

Inspired eLearning, LLC

**PROCEDURE FOR DOCUMENT AND RECORD CONTROL**

|  |  |
| --- | --- |
| Code: |  |
| Version: | 0.1 |
| Date of version: | 10/25/2018 |
| Created by: | Jennifer Mick |
| Approved by: |  |
| Confidentiality level: | Confidential |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 10/25/18 | 0.1 | Jennifer Mick | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415646389)

[2. Reference documents 3](#_Toc415646390)

[3. Control of internal documents 3](#_Toc415646391)

[3.1. Document formatting 3](#_Toc415646392)

[3.2. Document approval 3](#_Toc415646393)

[3.3. Publishing and distributing documents; withdrawal from use 4](#_Toc415646394)

[3.3.1. Documents with the lowest confidentiality level 4](#_Toc415646395)

[3.3.2. Documents with higher confidentiality level 4](#_Toc415646396)

[3.4. Document updates 4](#_Toc415646397)

[3.5. Records control 4](#_Toc415646398)

[4. Documents of external origin 5](#_Toc415646399)

[5. Managing records kept on the basis of this document 5](#_Toc415646400)

[6. Validity and document management 5](#_Toc415646401)

# Purpose, scope and users

The purpose of this procedure is to ensure control over creation, approval, distribution, usage and updates of documents and records (also called: documented information) used in the Information Security Management System (ISMS).

This procedure is applied to all documents and records related to the ISMS [BCMS], regardless of whether the documents and records were created inside [organization name] or whether they are of external origin. This procedure encompasses all documents and records, stored in any possible form ‑ paper, audio, video, etc.

Users of this document are all employees of [organization name] inside the scope of the ISMS [BCMS].

# Reference documents

* ISO/IEC 27001 standard, clause 7.5
* Information Security Policy
* Policy for handling classified information
* Retention Policy for ISMS

# Control of internal documents

Internal documents are all documents created inside the organization.

## Document formatting

The document text is written using font Calibri, size 11. Chapter titles are written using font size 14 bold, while level 2 chapter titles are written in font size 12 bold. Level 3 chapter titles are written in font size 11 bold italic.

The document header contains organization name and confidentiality level. The footer contains document name, current version and date of document, and number of pages.

Every document must also define its users.

## Document approval

All documents, regardless of whether they are new documents or new versions of existing documents, must be approved by Legal Counsel. [job title].

Documents are approved in the following way: Vice President of Engineering and IT Operations will approve the document via Conformio. .

## Publishing and distributing documents; withdrawal from use

### Documents with the lowest confidentiality level

In case of documents to which access is allowed for all employees within ISMS scope, Information Security Governance, Risk, and Compliance Specialist (hereinafter referred to as IS-GRC Specialist) must publish them on the intranet, in the folder Active Policies & Procedures with reading rights only. When a new document or new document version is published, Director of IT Operations must inform all employees listed as users of the document by e-mail.

If there is an older version of the document, IS-GRC Specialist must delete it from the Active Policies & Procedures documents folder and move it to Retired Policies & Procedures. If there are older versions of printed documents, [job title] must collect all such documents and destroy all copies except the signed original, which must be duly stored ‑ such originals must be marked as "Obsolete" using a marker pen.

### Documents with higher confidentiality level

Documents which have a higher confidentiality level, as specified in the Information Security Policy, and of which distribution is limited, are published by the document owner on the intranet with reading rights only, in a folder to which access is granted only to persons specified on the document's distribution list. The document owner must send an e-mail notification about such a document to all persons on the distribution list.

If there is an older version of the document, the document owner must delete it from the Active Policies & Procedures documents and move it to the folder containing obsolete documents (Retired Policies & Procedures), which can be accessed only by persons specified on the document distribution list.

## Document updates

The person listed as document owner has the responsibility for updating the document. Updates are performed in line with the frequency defined for each document, but at least once a year.

All changes to the document must be made using "Track changes," making visible only the revisions to the previous version and must be briefly described in the "Change History" table; if Track changes option is unavailable, or if the changes are too numerous, then the Track changes option is not used.

Each document should preferably have a "Change History" table used to record every change made to the document.

## Records control

Each internal document in the ISMS must define how records resulting from the use of such a document should be managed, i.e. it must specify the following: (1) record title, (2) storage location, (3) person responsible for storage, (4) controls for record protection, and (5) retention time.

Employees of the organization may access stored records only after obtaining permission from the person designated as the person responsible for storing individual records. If the sensitivity of certain records is such that permission for access must be obtained from a different person, this must be stated in the concerned internal document in the chapter describing records control.

Access and retrieval rights for records are determined by the owner of individual records. IS-GRC Specialist is responsible for destroying all records of which the retention time has expired.

# Documents of external origin

Each external document which is necessary for the planning and operation of the ISMS must be recorded in the incoming mail register. The incoming mail register must contain the following information: (1) document number, (2) sender, (3) document name, (4) date of receipt, (5) name of the person to whom the document has been forwarded.

The person who receives mail and courier parcels must forward them to [job title], who must make a record in the incoming mail register; the person who receives electronic mail must forward such a document to [job title], who must also record it in the incoming mail register. [job title] then classifies documents according to the Policy for handling classified information and determines to whom the document should be forwarded.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Record name*** | ***Storage location*** | ***Person responsible for storage*** | ***Controls for record protection*** | ***Retention time*** |
| Incoming mail register (electronic form ‑ Excel spreadsheet) | ISOC Sharepoint site or other document management site | IS-GRC Specialist | Only IS-GRC Specialist has the right to make entries into and changes to the incoming mail register. | Records are stored for a period of 3 years |

Only Director of IT Operations can grant other employees’ access to the incoming mail register.

# Validity and document management

This document is valid as of [date].

The owner of this document is IS-GRC Specialist, who must check and, if necessary, update the document at least once a year, unless other circumstances require a review and subsequent change.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* number of obsolete or out-of-date documents
* number of documents that were not distributed to intended employees
* number of documents for which no record is kept, or which are not appropriately stored

IS-GRC Specialist

Jennifer Mick

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