COMPANY document template instructions

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

For each document section

* Consider if this section applies 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 document language such that it reflects the practices of your organization

Document completion checklist

1. Use Find to make sure that all text in angled brackets is replaced
2. Proofread your document for spelling and grammar mistakes
3. Confirm that the document’s content reflects your organization’s 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 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 your Customer Success Manager or your auditor for additional guidance.

Document Name: Procedure for the Control of Documented Information

Document Number: 05-ISMS

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

# Purpose

Documents required in support of the Information Security Management System (“ISMS”) shall be protected and controlled. This document describes the management actions needed to:

* Approve the documents for adequacy and accuracy
* Review and update documents as necessary
* Maintain version control and availability of documents
* Ensure adequate protection
* Ensure that the distribution, access, retrieval, and use of the documents are controlled
* Retain documentation as an archive where required for legal or knowledge preservation

# Scope

This procedure applies to the control of policies, procedures, evidence and records pertaining to the <Company Name>’s ISMS. For further details please refer to the 01-ISMS Scope of the ISMS document.

# Master List of Documents

A document entitled 00-ISMS Master List of Documents, which identifies ISMS management documents and information security policies, shall be maintained by the Information Security Team. The Master List of ISMS Documents shall be maintained with the correct and latest version before use.

For the purposes of this policy, “ISMS Documents” shall include both ISMS Management Policies as well as Information Security Policies.

# Format

The format of all documents will be electronic. If hard copies are required, personnel are encouraged to print directly from <location of where this file is stored, e.g., COMPANY> to ensure current versions are used. Any printed or locally saved documents are uncontrolled.

# Document Structure

ISMS Documents shall contain the following information:

* Document Name: Name of the policy, procedure, guideline, or standard
* Classification: Classification of Confidential documents shall be noted in the document footer or in the document’s metadata
* Version History: The latest version of the document and history of changes made along with the person who updated the document.
* Purpose: This defines the purpose and objective of the document

# Naming Convention

## ISMS Management Policies

ISMS management policies shall be named using the following format:

##-ISMS Document Name

* ## = Number of the document (e.g., 01, 02, etc.)
* ISMS = Information Security Management System
* Document Name = Meaningful description

## Information Security Policies

Information Security Policies shall be named using the following format:

Document Name

* Document Name = Meaningful description

# Updates and Version Control

ISMS Documents shall be updated and maintained as follows:

* Review Period: ISMS documents must be reviewed by the ISMS Governance Council at least <review period for ISMS documents, e.g., once a year or following major changes>
* Revisions: Modifications shall follow the process defined within this document for change management and approval
* Change Management: The version of documents must be updated, 00-ISMS Master List of Documents, and any related documents must be updated, and the updates must be approved by the Information Security Management Leader
* Changes to the document version number shall be made when there have been significant changes made to the document
* Changes must be communicated to all relevant personnel mentioned in the distribution list
* Approvals: Following its review, the ISMS Governance Council will confer with the Information Security Management Leader to determine any necessary changes. Unless changes are explicitly requested by the ISMS Governance Council, the ISMS Documents will be considered approved upon review

# Ownership, Approval, Issuance, Distribution, and Maintenance

* The ISMS Governance Council is the final authority, which approves the ISMS Documents. The Information Security Management Leader is responsible for implementing ISMS Governance Council directive and maintaining and approving changes to policies and procedures (including communicating the latest version of the document).
* ISMS System Documentation: The Information Security Management Leader shall act on behalf of the ISMS Governance Council for the preparation of documents or making changes to them.
* ISMS Documents Distribution: The ISMS Documents shall be uploaded to <where required recipients can view ISMS Documents, e.g., COMPANY> and shared with all required recipients
* Maintenance of ISMS Documents: All ISMS Documents shall be stored in <where required recipients can view ISMS Documents, e.g., COMPANY> and protected from damage, abuse, loss, or alteration via access controls. All ISMS Documents are maintained in a manner to be readily retrievable.

# Archival, Retention, and Disposal

* Approved documents exceeding their useful life are stored in an archive in <where archived ISMS Documents will be stored, e.g., COMPANY> in order to form an audit trail of document development.
* Archived security policies and documents will be retained in accordance with time periods specified in the Data Management Policy.
* Once it has been decided to dispose of ISMS Documents, they shall be deleted in a secure manner consistent with company policy.

# Records

Records, reports, and artifacts may be added to the ISMS Documentation Repository as needed. Examples include Risk Assessment Reports, Internal Audit Reports, Report Artifacts, etc.

## Record Naming

* Records will not follow any naming requirements
* Records should use descriptive names where possible (i.e., laptop inventory, application log, screenshot of login screen, etc.)

## Record Storage and Retrieval

Records within the ISMS will be stored and retrieved, or accessed via the following methods:

* Via the tool / system creating them
* Text and image files
* Via web browser links to the source pages

## Record Archival, Retention and Disposal

* Records exceeding their useful life are stored in a separate archive in <where to find archive of records, e.g., Google Drive> in order to form an audit trail.
* Archived records will be maintained for at least <length of record archival, e.g., one (1) year>. Once it has been decided to dispose of records, they should be deleted in a manner consistent with company policy.

# Classification

<Company Name> follows the information classification scheme set forth in the company’s Data Management Policy.

# ISO 27001 Coverage

ISO 27001 7.5.1; 7.5.2; 7.5.3; A.5.33

# 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”

# Appendix A – ISMS Document Formatting Template

Document Name: <Document Name>

Document Number: <Document #>

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

# <Category>

## <Sub-category (if applicable)>

<Text>

# <Category>

<Text>

# Version History

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