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

# 1.0 Purpose and Benefits

The purpose of the Secure Configuration Standard is to establish a framework for ensuring that information systems are configured and maintained in a secure manner. By adhering to industry consensus guidelines and best practices, the standard aims to minimize vulnerabilities and enhance the overall security posture of the organization. It emphasizes the importance of structured change management processes, secure initial setups, and ongoing monitoring to protect against unauthorized access and potential security breaches.

The benefits of the Secure Configuration Standard include improved system security, reduced risk of data breaches, and enhanced compliance with regulatory requirements. By following standardized guidelines, the organization can achieve consistency in security practices, making it easier to identify and rectify misconfigurations. Additionally, the standard fosters a proactive approach to security through regular monitoring and assessment, ultimately leading to increased trust from stakeholders and a more resilient IT environment.

# 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 Secure Configuration Standard outlines guidelines for configuring and managing information systems at [Organization Name] to enhance security and compliance. It requires the use of industry consensus guidelines, such as CIS Benchmarks, NIST Checklists, and USGCB, as the basis for secure configuration profiles. Any modifications must be justified by business needs, developed with input from the Information Security Officer, and documented for audit purposes. Initial setups and configurations must occur in a secure environment, with changes following a formal process that includes review and security impact analysis. Configuration management plans must be maintained to align with secure system development life cycle practices. Ongoing monitoring is essential to detect unauthorized changes, misconfigurations, and vulnerabilities, ensuring systems remain secure over time.

* 1. Industry Standards

Standard secure configuration profiles, based on any one or more of the industry consensus guidelines listed below, must be used in addition to the latest vendor security guidance. Alterations to the profile must be based on business need, policy or standard compliance, developed in consultation with the Information Security Officer/designated security representative, documented and retained for audit purposes.

Industry Consensus Guidelines:

1. [Center for Internet Security (CIS) Benchmarks](http://benchmarks.cisecurity.org/)
2. [National Institute of Science and Technology (NIST) National Checklist Program](http://web.nvd.nist.gov/view/ncp/repository)
3. [United States Government Configuration Baselines (USGCB)](http://usgcb.nist.gov/usgcb_content.html)
   1. Secure Environment

The initial setup, software installation, and security configuration of new systems must be performed in a secure environment isolated from other operational systems with minimal communication protocols enabled.

* 1. Changes

Changes to configurations are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved prior to implementation in accordance with the change management procedures. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

* 1. Management

Entities must maintain configuration management plans that define detailed processes and procedures for how configuration management is used to support secure system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the secure system development life cycle.

* 1. Monitoring

A configuration monitoring process must be in place to identify undiscovered or undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes.

# 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) 800-128, Guide for Security-Focused Configuration Management of Information Systems](https://csrc.nist.gov/publications/detail/sp/800-128/final" \t "_blank)

[Center for Internet Security (CIS) Benchmarks](http://benchmarks.cisecurity.org/)

[National Institute of Science and Technology (NIST) National Checklist Program](http://web.nvd.nist.gov/view/ncp/repository)

[United States Government Configuration Baselines (USGCB)](http://usgcb.nist.gov/usgcb_content.html)