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 Corrective Action and Continual Improvement

Document Number: 09-ISMS

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

# Purpose

The purpose of this procedure document is to establish and outline the process for identifying, documenting, analyzing, and implementing corrective actions needed to remediate non-conformities or to improve the Information Security Management System (“ISMS”).

# Criteria

The following criteria may result in the identification of corrective actions and improvement opportunities which will be used to help drive the continual improvement:

* Non-conformities (“NC”) (major and minor) or observations identified during third-party audits (e.g., certification audits)
* Opportunities for Improvement (“OFI”) or observations identified during internal audits

# Plan Requirements

The corrective action and improvement plan items shall be added to the Risk Register and Treatment Plan and shall contain the following information at a minimum:

* Risk description or vulnerability
* Risk treatment plan or corrective action
* Risk or implementation owner
* Remediation ticket reference number(s) (if relevant)

The Information Security Team shall validate that the following supporting documentation is updated, if needed, based on the results of the completed corrective action (or improvement):

* Internal and external factors within the ISMS scope and boundaries
* Controls, policies, and procedures
* Risk Assessment and Risk Treatment Plan
* Effectiveness measure of the control.

# Monitoring

On an annual basis, the ISMS Governance Council shall monitor the status of any open items on the corrective action and improvement plan and discuss actions needed to complete these items.

# ISO 27001 Coverage

ISO 27001 6.1.1; 10.1; 10.2

# 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”