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 Internal Audits

Document Number: 07-ISMS

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

# Purpose

This policy delineates the approach to conducting internal audits to ensure the conformity, effectiveness, and continuous improvement of the organization's ISMS to both the organization's requirements and the ISO/IEC 27001 standards. The purpose of this procedure is to establish a framework for planning, conducting, and reporting on an internal audit of the <Company Name>’s Information Security Management System (“ISMS”). An internal audit is used to help determine whether the ISMS control objectives, controls, and policies and procedures:

* Conform to the applicable requirements of the ISO/IEC 27001 (“ISO 27001”) standard
* Conform to the identified information security requirements
* Are effectively implemented, maintained, or have opportunities for improvement

# Scope

The audits will cover all elements of the ISMS for all in-scope information assets and the applicable controls identified within the Statement of Applicability.

# Internal audit policy statements

Audit Frequency and Scheduling:

Internal audits of the ISMS will be conducted at planned intervals. The exact intervals and areas to be audited will be determined based on the organizational risk, complexity, and size, and shall be communicated annually.

Audit Principles:

All ISMS internal audits shall adhere to the principles of integrity, fair presentation, due professional care, confidentiality, independence, and an evidence-based approach.

Audit Program Management:

Internal audits shall be performed annually and shall include the complete scope of the ISMS unless otherwise specified. This program shall ensure a holistic review of all ISMS processes and controls within a defined timeframe. Adjustments to the program may occur based on audit findings and the evolving risk landscape.

Auditor Competence & Team Selection:

Auditors, whether internal or external, shall be selected based on their demonstrated competence, sector-specific knowledge, and understanding of information security. The organization commits to continuous monitoring and evaluation of auditor performance to maintain the highest audit standards. In situations where internal resources are inadequate, external auditors may be appointed. These external auditors should be equipped with sufficient knowledge about the organizational context.

Audit Execution and Reporting:

The Internal Auditor shall prepare audit plans by considering outcomes of previous audits and identified risks. These plans will guide the audit process, specifying the criteria, scope, and methods of the audit. Upon audit completion, a detailed report will be furnished and presented to top management, outlining findings, identified nonconformities, and recommended actions.

Addressing Nonconformities:

Any identified nonconformities during the audit process shall be addressed with a detailed action plan. This plan will describe the nonconformity, its cause(s), proposed corrective actions, and assign responsibility for implementing these actions.

# Auditor Selection

The Information Security Team may engage a third-party vendor knowledgeable in performing ISO 27001 internal audits. The selection of the auditor(s) shall be reviewed and approved by Senior Management. The auditor(s) shall be evaluated and selected based on their objectivity and impartiality in the auditing process. The auditor(s) should also be trained and/or otherwise qualified to perform the internal audit of an ISMS. It should also be confirmed that there is proper segregation of duties while choosing an auditor (i.e., the auditor has not implemented or does not operate or review any of the controls under audit).

The auditor(s) shall be evaluated based on their education and experience to validate their competence.

# Resources

The third-party or internal auditor(s) will carry out the internal audit process with input from the Information Security Management Leader and the Information Security Team.

The primary responsibilities of the auditor are as follows:

* To plan the ISMS internal audit(s) as per the defined frequency and schedule
* To conduct the internal audit as per the audit plan and to share the results of the audit findings with the Information Security Leader for review and approval
* To ensure the confidentiality and integrity of the audit data and the supporting evidence within the auditor’s control
* To provide all audit records to the Information Security Leader as requested
* To identify the corrective actions to be taken to close any identified audit observations/non-conformities, to review the actions taken to close the gaps reported, and to evaluate the effectiveness of such actions

# Frequency & Schedule

The frequency of the internal audit is scheduled to be conducted <frequency of internal audit, e.g., annually> at minimum. The ISMS Governance Council will determine if the frequency of the audit needs to be increased depending upon the number of findings identified during the audit, the severity of the previous audit findings, and the operating efficiency of conducting the audit annually.

# Audit Criteria

The audit criteria shall take into consideration the defined set of ISMS policies and procedures, any regulatory, legal, and contractual requirements, ISO 27001, and any additional authoritative standards as necessary.

# Evaluation Criteria

A non-conformity (“NC”) is a gap against the ISO 27001 standard which may have an adverse effect to the interests of ISMS.

* Major NC - the adverse effect is immediate and directly impacts the ISMS’ ability to achieve its objectives
* Minor NC - the effect may take place over a period of time and does not immediately adversely impact the ISMS
* Conforms - controls are designed and operating effectively in accordance with the requirements of ISO 27001
* Opportunity for Improvement (“OFI”) - an observation may arise out of an opportunity for improvement

# Alternative Labeling of Findings

<Company Name> reserves the right to apply any appropriate internal audit of information security controls to the ISO 27001 internal audit requirements. Alternative audit approaches may identify findings using alternate terms such as “Yes/No/Partial,” or “In Place/Not in Place.” In cases where an alternate standard or approach is applied to the ISO 27001 internal audit requirements, the controls will be “mapped” to ISO 27001 Controls and the finding language will be mapped to ISO 27001 evaluation criteria. For example, controls labeled, “Yes,” and, “In Place,” may be mapped to ISO 27001 as, “Conforms.”

# Audit Documentation

The internal auditor shall audit the ISMS policies and procedures, implemented information security controls, and the effectiveness of the ISMS against the ISO 27001 standard requirements. Artifacts and documents may be collected as evidence by the auditor in addition to observations and interviews.

# Audit Reporting

The internal auditor shall document the audit results and observations along with the supporting evidence. A final report will be produced and shared with the Information Security Leader for initial review and finalization. Highlights of the internal will be communicated to the ISMS Governance Council. The complete internal audit report will be provided to the ISMS Governance Council upon request. An internal audit report will show the audit results including non-conformities and observations.

# Audit Records Retention

The evidence collected and the documentation prepared as part of the internal audit shall be protected and retained in accordance with the requirements defined within the 05-ISMS Procedure for the Control of Documented Information document.

# ISO 27001 Coverage

ISO 27001 9.2.1; 9.2.2; A.8.34, A.8.35, A.8.36

# 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”