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: Information Security Communication Plan

Document Number: 06-ISMS

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

# Purpose

This document defines the considerations and steps to be used when communicating information relevant to <Company Name>’s Information Security Management System (“ISMS”), including its purpose and importance to internal and external parties.

# Content of Communications

Communications external to <Company Name> may include mention of the ISMS program, the certifying body, the ISMS scope statement, and the <Company Name> Management Team.

Any external request for documentation or specifics regarding the ISMS requires the approval of the Information Security Management Leader or a member of the ISMS Governance Council, as well as a signed non-disclosure agreement.

# Recipient of Communications

Internal program level communications will be distributed to all in-scope personnel or to pre-defined distribution lists. ISMS management will also directly communicate to specific roles based on their responsibilities.

External communication delivery will be defined for each business case and can include regulators.

# Originator of Communications

The content of materials communicated shall be originated by any of the below:

* ISMS Governance Council
* CIO
* Information Security Management Leader
* Information Security Team (internal only)

# Timing and Mechanism of Communications

The internal publication of the ISMS current state, scope, and operation shall be performed as the ISMS changes or as needed. Internal certification notices will be communicated annually through e-mail or via an alternate method of communication chosen by <Company Name>.

External communication will be on an on-demand basis with customers, prospects, regulators, government agencies (if applicable), and approved third parties.

# Communication Plan

The internal publication of the ISMS current state, scope, and operation shall be performed as the ISMS changes or as needed.

| **Content** | **Internal / External** | **Recipient(s)** | **Originator(s)** | **Timing\*** | **Mechanism(s)** | **Approval Required** |
| --- | --- | --- | --- | --- | --- | --- |
| * ISMS & InfoSec Policies * Information Security Objectives * Current state of the ISMS * Certificate details | Internal | * ISMS Governance Council * Relevant staff and contractors | Information Security Management Leader | Annually or as needed | * Email * Live presentation * Alternate method chosen by <Company Name> | None |
| * Highlights and summaries of risk assessment reports * Internal audits * Test results * Incident reports * Actions related to continuous improvement * Coordination of activities * Project timelines * Management of ISMS | Internal | * ISMS Governance Council * Relevant staff and contractors | * Information Security Management Leader * Information Security Team | Annually or as needed | * Email * Live presentation * Alternate method chosen by <Company Name> | None |
| * Confidentiality Agreements * Company Handbook containing company policies * Standards of Conduct * Information security policies including the Acceptable Use Policy shall be communicated to users | Internal and limited external | * Employees * Relevant contractors | Information Security Management Leader | Time of hire | * Email * Learning management system, Classroom * Alternate method chosen by <Company Name> | None |
| * ISMS Scope & Boundaries * Information Security Policy * Statement of Applicability * Evidence for ISMS controls (i.e., Annex A/SOC 2) | Internal and limited external | Third-party auditors (ISO 27001) | * ISMS Governance Council * Information Security Management Leader * Information Security Team | Annually | * Interview, observation * Document upload | Information Security Management Leader |
| * Statements of work (expectations of work and SLAs) * Confidentiality agreements * Relevant policies | External | Contractors | Information Security Management Leader | Time of engagement | * Email * Written agreement * Other mechanisms as needed | * Legal * Information Security Management Leader |
| * Incident Reports * Root Cause Analysis Reports | Internal | * Information Security Team * Relevant employees * ISMS Governance Council as needed | Information Security Team | Within <report sharing commitment, e.g., seven (7) days> of incident resolution | * Reports * In-person meeting * Other mechanisms as determined by the Information Security Management Leader | None |
| Relevant incidents and breach reporting | External | * Customers * Law enforcement * Regulatory bodies * Supervisory authorities | * President / CEO * Legal / General Counsel * Information Security Management Leader | Per legal or contractual requirements | * Email * Written letter * Other mechanisms as legally required, needed, or chosen by <Company Name> |  |
| General security reminders and awareness communications | Internal | Employees and relevant contractors | Information Security Management Leader | Ad-hoc | * Email * In-person meetings | None |

# ISO 27001 Coverage

ISO 27001 7.3; 7.4

# 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”