact Analysis [CM-4, CM-4 (2), {CM-4 (1) High Only}] 7](#_Toc196396940)

[8.5 Access Restrictions for Change [CM-5, CM-5 (1,5)] 8](#_Toc196396941)

[8.6 Configuration Settings [CM-6, CM-6 (1), {CM-6 (2) High Only}] 8](#_Toc196396942)

[8.7 Least Functionality [CM-7, CM-7 (1,2,5)] 9](#_Toc196396943)

[8.8 System Component Inventory and Information Location [CM-8, CM-8 (1,3), {CM-8 (2,4) High Only}] 9](#_Toc196396944)

[8.9 Configuration Management [CM-9] 10](#_Toc196396945)

[8.10 Software Usage Restrictions [CM-10] 10](#_Toc196396946)

[8.11 User Installed Software [CM-11] 11](#_Toc196396947)

[8.12 Information Location [CM-12, CM-12 (1)] 11](#_Toc196396948)

[8.13 Signed Components [{CM-14 High Only}] 11](#_Toc196396949)

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s 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 5.

# Purpose

The purpose of these policies is to establish Configuration Management requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s 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 {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

| **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 {Insert Company 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. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | 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 Director | 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 Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company 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 {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company 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
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. 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 {Insert Company Name}’s 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 by an external vendor and/or internal self-assessments 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 controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

8.1 Configuration Management Policies and Procedures [CM-1]

This document is intended to serve as the *Configuration Management Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Configuration Management Policy* and related controls have been developed, documented, and disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [CM-1 (a)]

* An organizational-level Configuration Management Policy that: [CM-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [CM-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [CM-1 (a) (1) (b)]
* Procedures to facilitate the implementation of Configuration Management Policy and the associated Configuration Management controls [CM-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Configuration Management policy and procedures. [CM-1 (b)]

{Insert Company Name} must review and update the current Configuration Management: [CM-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [CM-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [CM-1 (c) (2)]

8.2 Baseline Configuration [CM-2, CM-2 (2,3)]

As {Insert Company Name} has developed, documented, and maintains under configuration control, a current baseline configuration of the information systems. [CM-2 (a)]

A review and potential update of the baseline configuration occurs at the following times: [CM-2 (b)]

* At least annually or when a significant change occurs (defined by NIST SP 800-37 r2, Appendix F)
* When required by the Information Security Manager (ISM), system owner, or when directed by the government agency Authorizing Official (AO) or the StateRAMP Approvals Committee (SAC)
* As information system components are installed or upgraded

{Insert Company Name} must utilize automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. [CM-2 (2)] Additionally, the previous version of the baseline configuration of the information system shall be retained to support rollback. [CM-2 (3)]

8.2.1 Configure Systems and Components for High-Risk Areas [CM-2 (7)]

For those individuals traveling to locations that the organization deems to be of a significant risk, no systems, system components or devices will be issued to individuals with unencrypted media. [CM-2 (7) (a)] Employees must obtain permission from Corporate Information Security management and their Senior Leadership Executive prior to traveling outside of the United States with company equipment.

If the employee is traveling to an area deemed to be of significant risk, the employee may be issued an encrypted, “bare-bones loaner” system while traveling. Known good manufacturer firmware will be applied, and, when applicable, a replacement hard drive may be installed in the device(s) when the individual returns. [CM-2 (7) (b)]

8.3 Audit Storage Capacity [CM-3, CM-3 (2,4), {CM-3 (1,6) High Only}]

{Insert Company Name} has established the requirements outlined below to manage the configuration change control process and related activities. In the event of a configuration change, the designated personnel will complete the following actions:

* Determine and document the types of changes to the information system that are configuration-controlled [CM-3 (a)]
* Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses [CM-3 (b)]
* Document configuration change decisions associated with the information system [CM-3 (c)]
* Implement approved configuration-controlled changes to the information system [CM-3 (d)]
* Retain records of configuration-controlled changes to the system for at least one (1) year [CM-3 (e)]
* Monitor and review activities associated with configuration-controlled changes to the system [CM-3 (f)]
* Coordinate and provide oversight for configuration change control activities through a Change Management Board (CMB) that convenes at least weekly to review and authorize configuration changes when change request are pending [CM-3 (g)]
* Test, validate, and document changes to the system before finalizing the implementation of the changes [CM-3 (2)]
* An Information Security Manager or delegated member of the Information Security Team must be a member and present at the CMB [CM-3 (4)]

**For high impact systems only:**

{Insert Company Name} must ensure that cryptographic mechanisms used to provide all security safeguards that rely on cryptography are under configuration management. [CM-3 (6)] {Insert Company Name} must also use automated mechanisms to:

* Document proposed changes to the system [CM-3 (1) (a)]
* Notify the appropriate personnel of proposed changes to the system and request change approval [CM-3 (1) (b)]
* Highlight proposed changes to the system that have not been approved or disapproved monthly [CM-3 (1) (c)]
* Prohibit changes to the system until designated approvals are received [CM-3 (1) (d)]
* Document all changes to the system [CM-3 (1) (e)]
* Notify the Configuration Management Board (CMB) when approved changes to the system are completed [CM-3 (1) (f)]

8.4 Impact Analysis [CM-4, CM-4 (2), {CM-4 (1) High Only}]

{Insert Company Name} must analyze all changes to an information system to determine potential security impacts prior to change implementation. [CM-4] After system changes, {Insert Company Name} must verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regards to meeting the security and privacy requirements for the system. [CM-4 (2)]

**For high impact systems only:**

{Insert Company Name} must analyze changes to the system in a separate test environment that simulates an operational environment, ensure that the controls that have been implemented have not impacted the security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice. [CM-4 (1)]

8.5 Access Restrictions for Change [CM-5, CM-5 (1,5)]

{Insert Company Name} must:

* Define, document, approve, and enforce physical and logical access restrictions associated with changes to information systems [CM-5]
* Ensure that information systems automatically 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 certificates are unavailable, alternative cryptographic integrity checks, for example, hashes or self-signed certificates may be used. [CM-5 (1) (a)]
* Ensure that information systems automatically generate audit records of the enforcement actions [CM-5 (1) (b)]
* Limit privileges to change information system components and system-related information within a production or operational environment [CM-5 (5) (a)]
* Review and reevaluate privileges at least quarterly [CM-5 (5) (b)]

8.6 Configuration Settings [CM-6, CM-6 (1), {CM-6 (2) High Only}]

{Insert Company Name} must establish and document configuration settings for information technology products employed within its information systems that reflect the most restrictive mode consistent with operational requirements. {Insert Company Name} shall: [CM-6 (a)]

* Use industry standard configuration settings baselines in the following order of preference:

*Choose the highest-ranking baseline in the list below. If no configuration setting baselines are available, the last option in this list must be used.*

1. DoD DISA STIGs
2. Center for Internet Security (CIS) Level 2 benchmarks
3. Center for Internet Security (CIS) Level 1 benchmarks
4. A customized {Insert Company Name} baseline configuration benchmark

Example: If baselines (a) and (b) are unavailable, baseline (c) shall be used.

NOTE: If a baseline is not available for the version of a product in use, it is acceptable to use the baseline configuration guidelines from a prior version.

* Ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or create a SCAP compatible checklist if validated checklist is not available
* Implement configuration settings for information system components based on the operational requirements [CM-6 (b)] Identify, document, and approve any deviations from established configuration settings for all components based on operational requirements [CM-6 (c)]
* Monitor and control changes to the configuration settings in accordance with {Insert Company Name} policies and procedures [CM-6 (d)]
* Manage, apply, and verify configuration settings for information system components using automated baseline tools including configuration tools and monitoring tools [CM-6 (1)]

**For high impact systems only:**

{Insert Company Name} shall respond to any unauthorized changes to baseline configuration settings by:

* Alerting designated configuration and security personnel,
* Restoring established configuration settings, or
* In extreme cases, halting affected information system processing.

Beyond restoring configuration settings, actions taken will be based on the nature of the discovered event and may require invoking the Incident Response Plan (IRP), which could require additional actions. [CM-6 (2)]

8.7 Least Functionality [CM-7, CM-7 (1,2,5)]

{Insert Company Name} must:

* Maintain information system configurations that allows only essential capabilities. [CM-7 (a)]
* Prohibit or restrict the use of functions, ports, protocols, and/or services in accordance with Section 8.6 Configuration Settings. [CM-7 (b)]
* Review information systems at least annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services [CM-7 (1) (a)]
* Disable or remove unnecessary and/or nonsecure functions, ports, protocols, software, and services within information systems [CM-7 (1) (b)]
* Configure information systems to prevent unauthorized software programs from execution in accordance with policies, restrictions, or rules authorizing software usage. [CM-7 (2)]
* Identify the minimum required configuration necessary for operating information systems [CM-7 (5) (a)]
* Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information systems. [CM-7 (5) (b)]
* Review and update the list of authorized software programs at least quarterly or when there is a change. [CM-7 (5) (c)]

8.8 System Component Inventory and Information Location [CM-8, CM-8 (1,3), {CM-8 (2,4) High Only}]

{Insert Company Name} must develop and document an inventory of information system components that: [CM-8 (a)]

* Accurately reflects the current information system [CM-8 (a) (1)]
* Includes all components within the authorization boundary of the information system [CM-8 (a) (2)]
* Does not include duplicate accounting of components or components assigned to any other information system [CM-8 (a) (3)]
* Is at the level of granularity deemed necessary for tracking and reporting [CM-8 (a) (4)]
* Includes information deemed necessary to achieve effective information system component accountability [CM-8 (a) (5)]
* Is reviewed and updated at least monthly [CM-8 (b)]

{Insert Company Name} must:

* Update the inventory of system components as part of component installations, removals, and system updates [CM-8 (1)]
* Employ automated mechanisms to continuously detect the presence of unauthorized hardware, software, and firmware components within information systems with a maximum five-minute delay in detection running on a continuous basis [CM-8 (3) (a)]
* Take situationally appropriate actions when unauthorized components are discovered. Appropriate actions may include: [CM-8 (3) (b)]
  + Disabling network access on the discovered components
  + Isolating the discovered components
  + Notifying the appropriate Technology Team for further actions on the discovered components

**For high impact systems only:**

{Insert Company Name} must:

* Maintain the currency, completeness, accuracy, and availability of the inventory of system components using a combination of system component inventory and baseline configuration activities [CM-8 (2)]
* Include in the system component inventory, a means for identifying the position and role of individuals responsible and accountable for administering those components [CM-8 (4)]

8.9 Configuration Management [CM-9]

{Insert Company Name} must develop, implement, and maintain configuration management plans for information systems.

For systems that store or process Federal or State government data, the plan must follow NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, Appendix D and: [CM-9]

* Address roles, responsibilities, and configuration management processes and procedures [CM-9 (a)]
* Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items [CM-9 (b)]
* Define the configuration items for the information systems and places the configuration items under configuration management [CM-9 (c)]
* Must be reviewed and approved the Information Security Manager. [CM-9 (d)]
* Must be protected from unauthorized disclosure and modification. [CM-9 (e)]

8.10 Software Usage Restrictions [CM-10]

{Insert Company Name} must:

* Use software and associated documentation in accordance with contract agreements and copyright laws. [CM-10 (a)]
* Track the use of software and associated documentation protected by quantity licenses to control copying and distribution [CM-10 (b)]
* Control and document 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 [CM-10 (c)]
* Require the approval of the use of open-source software that takes the following into consideration prior to approval: [CM-10 (1)]
  + Licensing model
  + Redistribution entitlements/restrictions
  + Attribution requirements
  + Active maintenance of the project
  + Availability of source code

8.11 User Installed Software [CM-11]

{Insert Company Name} requires installed software to be on the Active Software Catalog list. [CM-11 (a)] {Insert Company Name} must enforce software installation policies through role-based access control that allows only authorized administrators to install software. [CM-11 (b)] {Insert Company Name} must continuously monitor compliance with the user installed software policies. [CM-11 (c)]

8.12 Information Location [CM-12, CM-12 (1)]

{Insert Company Name} must identify and document the location where sensitive information is processed and stored. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood. Adequate protection and policy management must be provided for sensitive information and system components. The security category of information is also a factor in determining the controls necessary to protect the information and the system component where the information resides. [CM-12 (a)]

{Insert Company Name} must:

* Identify and document users who have access to information systems and information system components where information is processed and stored. [CM-12 (b)]
* Document changes to the location where the information is processed and stored. [CM-12 (c)]
* For Federal and State government data, Knowledge Service must also:
  + Store and process data in accordance with *FedRAMP Authorization Boundary Guidance* or *StateRAMP Authorization Boundary Guidance* [CM-12]
  + Use automated tools to identify government data and system data that must be protected at the High or Moderate impact levels on {Insert Company Name} information systems to ensure controls are in place to protect organizational information and individual privacy [CM-12 (1)]

8.13 Signed Components [{CM-14 High Only}]

**For high impact systems only:**

{Insert Company Name} must prevent the installation of unauthorized software and firmware without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. Alternative cryptographic integrity checks can be utilized if digital signatures or certificates are not available. [CM-14]