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

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

Version Control

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

Review Table

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

Table of Contents

[Purpose 4](#_Toc143605205)

[Scope 4](#_Toc143605206)

[Types of Cybersecurity Documents 5](#_Toc143605207)

[Overview of the Cybersecurity Document Development process 6](#_Toc143605208)

[Details of the Cybersecurity Document Development process 7](#_Toc143605209)

[Phase 1. Determining the need and requirements for the document 7](#_Toc143605210)

[Phase 2. Identifying scope and context of the document 8](#_Toc143605211)

[Phase 3. Document preparation 10](#_Toc143605212)

[Phase 4. Document approval and implementation 13](#_Toc143605213)

[Phase 5. Reviews and updates 16](#_Toc143605214)

[Phase 6. Document revocation 18](#_Toc143605215)

[Roles and Responsibilities 20](#_Toc143605216)

[Update and Review 20](#_Toc143605217)

[Compliance 20](#_Toc143605218)

# [Purpose](#_heading=h.1fob9te)

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](#_heading=h.3znysh7)

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](#_heading=h.nuptowmiwgz3)

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:
   1. General rules
   2. Structure of the document
   3. 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 |
|  | 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 process within the organization or increasing the cybersecurity maturity level in the organization | Cybersecurity Department | Business need | Relevance and importance of the potential document | Cybersecurity Department |
|  | 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 | | | | | | |
|  | 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 |
|  | Including mandatory & optional elements | Every document should include the following elements:   1. Title page 2. Document Classification 3. Label 4. Document Approval 5. Amendment History 6. Table of contents 7. Purpose 8. Scope 9. Definitions and Abbreviations (if applicable) 10. Main Content 11. Roles and responsibilities 12. Compliance   Additionally, documents may include the following elements, if applicable:   1. Appendices | Cybersecurity Department | n/a | Mandatory elements included | Cybersecurity Department |
|  | 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 |
| Content of the document | | | | | | |
|  | 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 |
|  | 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 | | | | | | |
|  | Ensuring the quality | Cybersecurity document should be written in a concise and understandable way | Cybersecurity Department | New document | Ensured quality | Cybersecurity Department |
|  | 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 |
|  | 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 |
| --- | --- | --- | --- | --- | --- | --- |
|  | Initial verification | Verification of the compliance of cybersecurity document with this cybersecurity document Development procedure should be performed | Cybersecurity Department | New document | Compliance or lack of compliance | Cybersecurity Department |
|  | 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 |
|  | 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 |
|  | 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 |
|  | 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 |
|  | 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 |
|  | 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 parties who are supposed to comply with it. | Head of the Cybersecurity Department | Approved document | Effective date of implementation | Head of the Cybersecurity Department |

Phase 5. Reviews and updates



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Step | Description | Owner/ Responsible | Inputs | Outputs | Stakeholders |
|  | 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 |
|  | 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



| 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](#_heading=h.tyjcwt)

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](#_الالتزام_بالسياسة) 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](#_heading=h.3dy6vkm)

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.