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: Information Security Objectives Plan

Document Number: 10-ISMS

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

# Purpose

The purpose of this workbook is to establish <Company Name>’s Information Security Objectives and Information Security Objectives Plan to achieve them.

# Operational Planning and performance evaluation

At <Company Name>, we understand the importance of regular and accurate monitoring and measurement of our ISMS. To align with our commitment to maintaining the highest standards of information security, we utilize the COMPANY trust management platform. COMPANY seamlessly integrates with our existing infrastructure, automating the monitoring process to ensure that our security controls operate effectively.

## Monitoring and Measurement Procedures with COMPANY

### Defining the Criteria

What to Monitor and Measure: Using COMPANY, all vital components of our ISMS, including security controls, risk management activities, and related operational processes, will be under continuous automated observation.

Methodology: COMPANY offers reliable methodologies by integrating with our infrastructure, providing consistent monitoring, and ensuring results are comparable and reproducible.

Responsibility and Timing: The designated Information Security Team will oversee the COMPANY platform, ensuring timely reviews of automatically generated insights.

### Analysis and Evaluation Procedures

Analysis of Results: The Information Security Team will regularly analyze and interpret the data provided by COMPANY.

Evaluation Methods: Leveraging COMPANY's analytical tools, standardized methods will be employed for rigorous and valid evaluations.

Responsibility and Timing: The Information Security Management Leader, with the support of the Information Security Team, will analyze and evaluate COMPANY's findings at predetermined intervals.

### Evaluation Aspects

Information Security Performance Evaluation: With COMPANY's insights, this evaluates if <Company Name> is performing as expected, gauging the effectiveness of our ISMS's processes.

ISMS Effectiveness Evaluation: COMPANY aids in determining if <Company Name> is implementing the most suitable security measures by assessing the extent to which our security objectives are met.

### Team's Contribution to Evidence

The Information Security Team will provide regular updates on evidence, aligning with both COMPANY's suggested KPIs and those defined by <Company Name>. This collaboration ensures that the ISMS remains transparent, accountable, and continually improves.

# Information Security Objectives

| **Objective Description** | **Action Plan to Achieve Objectives** | **Effectiveness Measure(s)** | **Resources Required[[1]](#footnote-2)** | **Owner[[2]](#footnote-3)** | **Expected Completion Date** |
| --- | --- | --- | --- | --- | --- |
| Implement, maintain, and improve and information security management system (ISMS) that conforms to the requirements of ISO 27001 | Establish, implement, maintain, and continually improve an ISMS and undergo ISO 27001 certification audit | 1. Obtaining ISO 27001 certification | The Board  ISMS Governance Council  Information Security Team | <Information Security Management Leader> | <Q4 2024> |
| Comply with applicable laws / regulations and customer contractual obligations | Identify applicable laws / regulations and customer contractual obligations.   Provide security Training and Awareness.  Conduct annual risk assessments | 1. Completion of Management Review  2. Less than one (1) reportable breach events  3. Remediation plans for identified regulatory and contractual risks | ISMS Governance Council  Information Security Team | <Information Security Management Leader> | N/A - ongoing |
| Protect the confidentiality of customer data | 1. Adhere to access control requirements  2. Identify and remediate high-risk vulnerabilities   3. Perform Risk Assessment  4. Perform penetration tests on production network and application  5. Perform vulnerability scans on production systems at least <frequency of vulnerability scans, e.g., quarterly>  6. Create plans to remediate high risk vulnerabilities within 60 days | 1. Less than one (1) finding in quarterly access reviews of production systems  2. Remediation plans for high-risk vulnerabilities  3. Timely completion of remediation plans | ISMS Governance Council  Information Security Team | <Information Security Management Leader> | N/A - ongoing |
| Data minimization[[3]](#footnote-4) | 1. Only collect PII needed for a business purpose  2. Ensure PII collection and processing are limited to that which PII Principles are informed of, have consented to, and/or are in accordance with a legitimate business purpose  3. Securely delete PII when no longer needed  4. Employ the following de-identification processes: <de-identification processes> | 1. 100% of SARs are responded to and closed within applicable timeframes  2. 0 complaints to data authorities  3. 0 PII data breaches | S&PMS Governance Council  Information Security Team | Information Security Management Leader | N/A - ongoing |

# Measurement Metrics and Criteria

| **Policy/Procedure/ Control** | **ISMS Control (2013)** | **Detail of measurement** | **Who Gathers Metric** | **Who Receives Metric & Frequency** | **Criteria** |
| --- | --- | --- | --- | --- | --- |
| Technical Vulnerability Management | A.12.6.1 | Vulnerabilities detected and remediated | Operations team / Service provider | <Operations team - weekly>  <ISMS Governance Council - monthly> | Critical and high vulnerabilities are remediated within SLA timelines |
| User response to phishing attempts | A.7.2.2 | User responses to phishing tests | Operations teams | <CISO & ISMS Governance Council - quarterly> | 1. Number of users who pass phishing tests  2. Users who fail tests receive awareness training |
| Lost and stolen equipment is reported and managed | A.16.1.2 A.16.1.5 | 1. Users properly report incidents 2. Incidents response is appropriate and in accordance with policy and procedure | Systems Administrators | <CISO & ISMS Governance Council - quarterly> | Reporting and response is timely and according to policy and procedure |
| System patching | A.12.6.1 | Number of systems patched / unpatched  Time to patch (TTP) | Systems Administrators | <CISO & ISMS Governance Council - quarterly> | Systems with critical or high vulnerabilities are patched in accordance with SLA timelines |
| **Policy/Procedure/ Control** | **ISMS Control (2022)** | **Detail of measurement** | **Who Gathers Metric** | **Who Receives Metric & Frequency** | **Criteria** |
| Technical Vulnerability Management | A.8.8 | Vulnerabilities detected and remediated | Operations team / Service provider | <Operations team - weekly>  <ISMS Governance Council - monthly> | Critical and high vulnerabilities are remediated within SLA timelines |
| User response to phishing attempts | A.6.3 | User responses to phishing tests | Operations teams | <CISO & ISMS Governance Council - quarterly> | 1. Number of users who pass phishing tests  2. Users who fail tests receive awareness training |
| Lost and stolen equipment is reported and managed | A.6.8 A.5.26 | 1. Users properly report incidents 2. Incidents response is appropriate and in accordance with policy and procedure | Systems Administrators | <CISO & ISMS Governance Council - quarterly> | Reporting and response is timely and according to policy and procedure |
| System patching | A.8.8 | Number of systems patched / unpatched  Time to patch (TTP) | Systems Administrators | <CISO & ISMS Governance Council - quarterly> | Systems with critical or high vulnerabilities are patched in accordance with SLA timelines |

# ISO 27001 Coverage

ISO 27001 5.2; 6.1.1; 6.2; 8.1; 9.1; 9.3.2

# 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”

1. Many roles referenced here are defined in another Vanta document. Ensure these role references correspond to roles defined in 03-ISMS Roles, Responsibilities, and Authorities. [↑](#footnote-ref-2)
2. Many roles referenced here are defined in another Vanta document. Ensure these role references correspond to roles defined in 03-ISMS Roles, Responsibilities, and Authorities. [↑](#footnote-ref-3)
3. Required objective for ISO 27701 [↑](#footnote-ref-4)