# Configuration Management Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure Owner |  |  | |
| Procedure Approver(s) |  |
| Effective Date |  | Next Review Date |  |

## Purpose

The purpose of this procedure is to define a consistent approach to manage changes to the IT environment at [COMPANY NAME].

## Scope

According to the CMMC (Cybersecurity Maturity Model Certification) framework configuration management includes any applicable change processes affecting baseline configurations of systems or network operations.

This procedure is consistent with CMMC and covers all changes to existing IT applications and platforms within [COMPANY NAME]’s network. This procedure will be followed by all employees of [COMPANY NAME]. Excluded from the scope of this procedure are changes to applications that are in the process of being implemented. These changes are controlled by the change control process established for [COMPANY NAME] operations. The CMMC System Security Plan (SSP) will be updated to reflect any significant modifications made to this procedure.

## Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME].
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME].

## Governing Laws & Regulations and Standards

* NIST 800-171, 3.4.1 – 3.4.9
* CMMC CM.L2-3.4.1 – CM.L2-3.4.9
* [COMPANY NAME] – CM – 3.4 - Configuration Management Policy

## Procedure Statements

## CM.L2-3.4.1 – Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles:

1. [COMPANY NAME] has established a baseline configuration which is retained by the Change Control Board. The Change Control Board consist of: <role>, <role>, and <role>
2. The baseline configuration information will contain hardware, software, firmware, and documentation. The baseline configuration is reviewed and updated by the <role>:
   1. At least annually to ensure all current requirements are being met.
   2. When required due to approved changes to the Hardware/ Software baselines.
   3. If the result of an incident identifies that proper configuration guidelines have not been followed.
   4. Whenever overall systematic changes occur that affects the [COMPANY NAME] operating environment.
3. [COMPANY NAME] requires documentation be submitted to the Change Control Board for any new baseline configuration of the information system before it can be put into production. The CCB will retain this information as the Installation baseline for the devices. If changes or updates are required, they will be required to get CCB approval. All requests are to be submitted via the Control Change Board Request form and approved ticketing system.System Administrators are to review and update the baseline configuration of the information system as baseline configuration changes (to include installations, upgrades, removals, etc.) annually or as events dictate such as changes due to [COMPANY NAME] tactical orders/ directives or cyberattacks. [COMPANY NAME] retains the previous approved baseline configuration of Information System (IS) components for a minimum of 3 months. [COMPANY NAME] will notify the responsible party and requestor upon changes to approved baseline configuration. Retention of configurations are kept on the [COMPANY NAME] documents storage repository, Microsoft GCC High for secure storage and backups.
4. [COMPANY NAME] Information System inventory is established and retained by the Change Control Board.
5. The Information System inventory contains current hardware, software, firmware, and documentation.
6. The CCB will retain this information as the current Information System inventory list. If changes or updates are required, they will be required to get CCB approval. All requests are to be submitted via the Control Change Board Request form and approved ticketing system.System Administrators are to review and update the Inventory list of the information system as baseline configuration changes (to include installations, upgrades, removals, etc.) annually or as events dictate such as changes due to [COMPANY NAME] tactical orders/ directives or cyberattacks. [COMPANY NAME] retains the previous approved Inventory list of Information System (IS) components for a minimum of 3 months. [COMPANY NAME] will notify the responsible party and requestor upon changes to approved baseline configuration. Changes can be implemented by Internal IT staff and documentation is kept on the [COMPANY NAME] documents storage repository, Microsoft GCC High for secure storage and backups.

### CM.L2-3.4.2 - Establish and enforce security configuration settings for information technology products employed in organizational systems:

1. [COMPANY NAME] uses DoD and industry standard security configuration or implementation guidance (e.g. STIGs, National Security Agency (NSA) configuration guides, Communications Tasking Orders (CTO), Directive-Type Memorandums (DTM), National Institute of Standards and Technology (NIST) etc.) to establish and document configuration settings for the information system technology products employed. The DoD and industry standard security configuration or implementation guidance (e.g. STIGs, NSA configuration guides, CTOs, DTMs, NIST Frameworks etc.) reflect the most restrictive mode consistent with operational requirements for security configuration checklists. [COMPANY NAME] system baselines are maintained via configuration checklists when the system(s) are brought online. The configuration checklists are reviewed prior to the system being deployed. The checklist is annotated by the <role> for each system.
2. [COMPANY NAME] requires CCB Change Request, Plan of Action and Milestones (POA&M,) and Designated Approving Authority (DAA) risk Acceptance Waiver for any deviation from established configuration settings. [COMPANY NAME] requires CCB (to include the MSP) to Monitor and Control the configuration setting deviations. These documents provide deviation:
3. Identification
4. Justification
5. Mission Impact
6. Mitigation
7. Timeframe
8. Approval

* [COMPANY NAME] requires CCB (to include the MSP) to Monitor and Control the configuration setting deviations.

**CM.L2-3.4.3** **– Track, review, approve or disapprove, and log changes to organizational systems:**

1. All changes to the system are reviewed by the Control Change Board (CCB). All request is to be submitted via the Control Change Board Request form and approved ticketing system. The MSP will update tactics, techniques and procedures as directed by [COMPANY NAME], approved industry standards, and authorized threat feeds (sources). Major changes include major file version upgrades, network device configuration upgrades, or any other changes defined by the <ISSO>. Patch management, virus definition updates, or other similar change activities do not constitute a major change and as such discretion for application resides with the <ISSO> for update frequency, not to exceed patch management guidelines.
2. All changes to the system are approved or disapproved by the CCB. [COMPANY NAME] requires a Change Control Board and charter that outline personnel and processes to encompass the below requirements:
3. Determine the types of changes to the information system that are configuration controlled
4. Review proposed configuration controlled changes to the information system.
5. Approves or disapproves configuration controlled changes to the information system with explicit consideration for security impact analysis.
6. Documents configuration change decisions associated with the information system.
7. Implements approved configuration-controlled changes to the information system.
8. Retains records of configuration-controlled changes to the information system for an organization-defined time period.
9. Defines the time period that the record of configuration-controlled changes are to be retained.
10. Audits and reviews activities associated with configuration controlled changes to the system.
11. Coordinates and provides oversight for configuration change control activities through an organization defined configuration change control element (e.g., committee, board) that convenes at the organization defined frequency and/or for any organization defined configuration change conditions.
12. Defines frequency to convene configuration change control element.
13. Defines configuration change conditions that prompt the configuration change control element to convene.
14. Defines the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities.
15. Changes to the system are logged and kept by the CCB and the System Administrator for record. [COMPANY NAME] requires that all changes to the organizational baselines be documented including any lessons learned from the change. Changes, to include updates that will require downtime of organizational assets, will be coordinated and notification will be made to all [COMPANY NAME] users prior to the downtime occurring. Records of the change are maintained for the life of the system(s).

### CM.L2-3.4.4 - Analyze the security impact of changes prior to implementation:

1. [COMPANY NAME] provides a 14-day window for all severe or critical required updates to be applied to organizational information systems. This window provides for a one-week test period and a one-week application/verification period.

Any updates that are shown to adversely affect information system capabilities will be identified by the <role> and applicable mitigation steps determined to address the risk associated with the update will be addressed. The <role>, in conjunction with System Administrators, will provide information to the [COMPANY NAME] CCB.

Updates that require changes other than patch/update application will be reviewed to determine impact. If any system, system component, or application will require additional time, the <role> will brief the [COMPANY NAME] CCB on the requirements and identified completion date.

### CM.L2-3.4.5 - Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems:

1. [COMPANY NAME] requires the CCB to define physical access restrictions associated with changes to the information system dependent upon change
2. [COMPANY NAME] requires the CCB to document physical access restrictions associated with changes to the information system dependent upon change
3. [COMPANY NAME] requires the CCB to approve physical access restrictions associated with changes to the information system dependent upon change
4. [COMPANY NAME] requires the CCB to enforce physical access restrictions associated with changes to the information system dependent upon change
5. [COMPANY NAME] requires the CCB to define logical access restrictions associated with changes to the information system dependent upon change
6. [COMPANY NAME] requires the CCB to document logical access restrictions associated with changes to the information system dependent upon change
7. [COMPANY NAME] requires the CCB to approve logical access restrictions associated with changes to the information system dependent upon change
8. [COMPANY NAME] requires the CCB to enforce logical access restrictions associated with changes to the information system dependent upon change

* [COMPANY NAME] has defined separate accounts for users and administrators. These accounts are configured on organizational systems prior to them being utilized in production. Users are allowed to apply updates to their assigned systems. Any overall changes to underlying system configurations are prohibited to administrators only. Any and all changes made to information systems and information system components must be explicitly authorized and approved by the <role>.
* [COMPANY NAME] employs Microsoft Sentinel SIEM and local access control polices to ensure unauthorized changes are not processed and detected if executed. [COMPANY NAME] implements the use of group policies to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. Exceptions are granted on case-by by-case basis through [COMPANY NAME] leadership.
* [COMPANY NAME] requires the information system to enforce approved access restrictions and supports auditing of the enforcement actions. If this cannot be accomplished on the IS then another method must be approved through the CCB or the change cannot be approved.
* [COMPANY NAME] maintains and secures physical access to hardware and performs maintenance on all information system components. [COMPANY NAME] is responsible for application specific settings and device configurations which system access control and role policies enforce.

**CM.L2-3.4.6** **- Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities:**

1. [COMPANY NAME] restricts what items can be applied by an [COMPANY NAME] user. All systems have a separate administrator account to apply changes to systems outside of those available to the user. Access to the administrator account is restricted to authorized [COMPANY NAME] personnel. [COMPANY NAME] has defined essential system capabilities based on the principle of least functionality as all [COMPANY NAME] systems and devices are configured per their operational context prior to being deployed. This includes the roles and functions for each system identified to handle FCI/CUI along with the software and services required to perform those functions.
2. The system is configured to provide only the defined essential capabilities per the established baseline configuration. It is the practice of [COMPANY NAME] to configure system functions, ports, protocols, and/or services in accordance with functional needs and the risk tolerance of [COMPANY NAME], thus reducing functionality to only that required to perform a given function. No ports, protocols, and/or services will be enabled unless expectedly needed to perform the required system function.

**CM.L2-3.4.7 - Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.**

1. Essential company programs are defined within the [COMPANY NAME] SSP on the hardware/software list.
2. The use of nonessential programs is defined on the software whitelist/blacklist maintained by the CCB.
3. The use of nonessential programs is restricted, disabled, or prevented by employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system.
4. Essential [COMPANY NAME] Information Systems functions are defined within the [COMPANY NAME] SSP.

1. [COMPANY NAME] utilizes the DoD definition "The information system prohibited or restricted functions, ports, protocols, and/or services (PPS) as in accordance with (IAW) Department of Defense Instruction (DoDI) 8551.01."
2. The use of nonessential functions is restricted, disabled, or prevented by employing a deny-all, permit-by-exception policy to allow the functions on the information system.
3. Essential Ports are defined within the [COMPANY NAME] SSP on the Ports and Protocols list.
4. [COMPANY NAME] utilizes the DoD definition "The information system prohibited or restricted functions, ports, protocols, and/or services (PPS) as in accordance with (IAW) Department of Defense Instruction (DoDI) 8551.01."
5. The use of nonessential ports is restricted, disabled, or prevented employing a deny-all, permit-by-exception policy to allow essential ports on the information system.
6. Essential Ports are defined within the [COMPANY NAME] SSP on the Ports and Protocols list.
7. [COMPANY NAME] utilizes the DoD definition "The information system prohibited or restricted functions, ports, protocols, and/or services (PPS) as in accordance with (IAW) Department of Defense Instruction (DoDI) 8551.01."
8. The use of nonessential protocols is restricted, disabled, or prevented employing a deny-all, permit-by-exception policy to allow essential protocols on the information system.
9. Essential [COMPANY NAME] Information Systems functions are defined within the [COMPANY NAME] SSP.

1. [COMPANY NAME] utilizes the DoD definition "The information system prohibited or restricted functions, ports, protocols, and/or services (PPS) as in accordance with (IAW) Department of Defense Instruction (DoDI) 8551.01."
2. The use of nonessential services is restricted, disabled, or prevented by employing a deny-all, permit-by-exception policy to allow essential services on the information system.

* [COMPANY NAME] requires <role> of the information system to:

1. Provide only essential capabilities.
2. Prohibit or restrict the use of organization-defined programs, functions, ports, protocols, and/or services

* [COMPANY NAME] requires all functions, ports, protocols, and/or services are evaluated and documented by <role>. It is then submitted and forwarded to <role> for approval and implementation.
* [COMPANY NAME] requires review of the information system on a 30 day basis to:
  1. Identify unnecessary and non-secure programs, functions, ports, protocols, and services.
  2. Report unnecessary and/or non-secure programs, functions, ports, protocols, and services.
* [COMPANY NAME] requires all programs, functions, ports, protocols and services within the information system that are deemed unnecessary and/or non-secure be disabled.
* [COMPANY NAME] CCB defines registration requirements for programs, functions, ports, protocols, and services. [COMPANY NAME] requires that the <role> ensure compliance with industry standard well-known ports. Any unregistered port must be evaluated and listed in POA&M for justification of use with any additional systems and protocols information.

**CM.L2-3.4.8 - Develop a procedure for apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. This procedure should include how:**

1. [COMPANY NAME] CCB is required to:

* Define the software programs authorized to execute on the information system and review and update the list of authorized software programs every 90 days.
* Identify the software programs authorized to execute on the information system required review and update the list of authorized software programs every 90 days.

1. The software allowed to execute under whitelisting or denied use under blacklisting is specified in the [COMPANY NAME] SSP under Software/Hardware list and maintained by the CCB.
2. [COMPANY NAME] <role> are required to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system. The <role> will monitor Microsoft Sentinel SIEM to complete an audit of authorized software

**CM.L2-3.4.9 - Develop a procedure for controlling and monitoring user-installed software. This procedure should include how:**

1. [COMPANY NAME] requires all installation users and administrators to:
2. Utilize software in accordance with contract agreements.
3. Utilize software documentation in accordance with contract agreements.
4. Utilize software in accordance with copyright laws.
5. Utilize software documentation in accordance with copyright laws.
6. [COMPANY NAME] requires the CCB to:
   1. Maintain the policies for governing the installation of software by users.
   2. Define methods to be employed to enforce the software installation policies.
   3. Enforce software installation policies through organization-defined methods.
   4. Monitor monthly software installation policy compliance.
7. [COMPANY NAME] requires all installation organizations to:
8. Track the use of software protected by quantity licenses to control copying of the software.
9. Track the use of software documentation protected by quantity licenses to control copying of the software documentation.
10. Track the use of software protected by quantity licenses to control distribution of the software.
11. Track the use of software documentation protected by quantity licenses to control distribution of the software documentation.
12. 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.

* Any attempt to run or install unauthorized software that has not been approved by [COMPANY NAME] is captured to the event log and forwarded into the SIEM solution for monitoring and review.
* [COMPANY NAME] devices are configured to administratively prohibit non-privileged users from installing software onto a [COMPANY NAME] machine. User rights are further restricted by using application whitelisting to prevent any application from running that has not been installed into the programs or system directory, which requires administrative (privileged) access to do.

## Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at [COMPANY NAME]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 12/7/2022 | SecureStrux | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |