# PROCEDURE FOR DOCUMENT AND RECORD CONTROL

|  |  |
| --- | --- |
| Code | IT-2024-0002 |
| Version | **1.2** |
| Created by | **ISO** |
| Approved by | **Ms. Tharu - CISO** |
| Confidentiality level | **High** |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Created by | Description of change |
| 2024-10-19 | 1.0 | Mr.Dilshan - ISO | Initial completed |
| 2024-11-19 | 1.2 | Ms.Tharu - CISO | Reviewed and Checked |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Purpose, scope, and users 3](#_Toc148450734)

[Reference documents 3](#_Toc148450735)

[Document control procedure 3](#_Toc148450736)

[Naming Convention 3](#_Toc148450737)

[Version Control 4](#_Toc148450738)

[Version History 5](#_Toc148450739)

[Document Status 5](#_Toc148450740)

[Documents of External Origin 5](#_Toc148450741)

[Document review 6](#_Toc148450742)

[Document Approval 6](#_Toc148450743)

[Approval 6](#_Toc148450744)

[Communication and Distribution 7](#_Toc148450745)

[Distribution 7](#_Toc148450746)

[Review and Maintenance of Documents 7](#_Toc148450747)

[Archival of Documents 7](#_Toc148450748)

[Disposal of Documents 8](#_Toc148450749)

[Records Lifecycle 8](#_Toc148450750)

[Identification 8](#_Toc148450751)

[Storage 8](#_Toc148450752)

[Protection 9](#_Toc148450753)

[Retrieval 9](#_Toc148450754)

[Retention 9](#_Toc148450755)

[Disposal 9](#_Toc148450756)

# Purpose, scope, and users

Purpose: This procedure ensures control and integrity in managing documents and records within Information Security Management System (ISMS).

# Scope: It covers all ISMS-related documents and records, regardless of their origin or format, to maintain information security.

# Users: All employees operating under the ISMS should adhere to this procedure. It's a guide for document and record control practices within the organization

# Reference documents

* ISI/IEC 27001 standard, clause 7.5
* Information Security Policy
* Policy handling classified information

# Document control procedure

The content of the paper is written in the Calibri font, size 11. The font size 14 bold is used for chapter titles, while the font size 12 bold is used for level 2 chapter titles. The chapter titles of Level 3 are written in font size 11 bold italic.

The document header includes the name of the organization as well as the level of confidentiality. The footer includes the document's name, current version, and date, as well as the page number.

The documentation will be created at the request of the Orion Capital Finance PLC management team and may be completed by any element individual who is relevant to the subject and level of the document. However, there are several rules while preparing a document to be used in the ISMS.

## Naming Convention

Naming convention format:

ISMS-DOC-xx-yy Document Title Vn Status dd

ISMS = Information Security Management System

DOC = Document

xx = Subject are reference (Table 1)

yy = Unique document number

Document Title = Meaningful description of document

Vn = Version n

Status = status of document (draft or final)

dd = Number of drafts, if appropriate

Subject areas references are designed to map onto sections of the ISO/IEC 27001 standard as follows.

|  |  |
| --- | --- |
| Subject Area Reference | ISO/IEC 27001 subject are |
| 00 | Introduction and project resources |
| 01 | 1. Scope |
| 02 | 1. Normative references |
| 03 | 1. Terms and definitions |
| 04 | 1. Context of the organization |
| 05 | 1. Leadership |
| 06 | 1. Planning |
| 07 | 1. Support |
| 08 | 1. Operation |
| 09 | 1. Performance evaluation |
| 10 | 1. Improvement |
| A05 | A5. security policy |
| A06 | A6. Organization of information security |
| A07 | A7. Human resource security |
| A08 | A8. Asset management |
| A09 | A9. Access control |
| A10 | A10. Cryptography |
| A11 | A11. Physical and environmental security |
| A12 | A12. Operations security |
| A13 | A13. Community security |
| A14 | A14. System acquisition, development, and maintenance |
| A15 | A15. Supplier relationships |
| A16 | A16. Information security incident management |
| A17 | A17. Information security aspects of business continuity management |
| A18 | A18. Compliance |

## Version Control

Document version numbers will only contain a major number. Example: V2 is Version 2.

When a document is created for the first time it will have a version number of 1 and be in a status of Draft. Each time a draft is distributes, and further changes will result in the draft number being incremented by 1. Example: from 1 to 2. Or 1.2 – 2.0

For example, when document is first created it will be Version 1 draft 1. A second draft will be V1 Draft 2 etc. when the document is approved it will become V1 final.

The version number will be incremented when a subsequent version is created in draft status.

For example, a revision of an approved document which is at V1 Final will be V2 Draft 1 then V2 Draft 2 etc. until approved when it will become V2 Final.

Documents must be including a revision history as follows:

### Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Revision Author | Summary of Changes |
| 1.0 | 09-10-2022 | Mr.shanaka - ISO | Year Review |
|  |  |  |  |

Once the document reaches its final version, only approved versions should be recorded in this table.

## Document Status

The status reflects the stage that the document is at, as follows:

Draft = under development and discussion. Example: it has not been approved

Final = following approval and release into live work environment

## Documents of External Origin

Documents that originate outside of the organization, but from part of the ISMS will be allocated a reference and a header page attached at the front of the document, setting out information that is normally in internal documents.

Example:

* Document reference
* Version
* Date
* Status
* Distribution

Such documents will then be subject to the same control as those that originate internally.

## Document review

Draft document will be reviewed by a level and number of staff appropriate to the document content and subject.

Guidelines are as follows:

|  |  |
| --- | --- |
| Document type | Reviewers |
| Strategy | IOS |
| Policy | CISO |
| Procedure | GRC |
| plan | CISO |

Once approved, the date of next schedule review should be recorded in the information security management system documentation log.

## Document Approval

All documents must go through an approval board to ensure that they are correct fit for purpose and produced within local document control guidelines. The board will differ dependent upon the type of document and may go to numerous groups prior to being approved.

In standard terms, approval boards are:

|  |  |
| --- | --- |
| Document type | Approvers |
| Strategy | CISO |
| Policy | CISO |
| Procedure | CISO |
| plan | CISO |

Each document that requires approval should have a table for the purpose as shown below:

### Approval

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signature | Date |
| Mr.Shashi | CISO | Digital | 09-10-2023 |

Once approved a copy of the document must be printed and signed by the approver. [Note – you may choose to do this electronically rather than by printing a copy]. This copy will then be retained in a central file.

Upon approval of a new version of a document, all holders of previous versions will be instructed to obtain a new version and destroy the old one.

## Communication and Distribution

A distribution list will be included as follows:

### Distribution

|  |  |
| --- | --- |
| Name | Title |
| Management Review | Management Review V2.0 |
|  |  |
|  |  |

This must be accurate as it will be used as the basis for informing users of the document that new version is now available.

## Review and Maintenance of Documents

All final documents n=must be stored electronically and in paper format both locally and off-site to ensure that they are accessible in any given situation.

ISMS documents are stored electronically on the shared drive under relevant sub-folder (e.g., management responsibility, management review etc.). The drive is a shared drive to which all appropriate members of [organization name] have access, in line with the published Access Control Policy.

Final documents are stored in paper format in a filing structure that mimics the electronic version. [state the location of the paper files].

A full copy of final documentation will be reproduced and stored within the Definitive Media Library.

## Archival of Documents

Approved documents exceeding their useful life are stored in a superseded folder on the shared drive-in order to form an audit trail of document development and usage, they should be marked as being superseded to prevent them being used as a latest version by mistake.

## Disposal of Documents

Paper copies of approved documents that have been superseded are to be disposed of in secure bins or shredded, in line with agreed Asset Handling Procedures.

# Records Lifecycle

This section describes the control of the type of documented information that generally shows what been done i.e., is a record of activity such as a completed from, security log or meeting minutes.

## Identification

There is a variety of type of record that may from part of the ISMS, and these will be associated with specific processes that are involved, such as:

* Security incidents
* Change requests
* Configuration items
* Security event logs

In addition, there will be more general items such as meeting minutes which could apply across processes, in terms of identification, in many cases this will be dictated by the tool creating record for example a unique numbering system such as INC00001 for security incident or CHG00001 for changes will be used by the tool.

For those record that are manually created the following rules will apply:

1. Meeting minutes will be named according to the subject of the meeting and the date.
2. Reports will be named according to the subject of the report and the reporting period.
3. Logs will be named with the title of the log and the date/time covered.

For any other types of record not covered, the creator should use common sense to ensure that the name choose gives a good indication as the contents of the file and it should be stored in a location relevant to its purpose.

## Storage

many records within the ISMS will be stored in application databases specially created for the purpose i.e., the security incident database.

For none-database records a logical filing structure will be created according to area of the ISMS involved.

[describe the feeling is structure on your server in which you will store your ISMS records.]

## Protection

Records held in application database will be subject to regular backups in line with the agreed backup policy. File storage areas will also be backed up regularly, with all latest backups held at an offsite location.

Records will be restricted to authorized individuals in accordance with the [company name] Access Control Policy.

## Retrieval

Records will generally be retrieved application that created them, i.e., the service desk system for security incidents and an event viewer for logs.

Reporting tools will also be used to process and consolidate data into meaningful information.

## Retention

The period of retention of records within the ISMS will depend about their usefulness to [company name] an any legal, regulatory, or contractual constraints. Security related service desk records the useful for historical trend analysis and so will be kept for a period at least seven years. Care will be taken where records may have some commercial relevance in the event of dispute, example contracts and minutes of meeting with suppliers and these should be kept for the same length of time.

Records that are particularly detail and only relevant for a short period of time such as server event logs should only be kept as long as there is an immediate requirement for them.

Specific retention periods are set out in the records Retention and Protection Policy.

## Disposal

Many systems provide for the concept of a archiving and in most cases, this should be used rather than deletion. however once has been decided to dispose of a set of records they should be records deleted using the appropriate software, i.e., the service desk system will provide a facility to delete security incident records.

If such records are held on hardware that is also to be disposed of all hard disks must be shredded by an approved contractor. Paper copies of records that are to be disposed of should be shredded in line with agreed Assert Handling Procedures.