[Organization logo]

[Organization name]

Commented [270012]: All fields in this document marked by square brackets [ ] must be filled in.

PROCEDURE FOR DOCUMENT AND RECORD CONTROL

Commented [270013]: To learn how to manage documents, read these articles:

- How to manage documents according to ISO 27001 and ISO 22301 https://advisera.com/27001academy/blog/2021/06/27/how-to-manage-documents-according-to-iso-27001-and-iso-22301/
- Records management in ISO 27001 and ISO 22301 https://advisera.com/27001academy/blog/2014/11/24/records-management-in-iso-27001-and-iso-22301/
- How detailed should the ISO 27001 documents be? https://advisera.com/27001academy/blog/2014/09/22/detailed-iso-27001-documents/

Furthermore, take a look at this book: Managing ISO Documentation: A Plain English Guide https://advisera.com/books/managing-iso-documentation-plain-english-guide/

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Commented [270014]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

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) [Business Continuity Management System – BCMS].

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].

Commented [270015]: This is to be inserted instead of the ISMS in case the procedure refers exclusively to business continuity management.

Commented [270016]: Include the name of your company.

Commented [270017]: Include the name of your company.

2. Reference documents

- ISO/IEC 27001 standard, clause 7.5, and A.5.33
- ISO 22301 standard, clause 7.5
- Information Security Policy
- Business Continuity Policy
- Information Classification Policy
- [other documents and regulations specifying document control]

Commented [270018]: Delete this item if the procedure refers only to business continuity management.

Commented [270019]: Delete this if you are not implementing business continuity.

Commented [2700110]: Delete this item if the procedure refers only to business continuity management.

Commented [2700111]: Delete this if you are not implementing business continuity.

Commented [2700112]: Delete this item if no such document exists.

Commented [2700113]: E.g., contracts with customers.

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.

[illegible]

[illegible]

Commented [2700114]: Adapt to the organization's standard practice.

Commented [2700115]: Delete if under ISO 27001 the Statement of Applicability excludes control A.5.12

3.2. Document approval

[illegible]

Documents are approved in the following way: [job title] will approve the document via e-mail.

Commented [2700116]: E.g., Information Security Manager, Business Continuity Manager, CEO, etc.

[illegible]

Commented [2700117]: E.g., Information Security Manager, Business Continuity Manager, CEO, etc.

Commented [2700118]: Alternatively, you can define that the

[illegible]

3.3. Publishing and distributing documents; withdrawal from use

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 [job title].

If there is an older version of the document, [job title] must delete it from the valid documents folder such originals must be marked as "Obsolete" using a marker pen.

3.3.2. Documents with higher confidentiality level

Documents that have a higher confidentiality level, as specified in the Information Classification 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

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 document.

(3) person responsible for storage, (4) controls for record protection, and (5) retention time.

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.

Commented [2700119]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700120]: Change if documents are published through a document management system.

Commented [2700121]:

Commented [2700122]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700123]: Or in some other way if a document management system is used.

Commented [2700124]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700125]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700126]:

Commented [2700127]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700128]:

Commented [2700129]: For more information about information classification, see:

Information classification according to ISO 27001
https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/

Commented [2700130]:

Commented [2700131]: Change if documents are published through a document management system, or in case of paper documents.

Commented [2700132]: To learn more read this article:

Records management in ISO 27001 and ISO 22301
http://advisera.com/27001academy/blog/2014/11/24/records-management-in-iso-27001-and-iso-22301/

responsible for destroying all records of which the retention time has expired.

4. Documents of external origin

receipt, (5) name of the person to whom the document has been forwarded.

correspondence. [Job title] then classifies documents according to the Information Classification Policy 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*
Register of external correspondence (electronic form – Excel spreadsheet)	[intranet folder name]	[job title acting as owner of the Register of external correspondence]	Only [job title] has the right to make entries into and changes to the Register of external correspondence .	Records are stored for a period of 3 years

Only [job title] can grant other employees access to the Register of external correspondence.

6. Validity and document management

This document is valid as of [date].

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

-
-
-

Commented [2700133]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700134]: More details should be provided if records are stored on various media.

Commented [27A35]:

Commented [2700136]: Add additional information if required by the organization's record maintenance system.

Commented [2700137]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [27A38]:

Commented [2700139]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [27A40]:

Commented [2700141]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700142]: Delete if no such policy is in place.

Commented [2700146]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [27A43]: Adapt the document name to the organization's existing record maintenance system.

If you are using a CRM for recording all correspondence, you can write here "Customer relationship management software."

Commented [2700144]: Adapt to the organization's standard practice.

Commented [27A45]: Adapt the document name to the organization's existing record maintenance system. ... [1]

Commented [27A47]: Adapt the document name to the organization's existing record maintenance system. ... [2]

Commented [2700148]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [27A49]: Adapt the document name to the organization's existing record maintenance system. ... [3]

Commented [2700150]: E.g., Business Continuity Manager, Information Security Manager, Security Manager, document owner, etc.

Commented [2700151]: This is only a recommendation; adjust frequency as appropriate.

[job title]
[first and last name]

_____

[signature]

Commented [2700152]: Only necessary if clause 3.2. prescribes that paper documents must be signed.