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: Procedure for Management Review

Document Number: 08-ISMS

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

# Purpose

The purpose of this procedure document is to define the management process for the periodic review and evaluation of <Company Name>’s Information Security Management System (“ISMS”) to help ensure its continuing suitability, adequacy and effectiveness as defined in section 9.3 of ISO/IEC 27001 (“ISO 27001”).

# Frequency and Timing of Reviews

At <Company Name>, management reviews of the ISMS are to be conducted at least annually to ensure its continuing suitability, adequacy, and effectiveness. For newer or less mature ISMSs, more frequent reviews will be scheduled.

# Management Review Methodology

The review methodology shall include the following steps:

| **No.** | **Task List** | **Responsibility** |
| --- | --- | --- |
| 1 | Plan and schedule the management review and inform the ISMS Governance Council | Information Security Management Leader |
| 2 | Collate and analyze the review inputs to identify items of interest (i.e., trends, issues, assessments, reports, project updates, incidents, etc.) | Information Security Management Leader |
| 3 | Review the items of interest with the ISMS Governance Council to identify decisions and actions | Information Security Management Leader |
| 4 | Accept and approve the review results including the final outputs (decisions and actions) | ISMS Governance Council |
| 5 | Document and maintain the results of the management review | Information Security Management Leader |
| 6 | Integrate the outputs of the review (decisions and actions) into the ISMS | Information Security Management Leader/Information Security Team |

# Setting the Agenda for Reviews

The Management Review agenda will include review and consideration of the following items:

1. status of actions from previous management reviews;
2. changes in external and internal issues (see 4.1) that are relevant to the ISMS;
3. changes in needs and expectations of interested parties that are relevant to the information security management system;
4. feedback on the information security performance, including trends, in:
   1. nonconformities and corrective actions;
   2. monitoring and measurement results;
   3. audit results; and
   4. fulfillment of information security objectives.
5. feedback from interested parties, including suggestions for improvement, requests for change and complaints;
6. results of information security risk assessment(s) and status of information security risk
7. treatment plan
8. opportunities for continual improvement, including efficiency improvements of both the ISMS and information security controls.

# Management Review Input

The management reviews may include the following inputs as determined by the Information Security Management Leader:

* Changes in the internal or external context of the organization
* Feedback from interested parties
* Changes in leading practice and guidance
* Changes in legal, regulatory, or contractual requirements
* Status of the ISMS objectives
* Risk acceptance criteria
* Results of the risk assessment
* Status of the risk treatment plan and implementation plan
* Effectiveness monitoring and measurement results
* Internal audit results
* Status of action items from previous management reviews
* External third-party audit observations (e.g., external certification audit)
* Status of open non-conformities, corrective actions, and improvement plans
* Trends in non-conformities and corrective actions
* The results of the training program used to assess the level of information security awareness within the organization
* High risk incidents and the related root cause analysis and action plans
* Trends in internal information security incidents
* Results of any penetration or other technical tests
* Results from any privacy-related inquiries and the company response
* Any information security contacts, inquiries, warnings or penalties from a governmental or regulatory body
* Other items at the discretion of the Information Security Leader or the ISMS Governance Council
* Status of and/or results from any information security-related audit (i.e., certification, customer, etc.)

The Information Security Team shall analyze these inputs to identify issues, attention items, questions, etc. for the ISMS Governance Council. The Information Security Team will prepare a summary of the inputs, an analysis of the inputs, and proposed key decisions and actions that are needed based on the results to improve the ISMS. For example, an issue that may be identified during the analysis of review inputs is that elements of the Implementation Plan are past due and the proposed action for the ISMS Governance Council would be to reallocate specific resources / funding needed to complete the Implementation Plan.

# Management Review Output

The ISMS Governance Council shall review the summary of the review inputs, the analysis of the inputs, and the proposed key decisions and actions. The ISMS Governance Council will approve the review, results, and any final decisions/actions needed. These decisions and actions may include the following:

* Changes to the ISMS scope and boundaries
* Action items to improve the effectiveness of the ISMS
* Modifications to the information security policies, objectives, and related procedures
* Updates to the risk assessment, risk treatment plan, and implementation plan
* Identification or modification of resource and/or funding requirements needed to improve the ISMS or to execute defined plans (e.g., implementation plan, corrective action plan, etc.)

# Procedure for the Review of Effectiveness Measures

The ISMS Governance Council shall review the effectiveness measures for ISMS controls:

* The ISMS Governance Council is responsible for reviewing the control effectiveness measures at least annually.
* The Information Security Team will prepare the meeting presentation for the ISMS Governance Council by outlining the Measurement & Metrics and adding them to the <artifact in which the ISMS Governance Council summarizes and reports measurements and metrics, e.g., to the presentation>.
* The Information Security Team will identify if the current metric exceeds the levels defined in the Measurement & Metrics criteria.
* If a metric exceeds its Criteria, then the ISMS Governance Council will discuss actions which must be taken to correct the deficiency which allowed the control to become ineffective. Actions will be recorded in the Corrective and Preventive Action Plan.

# ISO 27001 Coverage

ISO 27001 9.3.1; 9.3.2; 9.3.3; A.5.36

# 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”