

{Insert CompanY Name}

Security Procedures

Configuration Management [CM]

**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

1 Introduction ............................................................................................................................................. 1

2 Purpose .................................................................................................................................................... 1

3 Scope ........................................................................................................................................................ 2

4 Roles and Responsibilities ........................................................................................................................ 2

5 Management Commitment ..................................................................................................................... 2

6 Authority .................................................................................................................................................. 3

7 Compliance .............................................................................................................................................. 3

8 Procedural Requirements [CM-1] ............................................................................................................ 4

8.1 Configuration Management Plan [CM-9] ......................................................................................... 4

8.2 Baseline Configuration [CM-2, CM-2 (2,3,7)] ................................................................................... 4

8.2.1 DISA STIG Updates ...................................................................................................................... 5

8.2.2 {Insert Product Name} Information System Dependencies .............................................................................. 5

8.2.3 Documentation Updates ............................................................................................................ 6

8.2.4 Software ..................................................................................................................................... 6

8.2.5 Hardware .................................................................................................................................... 6

8.2.6 Configure Systems and Components for High-Risk Areas .......................................................... 6

8.3 Configuration Change Control [CM-3] .............................................................................................. 7

8.4 Configuration Settings and Least Functionality [CM-6, CM-7] ......................................................... 9

8.5 Information System Component Inventory [CM-8] ....................................................................... 10

8.6 Security Impact Analysis [CM-4] ..................................................................................................... 11

8.7 Access Restrictions [CM-5] ............................................................................................................. 11

8.8 Software Usage Restrictions [CM-10] ............................................................................................ 12

8.9 User-Installed Software [CM-11] .................................................................................................... 13

8.10 Information Location [CM-12, CM-12 (1)] ................................................................................... 13

# 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 Access Control 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 access control 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. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | 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.

# Procedural Requirements [CM-1]

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 {Insert Company Name} information systems.

8.1 Configuration Management Plan [CM-9]

A Configuration Management Plan (CMP) describes all roles, responsibilities, activities required to establish configuration requirements, identify configuration items, establish and control configuration items, and manage configuration item baselines including configuration item status, reporting, and auditing. [CM-9 (a)] {Insert Company Name} has developed, documented, and implemented a CMP to manage and monitor configurations of the components that make up the {Insert Product Name} Information System. The latest version of the {Insert Company Name} CMP is reviewed and approved by the Information Security Manager, [CM-9 (d)]. The CMP defines:

* A process for identifying configuration items for the information system in operations, as well as in the System Development Life Cycle (SDLC) process [CM-9 (b)]
* Roles and responsibilities with regards to configuration management processes
* The overall configuration management operational policy and processes

Configuration items are documented and tracked within the {Insert Company Name} {Configuration Management Tool} module. All changes to the configuration items in the {Insert Product Name} Information System must go through the {Insert Company Name} Change Management Process. The configuration items in the {Insert Product Name} Information System can be linked to change requests as changes are planned and implemented. [CM-9 (c)]

{Insert Company Name} ensures the protection of the CMP from unauthorized disclosure and modification by implementing role-based access control based on need-to-know permissions. [CM-9 (e)] The CMP is only accessible to authorized {Insert Company Name} personnel supporting the {Insert Product Name} Information System. The CMP is stored in {Location of Documentation} to prevent unauthorized disclosure and modification. Only authorized personnel whose roles pertain to the {Insert Product Name} Information System have access to the CMP.

8.2 Baseline Configuration [CM-2, CM-2 (2,3,7)]

{Insert Company Name} maintains configuration information for baseline software configurations to ensure consistency and reproducibility.

{Insert Company Name} develops, documents, and maintains under configuration control, a current baseline configuration in the {Insert Hosting provider} portal. [CM-2 (a)] This is achieved by utilizing several tools, including {List tools utilized}.

{Insert Company Name} uses {Describe the Configuration Management Tool used to provision the network, servers, load balancers and components}. {Configuration Management Tool Name} applies desired state configuration settings, such as joining Virtual Machines to {Directory Service} domain and installing the required client agents such as {SIEM Tool}. {Insert Company Name} uses {Configuration Management Tool(s)} to maintain an up to date, complete, accurate, and readily available baseline configuration of the {Insert Product Name} Information System. [CM-2 (2)] {Insert Company Name} retains the previous version of the {Configuration Management Tool(s)} of the {Insert Product Name} Information System baselines in the {Directory Service Tool}. [CM-2 (3)]

{Insert Company Name} uses the DISA STIGs to harden the system. DISA STIGs for {OS System} are configured as {Directory Services Tool(s)}, which enforce baseline configuration of the {Insert Device Type} within the authorization boundary. The {Configuration Management Tool} are developed from the DISA STIGs. The {Insert Company Name} Information Security Team verifies the DISA STIGs are in place utilizing {Insert Device Name} Scans. {Insert Device Name} Scans are reviewed monthly to verify compliance with DISA STIGs and any non-compliances are documented within the Plan of Actions and Milestones (POA&M).

{Insert Company Name} additionally leverages {Configuration Management Tool(s)} to enforce baseline configuration settings. The {Directory Service Tool} then applies the group policy and installs the {Configuration Management} agent, which applies further configurations.

{Configuration Management Tool(s)} is used to deploy baseline management agents such as the {Directory Service Tool(s)} to systems in the environment. {Configuration Management Tool(s)} is also used to maintain and update {Insert Device Operating System and Components}, features, and settings.

The IT Team reviews and updates the {Insert Product Name} Information System’s baseline configuration at the following intervals: [CM-2 (b)]

* On at least an annual basis or when a significant change occurs [CM-2 (b) (1)]
* When required by the Information Security Manager, system owner, or when directed by the AO or StateRAMP Approvals Committee (SAC) [CM-2 (b) (2)]
* As information system components are installed or upgraded [CM-2 (b) (3)]

8.2.1 DISA STIG Updates

The Information Security Team, at least annually, will obtain the latest DISA STIG benchmarks for the components of the {Insert Product Name} Information System from the DOD Cyber Exchange website at <https://public.cyber.mil/stigs/>. If there are no updates to the DISA STIGs since the last review, the baseline configuration document revision table is updated to reflect that the annual check was performed, and the revision number is updated.

If there are updates (additions or subtractions) to the DISA STIGs, the updates are identified and tested for compatibility with the {Insert Product Name}. If the updates are deemed compatible, the updates are reflected in the configuration baseline document, taken through Change Management Board, and implemented. If the updates are found to be incompatible, either (i) the issue causing the incompatibility is remediated and the new benchmark is applied, or (ii) a deviation request is created to document the exception and the deviation request is documented in the POA&M. [CM-2 (b)]

8.2.2 {Insert Product Name} Information System Dependencies

As changes to the {Insert Product Name} and supporting infrastructure are proposed, the proposed changes are reviewed by the IT Team to determine if the proposed change modifies the baseline configuration. Any change to the baseline configuration of the {Insert Product Name} Information System requires updates to be reflected in the configuration baseline document and taken through Change Management Board prior to implementation.

On at least an annual basis, the baseline configuration documentation will be reviewed for accuracy and updated regardless of if there are dependency additions to the baseline configuration. The Information Security team, the IT team and the Development team review the configuration baseline document to ensure the listed dependencies are still needed. If a dependency is no longer needed, it will be presented to the Change Management Board for removal. If approved by the Change Management Board and removed, the baseline configuration documentation will be updated to reflect the component removal after completion of the change.

8.2.3 Documentation Updates

During the annual review, regardless of whether there are changes to the baseline configuration or not, the revision table of the baseline configuration document and the revision number of the baseline configuration document is updated to reflect the review.

8.2.4 Software

All software is documented monthly in an inventory workbook that includes the software name and version information. Software baselines are captured by {Directory Service Tool(s)} and are checked in to the {Configuration Management Tool(s)} as they become available. The following tasks are performed by the {Configuration Management Tool(s)} with oversight from the Information Security team:

{Examples may include}

* {Receive, verify, and process the receipt of approved software licenses and license keys}
* {Establish a media library with restricted access}

The {Insert Role(s) Name} maintains the inventory workbook for standard software configurations and installations and ensures that updating the baseline configuration is integrated into these related functions. The procedure to produce the inventory workbook, {Describe the Method and Location}.

8.2.5 Hardware

Hardware configuration {May be on property or inherited from CSP}.

8.2.6 Configure Systems and Components for High-Risk Areas

Individuals traveling to locations that are deemed to be of significant risk {Describe the process of securing company owned devices if applicable}. [CM-2 (7) (a)] {Describe steps and permissions an individual is required to do} prior to traveling outside of the United State with company equipment.

Individuals traveling to an area deemed to be of significant risk may be issued an encrypted loaner client operating system while traveling. {What steps if any are taken upon Individual and equipment returning to ensure device(s) are safe and secured prior to reintegration into the company network}. [CM-2 (7) (b)]

8.3 Configuration Change Control [CM-3

Configuration change control 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 and changes to the configuration settings for information technology products (e.g., operating systems, applications, and firewalls).

{Insert Company Name} Change Management Board (CMB) controls changes to the information system and infrastructure. All changes are documented and tracked in a {Insert Company Name} IT Software Management {Directory Service Tool(s)} change request and communicated to the appropriate personnel. All changes are considered “under configuration control” within the {Insert Product Name} Information System. [CM-3 (a)]

The CMB meets at least weekly to coordinate and review any proposed changes to the {Insert Product Name} Information System. [CM-3 (g)] The CMB reviews all proposed change requests and either approves or denies the proposed change with explicit consideration for security impact. [CM-3 (b)] The CMB consists of {Insert list of board members, such as Development, IT, and Information Security Managers} or their delegates as well as the Change Reviewer. [CM-3 (4)] CMB members may invite other team members as needed for additional review or clarification based on the components that could potentially be affected. The requester or a delegate must be present to discuss the change and any security implications during the meeting. All change request decisions are documented by the Change Reviewer in the {Directory Service Tool(s)}. [CM-3 (c)]

All changes are tracked in the {Directory Service Tool(s)} Change Management system and are retained indefinitely. The {Configuration Management Tool(s)} is used to manage the change control process including the following change types:

{Modify list below, per organization requirements}

* Normal Change Request: A Normal Change Request is the default change request type and is submitted for most changes to the environment aside for the cases documented below (Expedited, Emergency, and Routine Change Requests). A Normal Change Request must include the following information: short description, detailed description, justification, requested by, priority, implementer, category, implementation plan, test plan, backout plan, communication plan, business impact, risk, expectations for a production outage, and an event schedule for the planned change. Normal Change Requests are reviewed through the weekly CMB meeting and scheduled in advance of the change being implemented.
* Expedited Change Request: These are to prevent a possible outage or security requirement {Describe Current Process}.
* Emergency Change Request: These are in the event of an outage {Describe Current Process}.
* Routine Change Request: These are low-risk changes. {Describe Current Process}.

Before the change is implemented and finalized, it is tested and verified (validated) by a peer for success or failure and documented within the change record. If the change is tested but fails, the documented change backout plan is followed. Once each change stage is finished, the change stage is marked complete within the change request. Once all change stages are complete, the change request is closed. A final peer review is required to be performed after implementation to ensure the completed changes to the system component configurations are altered in accordance with the associated change request. The change and any implementation notes are reviewed at the next CMB meeting. [CM-3 (2)] Once the CMB approves the change request, the {Insert Role(s)} personnel responsible for the component implements the change. [CM-3 (d)] If the change is implemented but fails, the documented change backout plan is followed. Once each backout change stage is finished, the change stage is marked complete within the change request. Once all backout change stages are complete, the change request is closed. A peer review is required to be performed after implementation to ensure the completed changes to the system component configurations are altered in accordance with the associated change request. The change and any implementation notes are reviewed at the next CMB meeting. All change records and included notes/comments are retained within the {Directory Service Tool(s)} for at least one year. [CM-3 (e)]

{Insert Role(s)} monitors and controls changes to the configuration settings to limit risk of deviation from approved system configuration. [CM-3 (f)] The following list of tools are used to control and monitor configuration changes:

{Modify list below, per organization requirements}

* {Configuration Management Tool(s)}**:** used to deploy required software and apply security updates
* {Method}**:** used to deploy standardized build of servers in the environment
* {Directory Service Tool(s)}**:** used to monitor and configure operating system settings compliance and avoid drift from the baseline configuration
* {SIEM Tool(s)}**:** to centrally log and review audit logs and events

8.4 Configuration Settings and Least Functionality [CM-6, CM-7]

{Insert Company Name} establishes and documents system hardening settings for all {Insert Product Name} components in {Insert Company Name}’s secure {Insert Location} repository. [CM-6 (a)] Systems are configured {Describe Level of equipment hardening} to restrictive mode consistent with operational requirements, unless unavailable. If the DISA STIGs are not available for a particular system, operating system, or system component, {Insert Company Name} adheres to the following order of preference for implementing industry standard configurations:

* 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.

Implementation of the DISA STIG configurations are validated monthly using {Describe SIEM Tool(s) or Product used while running} Security Content Automation Protocol (SCAP) Auditor module. [CM-6 (b)] Various levels of automated configuration management tools have been implemented to maintain configuration compliance for information system components based on operational requirements. [CM-6 (1)] Operating System configuration settings {DISA STIGs, CIS Level 1 or 2 Benchmarks, or describe customized baseline configuration benchmark} (DISA STIGs) are implemented using {Directory Service Database}. Non-Operating System components {e.g., such as IIS and SQL Server} configuration settings are implemented through their respective management tools.

The Information Security Team identifies, documents, and approves deviations with justification from the established baseline configuration settings. [CM-6 (c)] All benchmark deviations are documented in the {Directory Service Database} with supporting evidence (for example, screenshots proving a false positive or a detailed operational requirement write up) stored in {Directory Service Database}. Benchmark deviations are also documented as Plan of Actions and Milestones (POA&Ms) entries for tracking agency approval as operationally required, false positive, or adjusted risk rating.

The {Insert Product Name} Information System is configured to provide only the necessary capabilities for proper operation of the system to include necessary functions, ports, protocols, and services. [CM-7 (a)] [CM-7 (b)] Each component is hardened in accordance with the applicable {DISA STIGs, CIS Benchmark, Customized Baseline Configuration Benchmark} to ensure the most secure and restrictive settings are configured. All non-secure and unnecessary functions, ports, protocols, and services are disabled {Policy Compliance Tool} in the {Insert Product Name}. {Insert Company Name} maintains a configuration baseline for the environment, which defines what is permitted to be enabled for each component within the environment. [CM-7 (5) (a)]

The Information Security Team performs a monthly vulnerability scan using {Policy Compliance Tool} to identify ports, protocols, and services. The Information Security Team reviews the scan reports to identify unnecessary and/or unsecured functions, ports, protocols, and services. [CM-7 (1) (a)] Any unnecessary functions, ports, protocols, and services identified and are reported to the IT Team for {Company Level Configuration Process}. [CM-7 (1) (b)] The IT Team is responsible for {Company Level Configuration Process}, ports, protocols, and services while the Information Security Team is responsible for changing port availability utilizing {Policy Compliance Tool}. [CM-6 (d)]

The {Insert Company Name} IT Team maintains a list of the currently approved software for the {Insert Product Name} Information System in {Directory Service Database}. The Information Security Team reviews the approved software list at least quarterly and approves all changes to the approved software list. [CM-7 (5) (c)]

The Information Security Team utilizes {Compliance Tool} to prevent all applications other than the allowed executables. [CM-7 (2)] The Information Security Team employs a {Company Level Configuration Process} utilizing {Policy Compliance Tool(s)}. [CM-7 (5) (b)]

8.5 Information System Component Inventory [CM-8]

{Insert Company Name} is responsible for developing, documenting, and maintaining an inventory of information system components [CM-8 (a)] that reflects the current {Insert Product Name} Information System, [CM-8 (a) (1)] and is consistent with the authorization boundary of the information system. [CM-8 (a) (2)] All components within the authorization boundary of the information system are inventoried via {Configuration Management Tool(s)} Vulnerability Management, Detection, and Response (VMDR) (software inventory, ports, protocols, and services). The inventory: should not include duplicate accounting of components or components assigned to any other information system, [CM-8 (a) (3)] is at the level of {company risk tolerance} deemed necessary for tracking and reporting, [CM-8 (a) (4)] and includes information deemed necessary to achieve effective information system component accountability. [CM-8 (a) (5)] Results are compiled in the {StateRAMP or Company Configuration} inventory workbook and are reviewed and updated monthly, [CM-8 (b)] when there are component installations, removals, and/or system updates. [CM-8 (1)]

{Insert Company Name} implements automated mechanisms to continuously monitor for the presence of unauthorized software components within the {Insert Information System Name} authorization boundary. {Insert Company Name} uses {Insert Vendor(s) Name} to continuously detect the presence of unauthorized software within the {Insert Information System Name}. [CM-8 (3) (a)] {Insert Vendor(s) Name} is configured to block all changes to components unless a change is scheduled. Software changes during a scheduled change request are automatically whitelisted. Outside of a change window, {Insert Vendor(s) Name} continuously scans the environment to detect unauthorized or rogue components with a maximum five-minute delay in detection. If an anomaly is detected, {Insert Vendor(s) Name} generates an alert to the Information Security Team and sends the event to {Insert Vendor(s) Name} for the Information Security Team to investigate.

New software installed on systems in the environment must be authorized by {Insert Vendor(s) Name}. Methods of approving new software include update mode, checksum, digital signature, trusted path, updaters, or trusted user. {Insert Vendor(s) Name} is configured to run in the following modes:

{Modify list below, per organization requirements}

* **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 {Insert Vendor(s) Name} and is used to inventory and whitelist software initially installed on a system

{Insert Vendor(s) Name} is configured to use the following methods of whitelisting software:

{Modify list below, per organization requirements}

* **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 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 on the file name or checksum

When unauthorized virtual machine instances or software are detected, the Information Security Team follows the Incident Response Plan. [CM-8 (3) (b)]

8.6 Security Impact Analysis [CM-4]

The Information Security Team performs a Security Impact Analysis (SIA) on all changes, prior to the change. [CM-4] SIAs are integrated into the change request form within the {Insert Company Name} {Insert Documentation Repository Name} Change Management system and are conducted to ensure that new changes implemented in the environment (e.g. software, virtual or physical hardware, firmware) are evaluated against the current security posture of the {Insert Product Name} Information System.

The Information Security Team accounts for all risk factors and ensures security has been considered prior to implementing the change in the {Insert Product Name} Information System. In the event of a high-risk issue, the Information Security Team identifies the risk to provide further insights when determining the approval of the change.

After changes are conducted, {Insert Company Name} verifies through Continuous Monitoring that the impacted controls are still 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)]

8.7 Access Restrictions [CM-5]

{Insert Company Name} implements role-based access control (RBAC) to define, document, approve, and enforce logical access restrictions associated with changes to the {Insert Product Name} Information System. [CM-5] RBAC is enforced through {Insert Documentation Repository Name} and {Insert Documentation Repository Name}. Only System and Network Administrators can make changes to the {Insert list of technologies used, such as: Terraform script, Desired State Configuration (DSC), Group Policy Objects (GPO), and {Insert Documentation Repository Name} Configuration Manager}. Only Information Security team members can make changes within security tools.

Changes to the {Insert Product Name} application code are managed within {Insert Vendor(s) Name}. The {Insert Vendor(s) Name} RBAC is detailed in the Development Team’s System Development Lifecycle (SDLC) document. The Development Team follows a set of code check-ins and a review prior to code being deployed and implemented in the {Insert Product Name} application environment. Only Database Administrators can make changes to the {Insert Product Name} application database structure and schema. For {Insert Vendor(s) Name} code, the Development Team implements {Insert Vendor(s) Name} which encrypt the {Insert Vendor(s) Name} pipelines to ensure unauthorized changes are not made to the code. [CM-5 (1) (a)]

The Information Security Team and IT team reviews and reevaluates privileges at least quarterly to ensure only IT and Information Security team members are authorized to make changes within the {Insert Product Name} Information System. [CM-5 (5) (b)] [CM-5 (5) (a)]

The IT team utilizes {Insert Vendor(s) Name} and {Insert Vendor(s) Name} for software patches and updates. {Insert Vendor(s) Name} retrieves updates from {Insert Vendor(s) Name} and ensures they are digitally signed. {Insert Vendor(s) Name} Configuration Manager is used to deploy the updates retrieved by {Insert Vendor(s) Name} to the systems in the {Insert Product Name} Information System.

{Insert Company Name} configures client operating systems and applications (such as {Insert Vendor(s) Name} ENS and IIS) for automated log generation and uses {Insert Vendor(s) Name} and {Insert Vendor(s) Name} to audit changes to the {Insert Product Name} infrastructure and {Insert Product Name} application changes are tracked via commits in the {Insert Documentation Repository Name} pipeline. [CM-5 (1) (b)]

8.8 Software Usage Restrictions [CM-10]

{Insert Company Name} use of software in the {Insert Product Name} Information System is managed in accordance with the associated license agreements and copyright laws and does not exceed contract terms. [CM-10 (a)] {Insert Company Name} tracks the use of licensed software and associated documentation protected by quantity licenses. [CM-10 (b)] Peer-to-peer file sharing is not allowed within the {Insert Product Name} Information System. Common peer-to-peer file sharing ports are blocked using {Insert Vendor(s) Name} and {Insert Vendor(s) Name} Firewall. [CM-10 (c)]

Open-source software requires approval prior to use and that approval takes the following into consideration: [CM-10 (1)]

{Modify list below, per organization requirements}

* Licensing model
* Redistribution entitlements/restrictions
* Attribution requirements
* Active maintenance of the project
* Availability of source code

Software may not be introduced to the production environment without being authorized by the Information Technology manager (or delegate) and Information Security manager (or delegate). After approval, the software is added to {Insert Company Name}’s approved software list.

8.9 User-Installed Software [CM-11]

All software installed within the environment must first be approved by the IT and Information Security Teams through the Change Management process. The approved software is recorded on the Active Software Catalog List. [CM-11 (a)] Only privileged users can deploy new software within the {Insert Product Name} Information System. [CM-11 (b)] {Insert Company Name} does not allow non-administrator users to install software within the production environment. Authorized administrators are unable to install software without an approved Change Request and until the Information Security Team places the system in ‘Update’ mode within {Insert Vendor(s) Name}. {Insert Vendor(s) Name} continuously monitors and enforces software policies within the {Insert Product Name} Information System. [CM-11 (c)]

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

{Insert Company Name} identifies and documents the location where sensitive information is processed and stored in the {Insert Product Name} Information System. 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 is provided for sensitive information and system components. {Insert Company Name} uses Transparent Data Encryption (TDE) to encrypt sensitive database data. TDE performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest for authorized users or applications when they access the data. 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}:

* Identifies and documents users who have access to the {Insert Product Name} Information System and information system components where information is processed and stored. [CM-12 (b)]
* Documents changes to the location where the information is processed and stored. [CM-12 (c)]
* Stores and processes data in accordance with StateRAMP Authorization Boundary Guidance [CM-12]
* Uses automated tools to identify government data and system data that must be protected at the Moderate impact levels on the {Insert Product Name} Information System to ensure controls are in place to protect organizational information and individual privacy [CM-12 (1)]