Corporate / Business Logo

# ISMS Policy and Scope Statement

## Operational Area / Process Area

Document Authorization

Name
Title

| | |
|---|---|
| Version: | |
| Date of Version: | |
| Created by: | |
| Approved by: | |
| Classification Level: | |

## Table of Contents

# 1. Purpose, Scope and Users

## 1.1. Purpose

This procedure establishes an Information Security Management System (ISMS) policy and scope statement.

## 1.2. Scope

The procedure addresses information security policy and scope, as necessary to meet ISMS objectives.

## 1.3. Users

This document applies to all personnel at Your Company and relevant external parties, including external providers who become obligated to adhere to this procedure by agreement with Your Company.

# 2. Responsibilities and Authorities

It is the responsibility of all personnel and employees of Your Company to implement and maintain the requirements of this procedure. It is the responsibility of all personnel to effectively communicate the requirements of this procedure (internal communication) to applicable functional groups, support teams, and other personnel involved in the effective implementation and continual improvement of the ISMS.

It is the responsibility of top management to review the policy and scope statement from time-to-time, provide guidance and continual improvement regarding policy and scope, and provide ultimate approval of the ISMS Policy and Scope.

The Appropriate Role has primary responsibility and approval authority for this procedure, including any changes, amendments, or updates.

# 3. Organizational Context

In this section, provide a brief history of your organization, how the organization arrived at an ISMS decision, and the general context of the organization in relation to the ISO International Standard. Provided below is an example that may be used as guidance for this section.

Your Company is a public/private organization with its principal place of business in city/state/nation/location. Briefly describe your business, products, services, etc.

Like many contemporary business organizations of this size and advanced complexity, Your Company has taken steps to ensure integrity and security in data, online access, and the management of data services. Your Company has implemented policies and procedures to protect employees, contractors, external providers, and other stakeholders, while offering the broadest possible range of services in its business pursuits. These efforts include establishing a management committee of leadership personnel that is responsible to ensure data protection and integrity. Your Company establishes policies and develops rules and guidelines for information security and the handling of security incidents.

In furthering the efforts of the organization, Your Company has adopted security standards recommended by the International Organization of Standardization, commonly known as ISO. ISO/IEC 27001:2022 is the International Standard for Information Technology – Security Techniques – Information Security Management System Requirements. By implementing the requirements of ISO 27001, Your Company helps ensure a system that preserves confidentiality, integrity, and availability of secure data, partially by applying risk management processes and giving confidence to interested parties that risk to information is adequately managed.

Corporate / Business Logo

# Document Control Procedure

## Operational Area / Process Area

Document Authorization

Name
Title

| | |
|---|---|
| Version: | |
| Date of Version: | |
| Created by: | |
| Approved by: | |
| Classification Level: | |

# 5. Configuration Management

## 5.1. Document Numbering

All controlled documentation shall be subject to document identification and revision control. The document numbering methodology shall be as follows:

XXX-Code1-###

where:

| XXX | Code 1 | | ### |
|---|---|---|---|
| Designates the document as a controlled document for Your Company | P | Procedure | Sequential Number |
| | WI | Work Instruction | Sequential Number |
| | F | Form | Sequential Number |
| | A | Ancillary Document | Sequential Number |

## 5.2. Revision History

Revision changes shall be documented, to include the new version number, the major changes made, the date of approval, and the last person to create or authorize the document.

A document revision (version history) block is required for procedures and work instructions. The document revision (version history) block shall be the last section of a document, unless it is appropriate to place it elsewhere. Revision change information described immediately above may be recorded in this area.

## 5.3. Formatting

In general, the following formatting shall be used for controlled documentation:

- Left and right margins shall be 1.0 inch.
- Top and bottom margins shall be 1.0 inch (it is acknowledged that the bottom margin may sometimes be enlarged in order to include document identification, security information, etc.).
- Appendices, when used, should be referenced in the body of the document.

It is acknowledged that these are general formatting suggestions and are not firm requirements. A variation from these suggestions is not reason for audit nonconformance.

All controlled documents shall be approved. If electronic signatures are used, then objective evidence of review and approval shall be maintained as part of documented information and records.

## 5.4. Documented Information Review

Documented information shall be reviewed for suitability and adequacy. Review is accomplished by the following activities:

- Documented information is reviewed during internal audits.
- Status of documented information may be reviewed during Management Reviews.
- If not otherwise reviewed, documented information shall be reviewed at least once every three years by appropriate process owners.