Seventh loop Tech

PROCEDURE FOR DOCUMENT AND RECORD CONTROL

Code:	001
Version:	0.1
Date of version:	16/8/2025
Created by:	Hammad Zahid Ali
Approved by:	Taimoor Ijlal
Confidentiality level:	Internal

Change history

Date	Version	Created by	Description of change
2025-08-16	0.1	Hammad	Job Title changes for CISO

Table of contents

1. 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, regardless of whether the documents and records were created inside Seventh loop Tech 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 Sevent loop Tech inside the scope of the ISMS.

2. Reference documents

- ISO/IEC 27001 standard, clause 7.5
- ISO 22301 standard, clause 7.5
- BS 25999-2 standard, clauses 3.4.2 and 3.4.3
- ISO/IEC 27018 standard, clause A.9.2
- Information Security Policy
- Business Continuity Policy
- Policy for handling classified information

3. Control of internal documents

Internal documents are all documents created inside the organization.

3.1. 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.

3.2. Document approval

All documents, regardless of whether they are new documents or new versions of existing documents, must be approved by CISO.

Documents are approved in the following way: CISO will approve the document via e-mail.

3.3. Publishing and distributing documents; withdrawal from use

3.3.1. Documents with the lowest confidentiality level

In case of documents to which access is allowed for all employees within ISMS scope, CISO must publish them on the intranet, in the folder Z:\Sharedrive\OfficialDocuments\ with reading rights only. When a new document or new document version is published, CISO must inform all employees listed as users of the document by e-mail. If a printed version of the document must be delivered to some employees, this is the responsibility of CISO.

If there is an older version of the document, CISO must delete it from the valid documents folder and move it to Z:\Sharedrive\ObsoleteDocuments\. If there are older versions of printed documents, CISO 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.

3.3.2. Documents with higher confidentiality level

Documents which have a higher confidentiality level, as specified in the Policy for handling classified information

, 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 valid documents folder and move it to the folder containing obsolete documents, which can be accessed only by persons specified on the document distribution list.

3.3.3. Documents regarding cloud service customer's Personally Identifiable Information (PII)

Previous versions of policies and procedures regarding the handling of cloud service customer's Personally Identifiable Information (PII) must be stored for a period of five years, unless specified otherwise by legal or contractual requirement. This information must be written in each such document in the section about validity and document management.

3.4. 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.

3.5. 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. [job title] is responsible for destroying all records of which the retention time has expired.

4. 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 CISO who must make a record in the incoming mail register; the person who receives electronic mail must forward such a document to CISO, who must also record it in the incoming mail register. CISO then classifies documents according to the Policy for handling classified information and determines to whom the document should be forwarded.

5. 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)	Z:\Sharedrive\CISO	CISO acting as owner of the incoming mail register	Only CISO has the right to make entries into and changes to the incoming mail register.	Records are stored for a period of 3 years

Only CISO can grant other employees access to the incoming mail register.

6. Validity and document management

This document is valid as of 28/12/2027.

The owner of this document is CISO, who must check and, if necessary, update the document at least once a year.

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

CISO
Taimoor Ijlal

_____
[signature]