Document Control Policy Template

Document Control Information

- **Document Title:** Document Control Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Document Control Policy establishes [ORGANIZATION NAME]'s approach to creating, updating, and controlling documented information in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that all ISMS documentation is properly managed throughout its lifecycle.

1.2 Scope

This policy applies to all documented information required by the ISO 27001:2022 standard and determined by [ORGANIZATION NAME] as necessary for the effectiveness of the Information Security Management System (ISMS), including: - Policies and procedures - Process descriptions - Work instructions - Forms and templates - Records and evidence - External documents

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Ensuring all ISMS documentation is properly identified, formatted, reviewed, and approved - Controlling access to and distribution of documented information - Protecting documented information from improper use, loss of integrity, or compromise of confidentiality - Maintaining documented information in a manner that ensures it is available and suitable for use when needed

2. Document Creation and Updating

2.1 Document Identification

All ISMS documents shall be uniquely identified with: - A descriptive title - A document reference number or identifier - A version number or date - The document owner or author - The document approver

2.2 Document Format and Structure

ISMS documents shall follow a consistent format and structure that includes: - Document control information (title, version, date, owner, approver) - Purpose and scope - References to related documents - Definitions of terms and abbreviations where necessary - Main content organized in a logical manner - Appendices or attachments as needed

2.3 Document Review and Approval

All ISMS documents shall be: - Reviewed for adequacy and suitability prior to issue - Approved by authorized personnel before release - Re-reviewed and re-approved after updates or changes - Reviewed at planned intervals, at least annually

2.4 Document Changes and Version Control

Changes to ISMS documents shall be: - Clearly identified and tracked - Reviewed and approved by the same functions that performed the original review and approval - Accompanied by an updated version number or date - Summarized in a document change log or history

3. Document Control

3.1 Document Availability

[ORGANIZATION NAME] shall ensure that: - Documents are available where and when needed - Documents are accessible to authorized personnel - Documents are protected from unauthorized access - Documents are retrievable in a timely manner

3.2 Document Distribution

The distribution of ISMS documents shall be controlled to ensure that: - Only current versions are available at points of use - Obsolete documents are promptly removed or protected from unintended use - Documents of external origin are identified and their distribution controlled

3.3 Document Storage and Preservation

ISMS documents shall be stored and preserved in a manner that: - Maintains their legibility and retrievability - Prevents damage, deterioration, or loss - Ensures backup copies are maintained where appropriate - Allows for recovery in case of disaster or system failure

3.4 Document Protection

[ORGANIZATION NAME] shall protect ISMS documents from: - Unauthorized changes or modifications - Unintended alterations or deletions - Unauthorized disclosure or access - Loss of confidentiality or integrity

3.5 Document Retention and Disposition

[ORGANIZATION NAME] shall: - Define retention periods for different types of documents - Ensure documents are retained for the specified period - Securely dispose of documents when no longer required - Maintain records of document disposition where required

4. Document Types and Classification

4.1 Document Hierarchy

[ORGANIZATION NAME] shall maintain a hierarchical structure of ISMS documentation: - Level 1: Policies (high-level statements of intent and direction) - Level 2: Procedures (detailed steps to implement policies) - Level 3: Work instructions and guidelines (specific instructions for tasks) - Level 4: Forms, templates, and records (evidence of activities performed)

4.2 Document Classification

ISMS documents shall be classified according to their sensitivity and confidentiality requirements: - Public: Documents that can be freely distributed outside the organization - Internal: Documents for general use within the organization - Confidential: Documents with restricted access within the organization - Restricted: Highly sensitive documents with strictly controlled access

4.3 External Documents

External documents relevant to the ISMS shall be: - Identified and registered in the document control system - Reviewed for relevance and applicability - Made available to appropriate personnel - Updated when new versions are released

5. Document Management System

5.1 Document Repository

[ORGANIZATION NAME] shall maintain a centralized repository for ISMS documents that: - Provides secure storage for all documents - Enables version control and change tracking - Facilitates document search and retrieval - Controls access based on user roles and permissions

5.2 Document Master List

A master list of all ISMS documents shall be maintained, including: - Document title and identifier - Current version number and date - Document owner and approver - Review frequency and next review date - Document classification and access restrictions

5.3 Document Access Control

Access to ISMS documents shall be controlled based on: - User roles and responsibilities - Need-to-know principle - Document classification - Authentication and authorization mechanisms

6. Roles and Responsibilities

6.1 Document Owner

- Ensure document content is accurate and up-to-date
- Initiate document reviews and updates
- Approve changes to the document
- Ensure document users are informed of changes

6.2 Document Controller

- Maintain the document control system
- Assign document identifiers and version numbers
- Ensure proper formatting and structure
- Distribute documents to authorized users
- Archive obsolete documents

6.3 Document Approver

- Review documents for adequacy and suitability
- Approve documents for release
- Ensure documents align with organizational policies and objectives

6.4 Document Users

- Use only current versions of documents
- Follow document control procedures
- Suggest improvements or updates when needed
- Report any issues with documents

7. Compliance and Monitoring

7.1 Compliance Verification

[ORGANIZATION NAME] shall verify compliance with this policy through: - Regular document audits - Management reviews - System access logs and reports - User feedback and suggestions

7.2 Performance Metrics

The effectiveness of document control shall be measured using: - Number of document control non-conformities - Time taken to approve and publish documents - User satisfaction with document availability and usability - Incidents related to document control issues

8. Related Documents

- Information Security Policy
- Records Management Procedure
- Document Template Guidelines
- Document Change Request Form
- [LIST OTHER RELEVANT DOCUMENTS]

9. Approval

This Document Control Policy is approved by:

Name: _______________________ Position: _____________________ Date: ________________________ Signature: ____________________