# Information Security and Privacy Governance 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.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. ISO 37000:<https://www.iso.org/standard/65036.html>
2. ISO 14001:<https://www.iso.org/standard/60857.html>
3. ISO/IEC 27001:2022: 4.1, 4.2, 5.1, 5.2, 6.2, 7.1, 7.5, 9.3, A.5.1, A.5.2, A.5.3, A.5.5, A.5.6, A.5.8, A.5.31, A.5.37, A.6.4
4. NIST 800-53 rev. 5: xx-1, AC-20, CA-6, IR-6, PL-1, PS-8, PS-9, SA-2
5. CIS v8: 12.1, 17.5
6. PCI DSS 4.0: x.1.1, x.1.2, 6.5.4, 12.1.3, 12.1.4, 12.4.2, 12.4.2.1
7. AICPA SOC 2 TSC: CC1.1, CC1.2, CC1.3, CC1.4, CC1.5, CC2.2, CC2.3, CC3.1, CC5.2, CC5.3, CC6.3

## 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

The purpose of this Governance Policy is to establish a structured framework for overseeing and directing the organization's information security and privacy practices. This policy aims to ensure the alignment of information security strategies with the organization's business objectives, promote ethical and sustainable practices, and maintain compliance with legal, regulatory, and industry standards. By clearly defining roles, responsibilities, and procedures, this policy supports the organization’s commitment to protecting its information assets, fostering a culture of security and ethics, and achieving operational excellence.

## Scope

This policy applies to all members of the Board of Directors, Executive Management Team, Information Security Officer, Compliance Officer, Human Resources, Information Security Team, and any other employees or contractors with responsibilities related to information security and privacy within the organization. It encompasses all activities and processes involved in the establishment, implementation, enforcement, and review of information security and privacy policies. This includes, but is not limited to, board oversight, ethical and sustainable practices, relationships with authorities and industry groups, policy enforcement, segregation of duties, and alignment of business objectives with security controls. The policy is applicable to all information systems, data, and assets owned, managed, or operated by the organization.

## 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. **Board of Directors**: The group of individuals elected to represent shareholders and oversee the overall direction and governance of the organization.
	2. **Executive Management Team**: Senior leaders within the organization responsible for strategic decision-making and operational oversight.
	3. **Information Security Officer (ISO)**: The designated individual responsible for developing and implementing the information security strategy and program within the organization.
	4. **Compliance Officer**: The individual responsible for ensuring that the organization adheres to legal, regulatory, and internal policies related to information security and privacy.
	5. **Human Resources (HR)**: The department responsible for managing employee relations, recruitment, and ensuring that organizational roles and responsibilities are defined and adhered to.
	6. **Information Security Team**: A group of professionals tasked with protecting the organization’s information assets by implementing and managing security measures.
	7. **Ethics**: A set of principles that guide behavior based on what is considered morally right and wrong within the organization.
	8. **Sustainability**: Practices that meet the needs of the present without compromising the ability of future generations to meet their own needs, often encompassing environmental, social, and governance (ESG) factors.
	9. **Regulatory Bodies**: Government agencies or other official organizations that oversee the adherence to laws and regulations within specific industries.
	10. **Law Enforcement Agencies**: Government organizations responsible for the enforcement of laws and maintenance of public order and safety.
	11. **Industry-specific Security and Privacy Groups**: Professional associations or consortia focused on advancing best practices, standards, and knowledge sharing in the field of information security and privacy.
	12. **Policy Violation**: An instance where an action or behavior goes against the established policies and procedures of the organization.
	13. **Segregation of Duties (SoD)**: The practice of dividing responsibilities among different individuals or teams to reduce the risk of error or fraud.
	14. **Standard Operating Procedures (SOPs)**: Detailed, written instructions designed to achieve uniformity of the performance of a specific function.
	15. **Threat Landscape**: The current state of potential threats that could exploit vulnerabilities in an organization’s information systems and cause harm.
	16. **Security Controls**: Safeguards or countermeasures implemented to protect information assets from threats and vulnerabilities.
	17. **Business Objectives**: The goals and targets that an organization aims to achieve as part of its business strategy.
	18. **Contractual Obligations**: Legal requirements agreed upon in a contract between two or more parties.
	19. **Legal Requirements**: Obligations imposed by law that an organization must adhere to.
	20. **ESG Performance**: The measurement of an organization’s sustainability and ethical impact based on environmental, social, and governance factors.
	21. **Audit**: A systematic review or assessment of an organization’s processes, systems, and policies to ensure compliance and effectiveness.
	22. **Executive Sponsorship**: The support and commitment provided by senior management to endorse and drive the successful implementation of initiatives within the organization.
	23. **Business Processes**: A series of steps or activities undertaken by an organization to achieve a specific goal or objective.
	24. **Policies**: Formalized rules and guidelines that dictate the expected behaviors and actions of individuals within the organization.
	25. **Controls**: Mechanisms or procedures put in place to mitigate risks and ensure compliance with policies and standards.
	26. **Incident Preparedness**: The state of being ready to effectively respond to and manage security incidents.
	27. **Legal and Regulatory Changes**: Updates or modifications to laws and regulations that impact how an organization conducts its business and manages information security and privacy.

## Policy

#### Board Oversight and Direction

The Board of Directors shall:

* + 1. Oversee the establishment and implementation of information security and privacy policies.
		2. Ensure that the information security strategy aligns with the organization's business objectives and risk appetite.
		3. Review and approve major policies, strategies, and frameworks related to information security and privacy annually.
		4. Monitor the effectiveness of the information security program and make necessary adjustments based on performance metrics and audit results.
		5. Establish a governance framework that supports ethical and sustainable practices within the organization.

#### Ethical and Sustainable Practices

The Executive Management Team shall:

* + 1. Promote a culture of ethics and sustainability within the organization.
		2. Ensure compliance with relevant environmental, social, and governance (ESG) standards and regulations.
		3. Incorporate ethical considerations into business decisions and operational practices.
		4. Develop and implement training programs to raise awareness about ethical and sustainable practices among employees.
		5. Monitor and report on the organization’s ESG performance regularly.

#### Establishing Relationships with Authorities

The [responsible party] shall:

* + 1. Establish and maintain relationships with relevant regulatory bodies and law enforcement agencies.
		2. Stay informed about legal and regulatory changes impacting information security and privacy.
		3. Participate in incident response exercises with local authorities to ensure preparedness for security incidents.
		4. Coordinate the organization's response to legal and regulatory inquiries related to information security and privacy incidents.

#### Establishing Relationships with Industry Groups

The [responsible party] shall:

* + 1. Establish and maintain relationships with industry-specific security and privacy groups.
		2. Participate in information-sharing and collaboration initiatives to stay informed about emerging threats and best practices.
		3. Represent the organization in industry conferences, working groups, and forums related to information security and privacy.
		4. Leverage insights and recommendations from industry groups to enhance the organization's security posture.

#### Policy Enforcement

The [responsible party] shall:

* + 1. Implement mechanisms to enforce compliance with information security and privacy policies.
		2. Conduct regular audits and assessments to ensure adherence to established policies and procedures.
		3. Investigate and address policy violations promptly and consistently.
		4. Report significant policy violations to the Board of Directors and Executive Management Team.

#### Segregation of Duties

The [responsible party] shall:

* + 1. Ensure that duties and responsibilities are appropriately segregated to reduce the risk of unauthorized access or fraud.
		2. Implement controls to enforce segregation of duties within critical processes and systems.
		3. Review and update role-based access controls (RBAC) regularly to reflect changes in job roles and responsibilities.

#### Roles and Responsibilities for Information Security and Privacy

The [responsible party] shall:

* + 1. Define and document roles and responsibilities for information security and privacy across the organization.
		2. Ensure that individuals with security and privacy responsibilities receive adequate training and resources.
		3. Conduct regular reviews to ensure that roles and responsibilities are clearly understood and effectively executed.

#### Establishment, Review, and Management Commitment to Policies

The Executive Management Team shall:

* + 1. Establish and approve information security and privacy policies.
		2. Ensure that policies are reviewed and updated annually or as needed to reflect changes in the threat landscape and business environment.
		3. Demonstrate a strong commitment to information security and privacy through resource allocation and executive sponsorship.

#### Business Alignment

The [responsible party] shall:

* + 1. Ensure that information security and privacy policies align with the organization’s contractual, legal, and business objectives.
		2. Collaborate with business units to integrate security controls into business processes and systems.
		3. Conduct regular reviews to ensure that security controls are effective and aligned with business needs.

#### System of Operating Procedures

The [responsible party] shall:

* + 1. Develop and document standard operating procedures (SOPs) to support the implementation of information security and privacy policies.
		2. Ensure that SOPs are easily accessible to relevant personnel and integrated into daily operations.
		3. Review and update SOPs regularly to reflect changes in policies, technologies, and business processes.

## 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** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |