**Document and Record Control Procedure**

Version:

Date:

Classification

Document Control

|  |  |  |
| --- | --- | --- |
| 1. | Document Number: |  |
| 2. | Version History: |  |
| 3. | Created Date: |  |
| 4. | Created By: |  |
| 5. | Approved By: |  |
| 6. | Contact: |  |

Document Modify History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modified By | Modification |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Objectives, Focus Area and Usable Parties 4](#_Toc179641308)

[Reference Documents 4](#_Toc179641309)

[Control of Internal Document 5](#_Toc179641310)

[Document Approval 7](#_Toc179641311)

[Document Distributing 8](#_Toc179641312)

[Document of external Origin 8](#_Toc179641313)

[Maintaining diary notes for records based on this document 8](#_Toc179641314)

[Lifestyle of Records 9](#_Toc179641315)

[Validity and Document Management 10](#_Toc179641316)

# Objectives, Focus Area and Usable Parties

**Objectives:**

This approach aims to show how to control and manage the production, review, launch, usage, and ongoing maintenance of documents and records, commonly known as "documented information," within the context of the Information Security Management System (ISMS).

**Focus Area:**

This process applies to all papers and data related to the ISMS, no matter their origin—whether they were produced within the organization or sourced externally. This technique covers all kinds of papers and records.

**Usable Parties:**

This document can be utilized by any employees of [organization name] who carry out tasks related to the ISMS.

# Reference Documents

* ISO/IEC 27001 Standard, clause 7.5
* Information Security Policy
* Policy Handling Classified Information
* [Other documents and Regulation specifying document control]

# Control of Internal Document

The management team at [Organization name] will request for the documentation to be prepared, and anyone suitable for the topic and level of the document can complete it. There are still a few guidelines to keep in mind when making a document for the ISMS.

1. **Document Format:**

Every text in this document is formatted in “Times New Roman.” Every level 1 heading is bold and set in a 16-point font size. Level 2 headings are bold and have a font size of 14.

The header of the document includes the name of the organization and the title of the document. The footer includes the organization's name, the page number, and the confidentiality level.

1. **Version Control:**

Document version numbers will have a simpler format, consisting of only one major number. For instance, Version 2 is denoted by "V2".

A document will initially be created with a version number of 1 and be referred to as a "Draft." Every time a draft is shared and subsequently revised, the draft number will increase by 1. For example, it will shift from "1" to "2."

When a document is first generated, for example, it is produced as "Version 1 Draft 1." The upcoming iterations will be designated as "V1 Draft 2," and so on. After it is authorized, the document moves on to "V1 Final."

The version number will grow each time a new version in draft form is created. When a document is revised and moves from "V1 Final" to "V2 Draft 1," "V2 Draft 2," and so on, until clearance is obtained, the modified document will be categorized as "V2 Final."

1. **Version History:**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Created by | Summary of Changes |
|  |  |  |  |
|  |  |  |  |

1. **Status of the Document:**

* The term "Draft" denotes that it is still in the draft stage and is subject to revision. For example, it has not yet received approval.
* The term "final" indicates that it has received approval and may now be used in actual professional settings.

1. **Review of the Document:**

|  |  |
| --- | --- |
| Document type | Reviewed by |
| Strategy |  |
| Policy |  |
| Procedure |  |
| plan |  |

# Document Approval

Every document must pass the approval board's inspection process to ensure that its purpose and content are accurate and appropriate for the infrastructure of the company.

|  |  |
| --- | --- |
| Type of the document | Approved by |
| Strategy |  |
| Procedure |  |
| Policy |  |
| Plan |  |

There should be a table for each document that needs to be approved.

**Approval:**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signature | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

For a document to get approved, it needs to be endorsed and signed electronically by someone who is authorized. Instead of using a physical printout, it's better to do this process electronically. When a new version of a document gets approved, people using the old version are expected to switch to the updated one.

# Document Distributing

|  |  |
| --- | --- |
| Name | Title |
|  |  |
|  |  |

It's really important to keep this information accurate because it helps document users know when a new version is available.

# Document of external Origin

Some parts of the ISMS are attached to the header of documents on the front page, usually found in documents that come from outside sources. The elements include document reference, date, version, status, and distribution.

Documents obtained from outside sources will go through the same control measures as those created internally.

# Maintaining diary notes for records based on this document

To ensure accessibility in every situation, all finished papers should be kept in both electronic and printed formats. The electronic archives of ISMS papers on the shared drive are organized into relevant subfolders, like management responsibility, management review, and so on. All qualified members of [organization name] can access this shared drive according to the Access Control Policy.

Final papers are stored in a physical format that looks a lot like their digital version. Can you tell me where the paper files are located? The Definitive Media Library is going to get a complete copy of the final documentation, which will be put together separately.

* **Document Archiving and Disposal:** Approved papers that have outlived their usefulness are safely stored in a designated "superseded" folder on the shared drive. To create an audit trail that demonstrates how documents have been used and altered over time, this process is required. It would be best to clearly mark them as "superseded" to avoid anyone mistakenly using them as the latest version. Paper copies of these authorized documents that have been replaced should be disposed of in accordance with the specified asset handling procedures. This technique of disposal typically involves a shredder or lockable containers to secure sensitive information.

# Lifestyle of Records

1. **Identification:**

Different kinds of records—like security incident logs, change requests, configuration items, and security event logs—within the ISMS correspond to different processes. More general documents, such as minutes from meetings, might also be applicable to other procedures. With the use of instruments that have distinct numbering systems, such as INC00001 for security incidents or CHG00001 for changes, many of these data are automatically detected. Regarding records that were manually created:

* The minutes from the meeting will be titled based on the subject and the date of the meeting.
* Reports will be titled according to the subject of the report and the time frame it covers.
* Logs will be titled with the log name and the date/time they cover.

1. **Storage:**

Records in the ISMS are stored in application databases that are created for specific functions, like the security incident database. A logical filing structure will be set up for non-database records to match the ISMS areas.

1. **Protection:**

Application databases have regular backups according to the backup policy we agreed on. File storage areas are backed up regularly, and the most recent backups are safely kept offsite. Access to records is managed in line with the [company name] Access Control Policy.

1. **Retrieval, Retention and Disposal:**

The programs that manage record creation are key to retrieval, with the service desk system and event viewers being really important in this process. Reporting tools help process data so that we can analyze it more intelligently. ISMS records are kept depending on how useful they are over time and the need to comply with responsibilities, with specific retention periods outlined in the Records Retention and Protection Policy. When it's time to get rid of documents, it's really important to use the right software for safe deletion, and shredding the hard disc is essential for the hardware. In line with the established Asset Handling Procedures, paper records that are ready for destruction are carefully destroyed.

# Validity and Document Management

The document's validity commences on: [date]

As the document's owner, [job title] is in charge of carrying out routine inspections and making the required revisions, at least once a year.

When executing this procedure, the following criteria must be adhered to:

* All documents must be created in accordance with the procedures outlined in this document.
* Every document must undergo a controlled process for creation, approval, distribution, utilization, and updates.

[Job Title]

[Name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Signature]