|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Policy**:  **Configuration Management** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The Configuration Management Policy aims to establish a structured approach for managing and controlling changes to the organization’s information systems. By defining baseline configurations, change control procedures, and security impact analyses, this policy seeks to ensure that all configurations are documented, maintained, and monitored effectively. The ultimate goal is to enhance the security posture of the organization by minimizing the risks associated with unauthorized changes, misconfigurations, and vulnerabilities in the IT environment.

Implementing the Configuration Management Policy provides several key benefits, including improved security and operational efficiency. By maintaining baseline configurations and systematically controlling changes, the organization can reduce the likelihood of security incidents resulting from configuration errors. Regular reviews and audits enhance accountability and compliance with industry best practices, contributing to a more secure information system. Additionally, the policy fosters a culture of discipline around configuration management, ensuring that all personnel understand their roles in protecting the integrity and security of organizational assets.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Configuration Management Policy outlines the framework for managing the configuration of the organization’s information systems, applicable to all employees, contractors, and third-party vendors. Key components include the establishment of baseline configurations, a structured change control process, and the documentation of configuration settings in accordance with recognized security standards. The policy mandates regular reviews and updates of configurations and inventories to ensure accuracy and compliance. By adhering to these guidelines, the organization aims to protect the confidentiality, integrity, and availability of its information assets while minimizing risks associated with configuration management practices. Non-compliance with this policy may result in disciplinary action.

* 1. Baseline Configuration

The [Owner] shall:

1. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.
2. Review and update the baseline configuration of the information system annually.
3. Review and update the baseline configuration of the information system when required as a result of major system updates or changes in security posture and as an integral part of information system component installations and upgrades.
4. Retain one previous version of baseline configurations of information systems to support rollback.
   1. Configuration Change Control

The [Owner] shall:

1. Determine the types of changes to the information system that are configuration-controlled.
2. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.
3. Document configuration change decisions associated with the information system.
4. Implement approved configuration-controlled changes to the information system.
5. Retain records of configuration-controlled changes to the information system for three years.
6. Audit and review activities associated with configuration-controlled changes to the information system.
7. Coordinate and provide oversight for configuration change control activities through a Change Control Board (CCB) that convenes monthly; when critical system updates, security patches, or new hardware components are introduced.
8. Test, validate, and document changes to the information system before implementing the changes on the operational system.
   1. Security Impact Analysis

The [Owner] shall analyze changes to the information system to determine potential security impacts prior to change implementation.

* 1. Access Restrictions for Change

The [Owner] shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

* 1. Configuration Settings

The [Owner] shall:

1. Establish and document configuration settings for information technology products employed within the information system using CIS (Center for Internet Security) Benchmarks and NIST Security Configuration Checklists that reflect the most restrictive mode consistent with operational requirements.
2. Implement the configuration settings.
3. Identify, document, and approve any deviations from established configuration settings for critical servers, workstations, and networking equipment based on operational and business continuity needs.
4. Monitor and control changes to the configuration settings in accordance with policies and procedures.
   1. Least Functionality

The [Owner] shall:

1. Configure the information system to provide only essential capabilities.
2. Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.
3. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.
4. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.
5. Identify software programs not authorized to execute on information systems.
6. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.
7. Review and update the list of unauthorized software programs annually.
   1. Information System Component Inventory

The [Owner] shall:

1. Develop and document an inventory of information system components that:
2. Reflects the current information system accurately.
3. Includes all components within the authorization boundary of the information system.
4. Is at the level of granularity deemed necessary for tracking and reporting.
5. Includes information deemed necessary to achieve effective information system component accountability.
6. Review and update the information system component inventory quarterly.
7. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.
8. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system.
9. Take the following actions when unauthorized components are detected:
10. Disable network access by such components, or
11. Isolate the components and notifies the [Authority] and system owner.
12. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.
    1. Configuration Management Plan

The [Owner] shall develop, document, and implement a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures.
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
3. Defines the configuration items for the information system and places the configuration items under configuration management.
4. Protects the configuration management plan from unauthorized disclosure and modification.
   1. Software Usage Restrictions

The [Owner] shall:

1. Use software and associated documentation in accordance with contract agreements and copyright laws.
2. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.
3. 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.
   1. Configuration Management Plan

The [Owner] shall:

1. Establish policies governing the installation of software by users.
2. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.
3. Monitor policy compliance at quarterly.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-116 – Guidelines for the Use of PIV Credentials in Facility Access](https://csrc.nist.gov/pubs/sp/800/116/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-34 – Contingency Planning Guide for Federal Information Systems](https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-50 – Building a Cybersecurity and Privacy Learning Program](https://csrc.nist.gov/pubs/sp/800/50/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-84 – Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](https://csrc.nist.gov/pubs/sp/800/84/final)