# Configuration Management Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. CIS Benchmarks: <https://www.cisecurity.org/cis-benchmarks>
2. ISO 10007: <https://www.iso.org/obp/ui/#iso:std:iso:10007:ed-3:v1:en>
3. ISO/IEC 29146: <https://www.iso.org/obp/ui/#iso:std:iso-iec:29146:ed-2:v1:en>
4. NIST 800-128: <https://csrc.nist.gov/pubs/sp/800/128/upd1/final>
5. ISO/IEC 27001:2022: A.5.15, A.5.30, A.8.6, A.8.9, A.8.14, A.8.17, A.8.18
6. NIST 800-53 rev. 5: AC-6, AC-6(1), AC-6(2), AC-6(10), AC-17(4), AU-8, CM-1, CM-2, CM-2(2), CM-2(3), CM-2(7), CM-5, CM-5(5), CM-6(1), CM-7, CM-7(1), CM-7(2), CM-9, CP-6, CP-10, MA-3, MA-3(1), SA-9(2), SC-1, SC-5, SC-7(18), SC-39, SC-45, SC-45(1)
7. CIS v8: 4.1, 4.2, 4.7, 4.8, 6.8, 8.4, 12.2, 12.3, 12.6, 12.8, 16.7
8. PCI DSS 4.0: 1.2.5, 1.2.6, 1.2.8, 2.1.1, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.6, 2.2.7, 5.3.5, 7.2.5, 7.3.1, 7.3.3, 10.6.1, 10.6.2, 10.6.3
9. AICPA SOC 2 TSC: A1.1, CC4.1, CC6.2, CC6.3, CC6.5, CC6.7, CC7.1, CC9.1, P5.1, PI1.2

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

This Configuration Management Policy aims to establish a framework for managing and controlling the configuration of the organization's information systems, ensuring that systems and processes are secure, consistent, and compliant with organizational and industry standards. This policy aims to enhance the security, reliability, and performance of the organization's IT infrastructure by enforcing systematic processes for baseline configuration management, system hardening, and the management of system changes.

## Scope

This policy applies to all information systems and any other IT assets owned, operated, or managed by the organization. It includes all employees, contractors, and third-party service providers who have access to or are responsible for configuring and maintaining these systems. This policy covers the following key areas:

* Baseline configuration management
* System hardening, including least functionality, disabling default credentials, securing clocks, and operating system configuration
* Use of secure components
* Ensuring fail-secure configurations
* Restriction of configuration changes
* Cost management, scalability, and elasticity of systems
* Availability and capacity of system services and data storage
* Quality and performance standards of the system

By adhering to this policy, the organization aims to mitigate risks associated with misconfigurations, unauthorized changes, and system vulnerabilities, thereby maintaining a secure and resilient IT environment.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], Operational owner title] |  |
| Information Systems Administrators | System Administrators  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. Baseline Configuration: A documented set of specifications for an information system, derived from the current operational environment, which serves as a foundation for future changes and maintenance.
	2. Least Functionality: The practice of configuring systems to operate with only the necessary capabilities, removing or disabling all non-essential functions and services.
	3. Default Credentials: Pre-configured usernames and passwords set by manufacturers for accessing systems or devices, which must be changed or disabled to prevent unauthorized access.
	4. Secure Clocks: The synchronization of system clocks with a reliable and authoritative time source to ensure accurate timekeeping and log integrity.
	5. Operating System Hardening: The process of securing an operating system by reducing its surface of vulnerability, which includes applying patches, configuring settings securely, and disabling unnecessary services.
	6. Network Components: Hardware and software that facilitate network connectivity, communication, and management, including routers, switches, firewalls, and load balancers.
	7. Fail Secure: A configuration principle ensuring that systems default to a secure state in the event of a failure, thereby maintaining security even during unexpected outages or malfunctions.
	8. Privileged Accounts: User accounts with elevated permissions that allow for administrative access to systems and data, typically restricted to authorized personnel only.
	9. Least Privilege: The principle of granting users and processes the minimum levels of access—or permissions—needed to perform their job functions or tasks.
	10. Administrative Software, Scripts, and Services: Tools and utilities used by system administrators to manage, configure, and maintain information systems, which must be protected from unauthorized access.
	11. Service Accounts: Specialized accounts used to run application services or perform automated tasks, typically configured with limited permissions to reduce security risks.
	12. Scalability: The capability of a system to handle a growing amount of work or its potential to accommodate growth.
	13. Elasticity: The ability of a system to dynamically adjust resources and services to meet varying demands, ensuring efficient use of resources.
	14. Availability: The measure of a system's ability to be accessible and operational when required for use, ensuring continuous service delivery.
	15. Capacity: The maximum amount of work that a system is capable of handling, which must be managed to meet current and future demands.
	16. Quality and Performance: The adherence to predefined standards and the efficiency with which a system operates, affecting user satisfaction and operational effectiveness.
	17. Backup Systems and Services: Mechanisms and processes used to create and store copies of data and systems to ensure data recovery and continuity in the event of a failure or loss.

## Policy

#### Baseline Configuration Management

The [responsible party] shall:

* + 1. Establish and maintain documented baseline configurations for all information systems and assets.
		2. Ensure that baseline configurations are reviewed and updated regularly to reflect the current operational environment.
		3. Utilize automated tools to enforce baseline configurations across all systems.
		4. Document and approve all deviations from established baselines.

#### Configuring and Hardening Systems

The [responsible party] is required to:

* + 1. Configure systems to provide only essential capabilities, removing or disabling all unnecessary functions and services.
		2. Remove or change all default passwords and disable default accounts immediately upon system installation.
		3. Configure system clocks to synchronize with an authoritative time source to ensure accurate timekeeping across the network.
		4. Harden operating systems according to industry best practices and organization-specific security guidelines.
		5. Ensure only approved, secure configurations are deployed, and document all configuration settings.
		6. Deploy only those network components, servers, domain name servers, wireless access points, and other system components that meet organizational security standards.
		7. Regularly review and update configurations to protect against emerging threats and vulnerabilities.
		8. Configure systems to default to a secure state in the event of a failure, ensuring that security is not compromised during outages or malfunctions.

#### Configuration Management

The [responsible party] shall:

* + 1. Grant administrative privileges only to those accounts that require them for their job functions.
		2. Review and adjust privileges regularly to ensure the principle of least privilege is maintained.
		3. Restrict access to administrative tools, scripts, and services to authorized personnel only.
		4. Use dedicated service accounts to run application services, ensuring these accounts have the minimum necessary privileges.
		5. Regularly review service accounts and their privileges, updating or deactivating accounts as needed.

#### Availability and Capacity

The [responsible party] is required to:

* + 1. Monitor and manage the costs associated with configuration management and system maintenance.
		2. Regularly assess and adjust system services and data storage capacity to meet current and projected needs and optimize performance.
		3. When applicable, plan and implement scalable and elastic system configurations to accommodate growth and changing operational demands.
		4. Consider the location of data and processing (on-prem, hybrid, private cloud, community cloud, etc) to maximize cost-effectiveness
		5. Implement configurations that cost-effectively meet the availability and capacity requirements of system services and data storage
		6. Employ redundancy and failover mechanisms to ensure continuous availability of critical systems in the event of hardware or software failures.
		7. Configure systems to meet quality and performance standards as defined by organizational policies and industry best practices.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |