This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Procedure for Development of Cybersecurity Documents Template

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated by	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This procedure aims to define the detailed step-by-step cybersecurity requirements related to the process of developing cybersecurity documents at <organization name>. These requirements are aligned with best practices to ensure the quality and consistency of structure and content between cybersecurity documents.

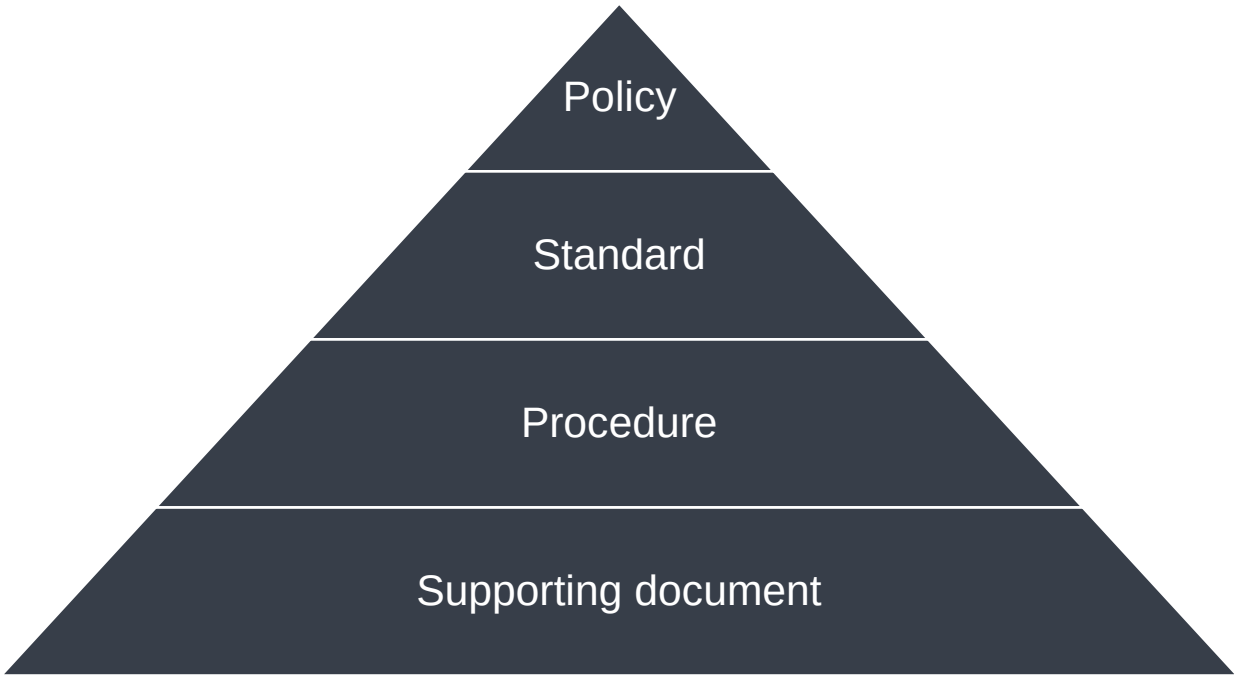
The requirements in this procedure are also aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

The procedure covers <organization name>'s development process for cybersecurity documents as it relate to creation and managing of documents throughout its lifecycle and applies to all personnel (employees and contractors) in <organization name>.

Types of Cybersecurity Documents

Cybersecurity document structure and types of documents are depicted below.



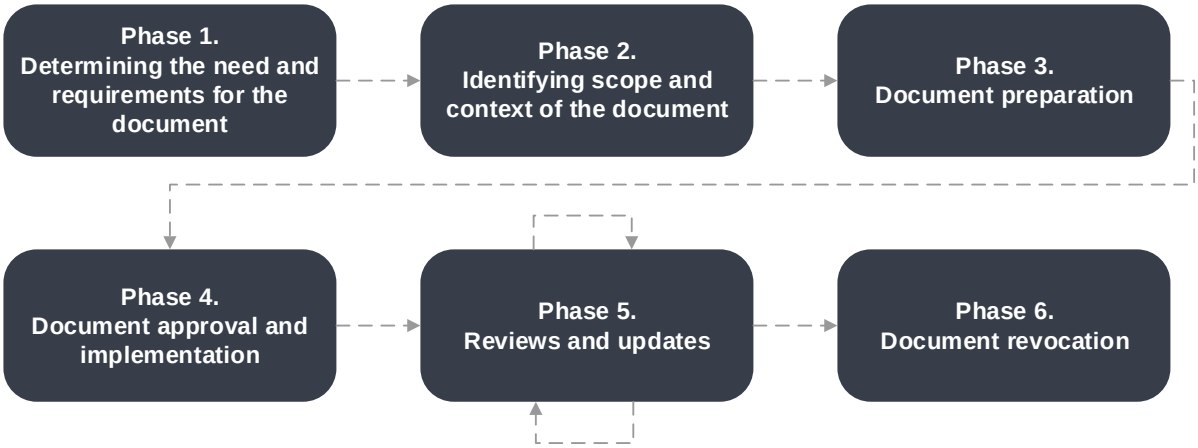
The cybersecurity document structure defines four classes of documents, ranked by their importance, and intended access and use scopes.

No	Document type	Description
1	Policy	Document formulated with consideration to regulatory requirements, supporting business strategy, presenting an overview of the matter, general directions, and goals.
2	Standard	Document in the form of predefined frameworks, models or formal recognized best practices adopted by <organization name> to ensure controls stated in policies.
3	Procedure	Detailed optional document specifying directions stated in policies, defining individual activities and responsibilities.
4	Supporting document	Optional document specifying individual activities stated in procedures, providing additional advice, e.g., register, guideline, report, guide, checklist, playbook.

Overview of the Cybersecurity Document Development process

Document development process should include the following steps:

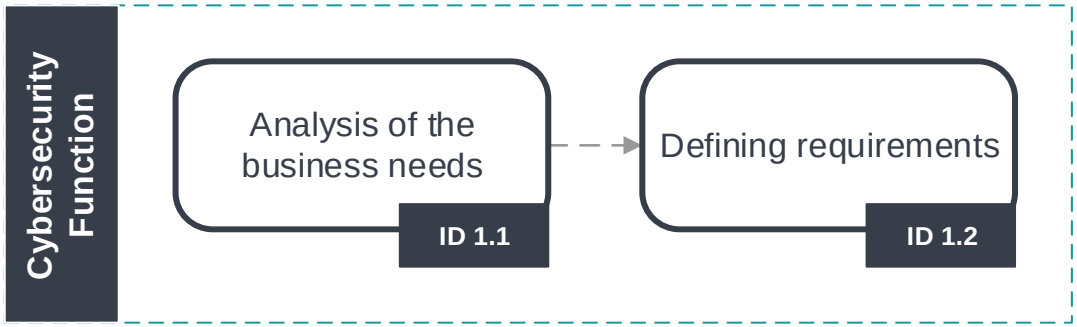
1. Determining the need and requirements for the document
2. Identifying scope and context of the document
3. Document preparation:
    a. General rules
    b. Structure of the document
    c. Content of the document
4. Document approval and implementation
5. Reviews and updates
6. Document revocation



<organization name>'s personnel are responsible for complying with this procedure whenever creating or/and managing any cybersecurity document within <organization name>.

Details of the Cybersecurity Document Development process

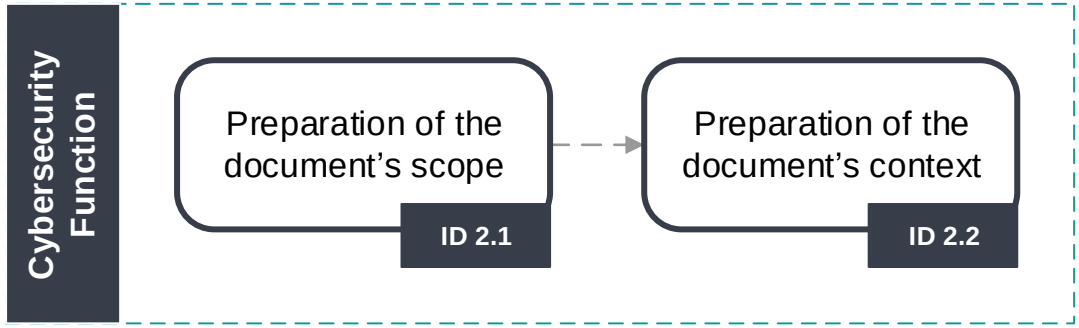
Phase 1. Determining the need and requirements for the document



ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
1.1	Analysis of the business needs	Once there is a business need for creating new cybersecurity document, it should be analyzed to determine the relevance and importance of the document for the <organization name> ‘s operations. Business need may result e.g., from performed gap analysis within existing cybersecurity documentation, implementing a new	Cybersecurity Department	Business need	Relevance and importance of the potential document	Cybersecurity Department

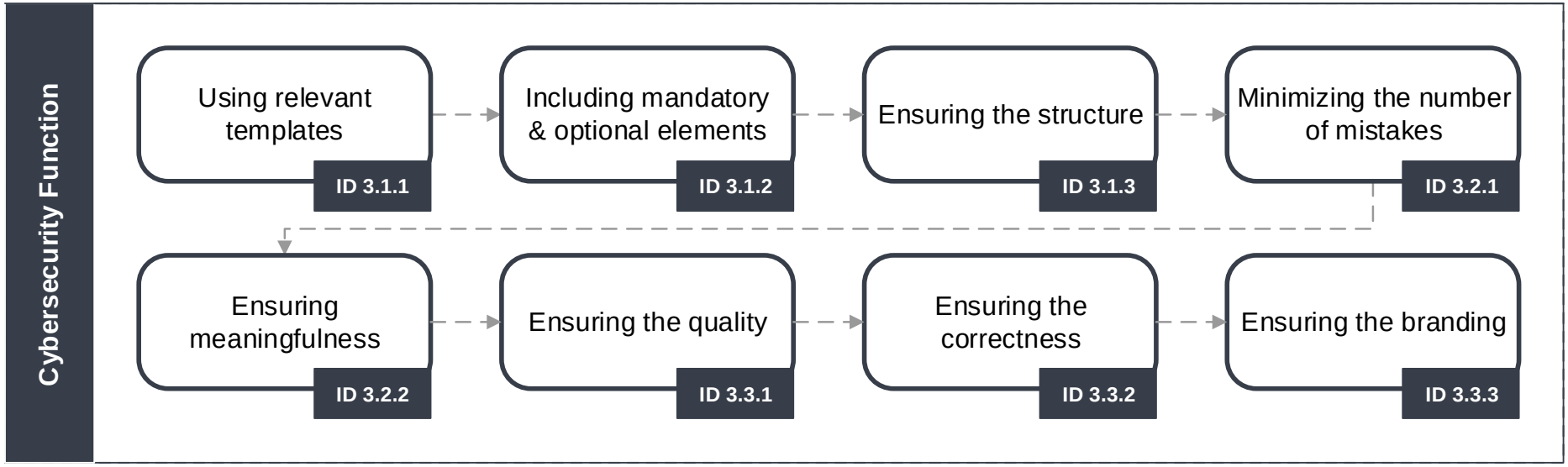
		process within the organization or increasing the cybersecurity maturity level in the organization				
1.2	Defining requirements	Clear requirements for the document content and type should be defined	Cybersecurity Department	Business need	Set of requirements	Cybersecurity Department

Phase 2. Identifying scope and context of the document



ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
	Preparation of the document's scope	Scope of document should be created, taking into consideration document type and its intended use	Cybersecurity Department	Set of requirements	Scope of the document	Cybersecurity Department
	Preparation of the document's context	Context for the document, including superior documents, its placement in the document's structure within the organization, reasons for document existence, personnel responsible for development and maintenance of the document, should be prepared	Cybersecurity Department	Set of requirements	Context for the document	Cybersecurity Department

Phase 3. Document preparation

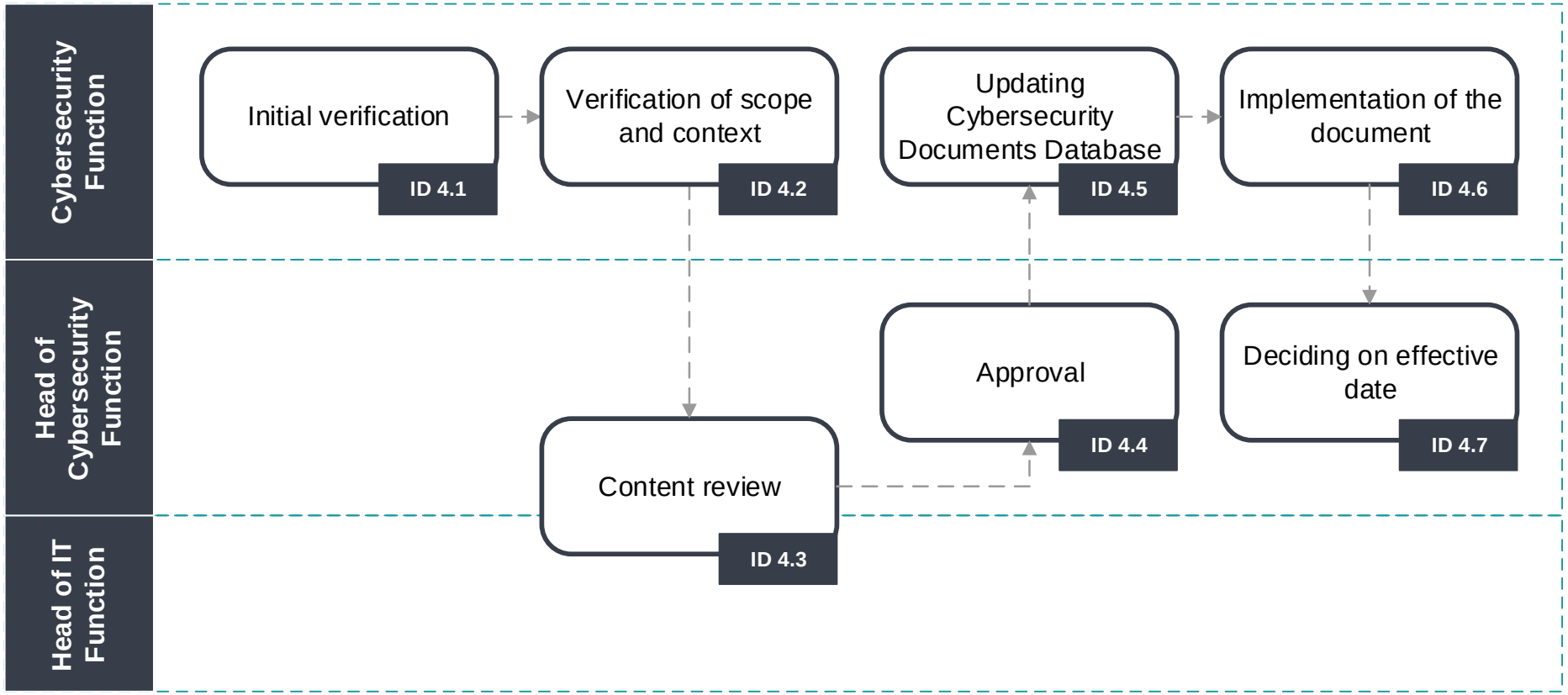


ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
Structure of the document						
3.1.1	Using relevant templates	Templates of the document types should be used	Cybersecurity Department	Business need, Set of requirements	Document based on relevant template	Cybersecurity Department

ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
3.1.2	Including mandatory & optional elements	Every document should include the following elements: A. Title page B. Document Classification C. Label D. Document Approval E. Amendment History F. Table of contents G. Purpose H. Scope I. Definitions and Abbreviations (if applicable) J. Main Content K. Roles and responsibilities L. Compliance Additionally, documents may include the following elements, if applicable: A. Appendices	Cybersecurity Department	n/a	Mandatory elements included	Cybersecurity Department
3.1.3	Ensuring the structure	Structure of every document should be adjusted to the type of the document	Cybersecurity Department	Set of requirements	Ensured structure	Cybersecurity Department

ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
Content of the document						
3.2.1	Minimizing the number of mistakes	Content of the document should be based on facts, experience of staff and cybersecurity best practices	Cybersecurity Department	New document	Mistakes minimized	Cybersecurity Department
3.2.2	Ensuring meaningfulness	Content of the document should be practical and relevant to the purpose and scope of the document	Cybersecurity Department	New document	Ensured meaningfulness	Cybersecurity Department
General rules						
3.3.1	Ensuring the quality	Cybersecurity document should be written in a concise and understandable way	Cybersecurity Department	New document	Ensured quality	Cybersecurity Department
3.3.2	Ensuring the correctness	Cybersecurity document should be checked for grammatical and punctuation accuracy as well as spelling.	Cybersecurity Department	New document	Ensured correctness	Cybersecurity Department
3.3.3	Ensuring the branding	Every document should have the <organization name>'s branding	Cybersecurity Department	New document	Ensured branding	Cybersecurity Department

Phase 4. Document approval and implementation



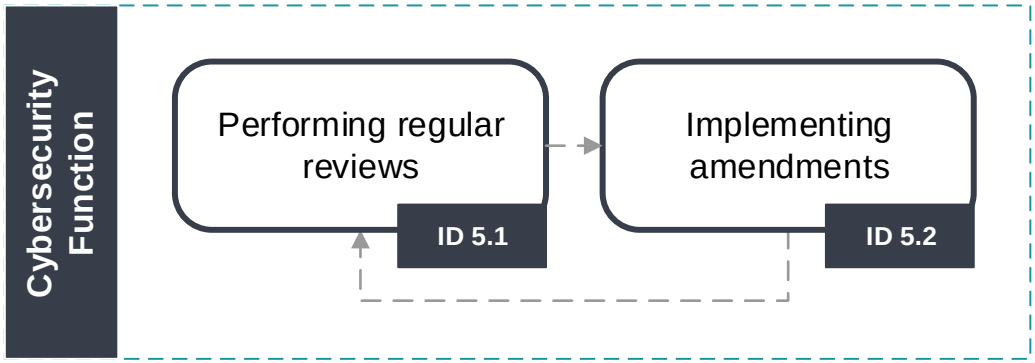
ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
4.1	Initial	Verification of the compliance of	Cybersecurity	New	Compliance	Cybersecurity

ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
	verification	cybersecurity document with this cybersecurity document Development procedure should be performed	Department	document	or lack of compliance	Department
4.2	Verification of scope and context	Verification of the cybersecurity document in terms of its alignment with defined scope and context	Cybersecurity Department	New document	Scope and context verified	Cybersecurity Department
4.3	Content review	Cybersecurity document should be reviewed to ensure its content is accurate, meaningful, and aligned with other documents in force within <organization name>	Head of the Cybersecurity Department	New document	Content is reviewed and accepted	Head of the Cybersecurity Department Head of IT Department (if applicable) Representative of the Human Resources Department Representative of the Legal Department

ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
4.4	Approval	Cybersecurity document should be approved if the initial verification and review is passed	Head of the Cybersecurity Department	New document	Approved document	Head of the Cybersecurity Department
4.5	Updating cybersecurity documents Database	Once the cybersecurity document is approved, the cybersecurity documents Database should be updated, and the document should be made available for all the relevant personnel of <organization name>	Cybersecurity Department	Approved document	Updated cybersecurity documents Database	Cybersecurity Department
4.6	Implementation of the document	Implementation of cybersecurity document by adjusting relevant existing processes, tasks and activities or creating new ones to meet requirements and guidelines stated in the document	Cybersecurity Department	Approved document, relevant existing processes, tasks, and activities	Document implemented	Cybersecurity Department
4.7	Deciding on effective date	Date of announcing the cybersecurity document is the effective date of implementation unless it is decided otherwise. The documents must be communicated to the concerned	Head of the Cybersecurity Department	Approved document	Effective date of implementation	Head of the Cybersecurity Department

ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
		parties who are supposed to comply with it.				

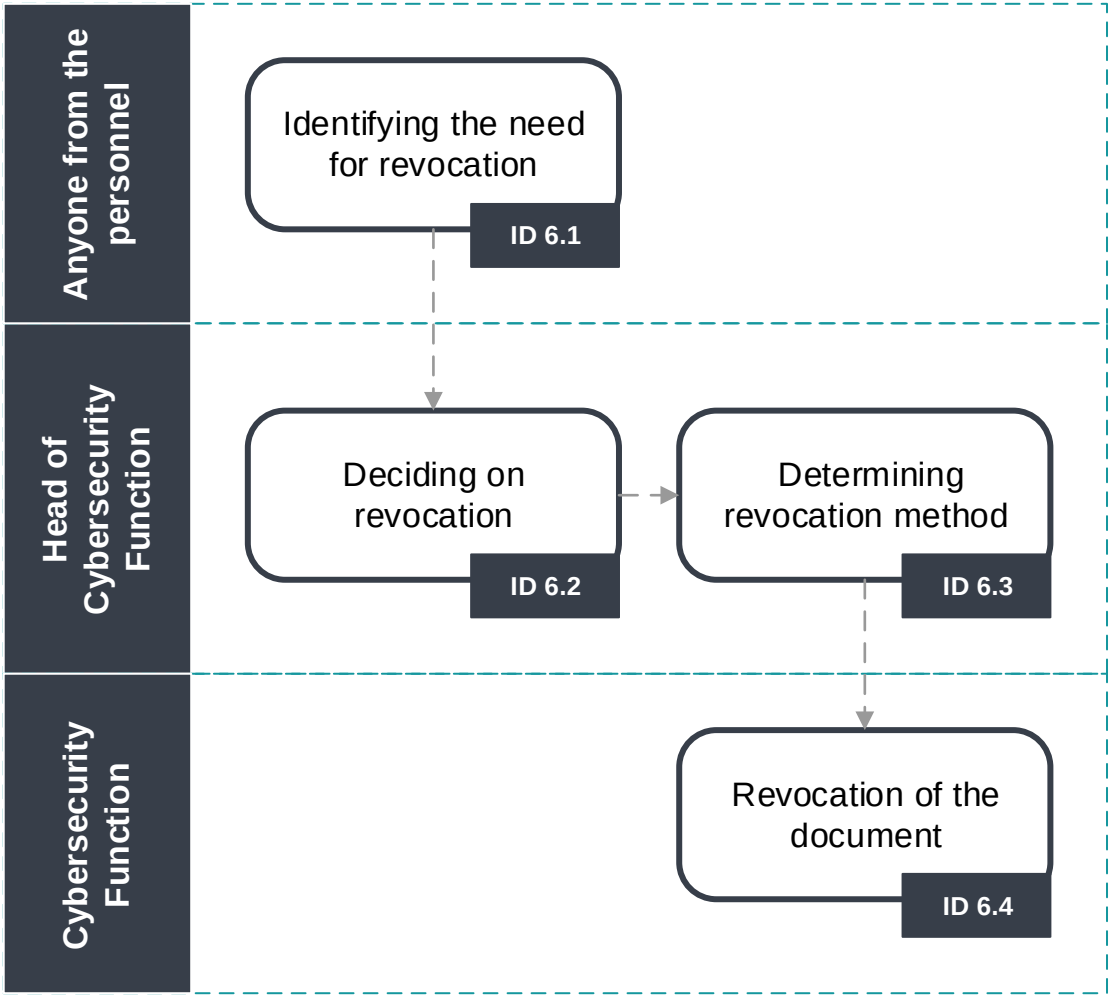
Phase 5. Reviews and updates



ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
5.1	Performing regular reviews	Cybersecurity documents should be reviewed at least on annual basis	Cybersecurity Department	Document	Need or lack of need for amendments	Cybersecurity Department

5.2	Implementing amendments	Any discrepancies, mistakes or gaps found in any cybersecurity document should be corrected and the document should be updated as soon as possible	Cybersecurity Department	Need for amendments	Implemented amendments	Cybersecurity Department

Phase 6. Document revocation



Choose Classification

ID	Step	Description	Owner/ Responsible	Inputs	Outputs	Stakeholders
6.1	Identifying the need for revocation	In case of necessity to revoke a cybersecurity document, the Head of the Cybersecurity Department should be informed in writing, including the reasons for the revocation	Anyone from <organization name>	Need for revocation	Need + justification written down	Anyone from <organization name>
6.2	Deciding on revocation	The reasons for revocation should be reviewed and analyzed to decide on potential revocation of the cybersecurity document	Head of the Cybersecurity Department	Need + justification written down	Decision to revoke the document or not	Head of the Cybersecurity Department
6.3	Determining revocation method	The decision on the method and time of revocation and removal of the cybersecurity document from the cybersecurity documents Database should be taken	Head of the Cybersecurity Department	Decision to revoke the document	Decided method and time or revocation	Head of the Cybersecurity Department
6.4	Revocation of the document	The cybersecurity document should be revoked according to decided method and time	Cybersecurity Department	Decided method and time or revocation	Document revoked; cybersecurity documents Database updated	Cybersecurity Department

Roles and Responsibilities

1- **Procedure Owner:** <head of the cybersecurity function>
2- **Procedure Review and Update:** <cybersecurity function>
3- **Procedure Implementation and Execution:** <cybersecurity function>
4- **Procedure Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the procedure at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this procedure on a regular basis.
2- All personnel at <organization name> must comply with this procedure.
3- Any violation of this procedure may be subject to disciplinary action according to <organization name>'s procedures.