# [Document Title]

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. [List of applicable compliance frameworks and requirements]

## 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

## Scope

[description of scope]

## 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

## Policy

## 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 |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |