[Organization logo]

[Organization name]

Commented [270011]: All fields in this document marked by square brackets [ ] must be filled in.

INFORMATION CLASSIFICATION POLICY

Commented [270012]: To learn how to classify information, read this article:

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

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

Commented [270013]: 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 3

2. REFERENCE DOCUMENTS 3

3. CLASSIFIED INFORMATION 3

- 3.1. STEPS AND RESPONSIBILITIES 3
- 3.2. CLASSIFICATION OF INFORMATION 4
  - *3.2.1. Classification criteria 4*
  - *3.2.2. Confidentiality levels 4*
  - *3.2.3. List of Authorized Persons 4*
  - *3.2.4. Reclassification 5*
- 3.3. INFORMATION LABELING 5
- 3.4. HANDLING CLASSIFIED INFORMATION 5
- 3.5. DATA MASKING 8

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 8

5. VALIDITY AND DOCUMENT MANAGEMENT 9

1. Purpose, scope and users

The purpose of this document is to ensure that information is protected at an appropriate level.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all types of information, regardless of the form – paper or electronic documents, applications and databases, people's knowledge, etc.

Users of this document are all employees of [organization name].

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.9, A.5.10, A.5.12, A.5.13, A.5.14, A.7.10, A.8.3, A.8.5, A.8.11, and A.8.12
- Information Security Policy
- Risk Assessment and Risk Treatment Report
- Statement of Applicability
- Inventory of Assets
- List of Legal, Regulatory, Contractual and Other Obligations
- Incident Management Procedure
- [Security Procedures for IT Department] / [Disposal and Destruction Policy]
- IT Security Policy

Commented [27A4]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "05_General_Policies".

Commented [27A5]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "06_Risk_Assessment_and_Risk_Treatment".

Commented [27A6]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "07_Applicability_of_Controls".

Commented [270017]: If you don't have this List, then in these bullets list all the legislation and contractual obligations related to classification of information.

Commented [270018]: Select the document which prescribes secure erasure of data.

Commented [270019]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "09_Annex_A_Security_Controls".

3. Classified information

3.1. Steps and responsibilities

Steps and responsibilities for information management are the following:

Step name	***Responsibility***
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted] owner of such an information asset.

3.2. Classification of information

3.2.1. Classification criteria

The level of confidentiality is determined based on the following criteria:

- value of information – based on impacts assessed during risk assessment
- sensitivity and criticality of information – based on the highest risk calculated for each [redacted]
- [redacted]

Commented [2700110]: This also includes privacy regulations.

3.2.2. Confidentiality levels

All information must be classified into confidentiality levels.

Confidentiality level	***Labeling***	***Classification criteria***	***Access restriction***
Public	(unlabeled)	Making the information public cannot harm the organization in any way	Information is available to the public
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Commented [2700111]: Confidentiality levels and labeling [redacted]

The basic rule is to use the [redacted]

3.2.3. List of Authorized Persons

[redacted] the right to access that information.

The same rule applies to the [illegible]

3.2.4. Reclassification

Asset owners must review the confidentiality level of their information assets every [two years] and [illegible]

3.3. Information labeling

Confidentiality levels are labeled in the following way:

- [illegible]
- [illegible] document page
- **information systems** – the confidentiality level in applications and databases must be [illegible]
- [illegible]
- [illegible] indicated on the top surface of such a medium
- [illegible]

3.4. Handling classified information

All persons accessing classified information must [illegible]

Information assets may be taken off-premises only after obtaining authorization in accordance with the IT Security Policy.

[illegible]

	Internal use	[illegible]	[illegible]
Paper documents	[illegible]	[illegible]	[illegible]

Commented [2700112]: This is only a recommendation; adjust frequency as appropriate.

Commented [2700113]: All rules stated here should be adapted to the organization's needs.

Commented [2700114]: Delete this paragraph if control A.7.10 is excluded from the Statement of Applicability.

Commented [2700115]: [illegible]

	kept in rooms without public access • [redacted]	and outside the organization only in a closed envelope • if sent outside the organization, the document must be mailed with a return receipt service • documents must immediately be [redacted] • [redacted] • [redacted] owner may destroy the document	organization only by a trustworthy person in a closed and sealed envelope • [redacted] • [redacted] • [redacted] • [redacted] owner may destroy the document
Electronic documents	• access to the information system where the document is stored must [redacted] • [redacted]	• access to the information system [redacted] • [redacted] etc., they must be password protected • [redacted]	• the document must be stored in [redacted] • [redacted] • [redacted] • [redacted] services such as FTP, instant messaging, [redacted] • [redacted]

[illegible]	[illegible]	[illegible]	[illegible]
Electronic mail	• the sender must carefully check the recipient • [illegible]	• [illegible] • the sender must carefully check the recipient • [illegible]	• all e-mails must be encrypted • [illegible] • [illegible]
[illegible]	[illegible]	[illegible]	[illegible]

			destroy the medium
Information transmitted orally	- unauthorized persons [redacted] communicated	- the room must be [redacted] - [redacted]	- the room must be [redacted] - [redacted] - [redacted] - [redacted] kept

*Controls are implemented cumulatively, meaning that controls for any confidentiality level imply [redacted]

3.5. Data masking

Commented [2700116]: Delete this section if control A.8.11 was found inapplicable in the Statement of Applicability.

If the asset owner decides that data exposure is a concern (e.g., personally identifiable information, [redacted]

- Information on paper media: data not needed by the user must be masked by means of data [redacted]
- [redacted] sensitive data).

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
[List of Authorized Persons with access to documents]	Together with the information where the confidentiality level is indicated	Information asset owner	The same as for the protection of information	The List must exist as long as the information itself exists

Commented [2700117]: Alter this record to match what you already have in your company. If you do not have a similar record, you can create a new one in the format that suits you best.

5. Validity and document management

This document is valid as of [date].

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

Commented [2700118]: This is only a recommendation; adjust frequency as appropriate.

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

- [redacted]
- [redacted]

[job title]
[name]

____
[signature]

Commented [2700119]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.