COMPANY policy template instructions

This COMPANY policy template represents a complete, compliance-ready policy with placeholders for company specific text. Each policy section represents a policy-specific topic that you should consider and/or modify to match your company’s practices.

For each policy section

* Consider if this section and its corresponding risks apply to you. If it does not, remove it and/or replace it with your organization’s corresponding practices.
* Replace any highlighted text in angled brackets < > with your own language
* Rewrite the policy language such that it reflects the practices of your organization

Policy completion checklist

1. Use Find to make sure that all text in angled brackets is replaced
2. Proofread your policy for spelling and grammar mistakes
3. Confirm that the policy’s content reflects your organizations practices
4. Add any company-specific letterhead, branding, and formatting
5. Remove this instructions page
6. Export this document as PDF — File > Save As > Change “File Format” to PDF
7. Upload the PDF to COMPANY at https://app.COMPANY.com/policies

More questions?

A good rule-of-thumb is to keep your language at a high enough level such that it stays representative for at least a year. If you have more questions about how to use this template, please reach out to support@COMPANY.com or your auditor for additional guidance.

Document Name: Roles, Responsibilities, and Authorities

Document Number: 03-ISMS

| Company Name: | <Company Name> |
| --- | --- |
| Policy Owner(s): | <Policy owner(s)> |
| Effective Date: | <Effective date> |

# Purpose

The purpose of this document is to clearly define the roles, responsibilities, and authorities that are essential to the establishment, implementation, maintenance and continual improvement of <Company Name>’s Information Security Management System (“ISMS”).

# Scope

This policy applies to all top management and personnel associated with the ISMS across the organization.

# Roles and Responsibilities

Top management shall periodically review the ISMS and ensure the adequate assignment of responsibilities and authorities.The <Company Name> identified the following high level roles and responsibilities:

* Top Management: Accountable for the review and adequate delegation of ISMS roles and responsibilities. Major roles and their functionalities should be sanctioned by this tier.
* ISMS Coordination: Entrusted with overseeing the establishment, regular maintenance, performance analytics, and improvement of the ISMS.
* ISMS Advisory: Dedicated to providing guidance on the risk assessments and treatments associated with information security.
* Designing: Tasked with the development of information security processes and systems tailored to the organization's needs.
* Standard Setting: Involved in the formulation and adjustment of information security standards and controls within the organization.
* Incident Management: Engages in the swift and effective handling of any information security incidents that arise.
* Review & Audit: Responsible for the periodic and thorough examination and evaluation of the ISMS's efficiency and compliance.

# ISMS Roles

## ISMS Governance Council

The ISMS Governance Council is chaired by the Information Security Management Leader and composed of executive management or their delegates needed to support information security or drive the future vision of information security. The ISMS Governance Council members are comprised of the following roles:

* CIO (Information Security Management Leader & Data Protection Officer)
* COO
* Director of Operations
* Delegates from <Company Name> Companies
* IT Leaders
* Other interested parties/stakeholders (optional)

## Information Security Management Leader

The Information Security Management Leader role has the authority to drive information security at <Company Name> at the functional and operational levels and is responsible for the coordination of the ISMS activities across the organization. Additionally, the Information Security Management Leader should cover the ISMS Coordination: Entrusted with overseeing the establishment, regular maintenance, performance analytics, and improvement of the ISMS.

The <role that is the designated Information Security Management Leader, e.g., CIO> is the designated Information Security Management Leader.

## Information Security Team

The Information Security Team is composed of individuals that manage the day-to-day compliance and monitoring activities necessary to achieve, maintain, and improve the ISMS to meet the Information Security Objectives.

The Information Security Team members are comprised of the following roles:

* CIO
* Systems & Network Administrator(s)
* Senior Engineer(s)
* COO (Optional)
* Human Resource Representative (as needed)

## Data Protection Officer

The Data Protection Officer role has the authority to drive data privacy at <Company Name> at the functional and operational levels and is responsible for the coordination of the data privacy activities across the organization.

The <role that is the designated Data Protection Officer, e.g., CIO> is the designated Data Protection Officer.

## Risk Owners

A Risk Owner is a person or entity that has the authority to manage a particular risk and is accountable for doing so.

## Employees, Third-Parties, Vendors, Contractors, and Consultants

This role includes all employees, third-parties, vendors, contractors, and consultants within the in-scope departments that support the ISMS.

# ISMS Responsibilities

This section details the responsibilities for each role which are essential to the establishment, implementation, maintenance and continual improvement of the ISMS.

## ISMS Governance Council

| **Responsibility** | **Frequency\*** |
| --- | --- |
| Overseeing major initiatives to enhance information security | Annually or as needed |
| Confirming that the information security objectives are established, compatible, and updated based on strategic direction of the organization | Annually |
| Reviewing corrective actions and improvements to the ISMS to achieve its intended objectives | Annually |
| Identifying customer security requirements (exceptions to standard controls) | As needed |
| Monitoring progress against the Communication, Implementation, Corrective Action and Improvement Plans | Annually |
| Reviewing information security incidents and supporting the resolution within their function | As needed |
| Providing adequate resources (i.e., budget, human, equipment, software) to establish, operate, and improve the ISMS | Annually |
| Approving the information security policies | Annually |
| Approving the results of the Risk Assessment and Risk Treatment Plan | Annually |
| Communicating the importance of the ISMS and the criticality of continual improvement | Annually |
| Performing management review of the ISMS | Annually |
| Reviewing the results of technical tests and internal and external audits of the ISMS | Annually |
| Identifying, managing, and supporting personnel operating the ISMS owned by their respective function | Continuously |

## Information Security Management Leader

| **Responsibility** | **Frequency\*** |
| --- | --- |
| Ensuring that the ISMS conforms to the requirements of the ISO 27001 Standard | Continuously |
| Reporting on the performance of the information security management system to top management | Annually or as needed |
| Oversee all ISMS initiatives for the organization | Continuously |
| Oversee the execution of the Communication / Implementation Plan, internal audits, management review and corrective actions/improvements | Continuously |
| Maintaining and updating of the ISMS Governance and Oversight model | Continuously |
| Confirming material needed for the ISMS Governance Council to meet their responsibilities is prepared, aggregated, and presented | Annually |
| Confirming minutes are kept during ISMS Governance Council meetings and all actions are executed upon | Quarterly |
| Confirming that the ISMS Governance Council is informed of material changes to the organization’s risk profile or key controls | As needed |
| Reviewing, updating and confirming that ISMS policies are current and meet objectives | Annually |
| Oversee the execution of the internal ISMS audit and other audits and technical tests | Annually |
| Requesting resources (i.e., budget, human, equipment, software) needed to establish, operate, and improve the ISMS | Annually |
| Communicating the importance of the ISMS and the criticality of continual improvement within their function | Annually |
| Implementing and coordinating security training and awareness | Annually |
| Ensuring that new risk treatments are integrated into the ISMS | Annually |
| Managing the ISMS documents and records | Continuously |

## Information Security Team

| **Responsibility** | **Frequency\*** |
| --- | --- |
| Defining, monitoring, and reporting the Communication, Implementation, Improvement, Corrective Action Plans, and effectiveness measurement metrics | As needed |
| Following up on all incidents reported to resolution and sharing learning opportunities with all applicable functions | As needed |
| Identifying changes and their impact to the internal/ external context of the organization, interested parties, scope and boundaries, and objectives | Continuously |
| Tracking exceptions to ISMS policies and standards | As needed |
| Notifying the Information Security Management Leader of any issues regarding the competence of personnel supporting the ISMS | As needed |
| Coordinating and managing the execution of the internal / external audits and treatment of gaps / non-conformities | Annually |
| Facilitating risk assessments and technical testing | Annually |
| Providing inputs for the management review | Annually |
| Supporting staff who are implementing and operating controls managed and owned by their respective function. | Continuously |
| Implementing corrective actions and improvements for the controls managed and owned by their respective function | Continuously |
| Measuring and reporting on the effectiveness of the ISMS controls managed and owned by their respective function | Annually and As needed |
| Assessing vendor and third-party risk, including cloud service providers | Annually and As needed |
| Participating in internal audits, management reviews, and external audits | As needed |

## Employees, Third-parties, Vendors, Contractors, and Consultants

| **Responsibility** | **Frequency\*** |
| --- | --- |
| Active participation in ISMS initiatives like ISMS training and awareness, ISMS audits, reviews, etc. | Continuously |
| Disposing of information in their possession in accordance with company policy | As needed |
| Maintaining the strict confidentiality and integrity of company and customer information | Continuously |
| Reporting on incidents/ security breaches and suspected incidents through the incident management process | As needed |
| Understanding their security responsibilities and following the information security policy, objectives, regulatory, legal, and contractual requirements/obligations | Continuously |
| Adhering to the Company Policies, Ethics Code and Standards of Conduct | Continuously |

\* Frequency of any activity may be performed on an as needed basis

# Competence

For the successful implementation and maintenance of the Information Security Management System (ISMS), it's crucial to ensure the competence of individuals involved. This policy aims to ensure clarity in determining, assigning, and maintaining competence. <Review frequency, e.g., Annually>, <Company Name> will assess the performance and competence of applicable personnel against the ISMS-required competencies. This will be completed by defining personnel’s role, assessing job performance, and competence during performance reviews and by addressing any competency gaps.

# Define

Personnel’s roles are defined through individual job descriptions in which a <Company Name> manager coordinates directly with Human Resources to develop. In addition to job descriptions, roles and responsibilities pertinent to the management of the ISMS are documented within sections 2 and 3 of this document.

# Measure

Personnel are measured initially for their competence to meet the requirements of the job description throughout the interview process which is inclusive of Human Resources and <Company Name> Manager or delegate. <Performance appraisal frequency, e.g., Annually>, <Company Name> conducts an employee performance appraisal to evaluate an employee’s performance which is performed by Human Resources and direct managers.

As part of the <frequency of security awareness training, e.g., annual> Information Security Awareness training the Information Security Team may issue tests to evaluate an individual’s knowledge and awareness of security topics and company policies.

# Competency Gaps

Solutions for remediating competency gaps will be monitored and evaluated for effectiveness by an individual’s direct manager and documented with Human Resources through the <frequency of employee performance appraisal, e.g., annual> employee performance appraisal. Solutions may include providing training or mentoring, re-assigning tasks or personnel, or supplementing with contractors and/or consultants.

Employees who do not pass the security awareness test(s) may be required to complete the training again and retake the test(s), or other remediation activities as needed.

# ISO 27001 Coverage

ISO 27001 5.1; 5.2; 5.3; 7.1; 7.2; A.5.2

# Version History

| **Version** | **Date** | **Description** | **Author** | **Approved by** |
| --- | --- | --- | --- | --- |
| <1.0> | <Date of change> | Initial policy | <Author of changes> | <Approver of changes> |
|  |  |  |  |  |
|  |  |  |  |  |

# 27701 Privacy Information Management System (PIMS) Addendum

This addendum is automatically applicable for organizations implementing ISO 27701 and optional for organizations who are implementing ISO 27001 only.

* All references to “ISMS” in this document are changed to “IS&PMS”
* All references is ISO 27001 in this document are changed to “ISO 27001/27701”
* All references to “information security management system” are changed to “information security and privacy management system”