[organization logo]

[organization name]

**INFORMATION CLASSIFICATION POLICY**

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

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc454538941)

[2. Reference documents 3](#_Toc454538942)

[3. Classified information 3](#_Toc454538943)

[3.1. Steps and responsibilities 3](#_Toc454538944)

[3.2. Classification of information 4](#_Toc454538945)

[3.2.1. Classification criteria 4](#_Toc454538946)

[3.2.2. Confidentiality levels 4](#_Toc454538947)

[3.2.3. List of Authorized Persons 4](#_Toc454538948)

[3.2.4. Reclassification 5](#_Toc454538949)

[3.3. Information labeling 5](#_Toc454538950)

[3.4. Handling classified information 5](#_Toc454538951)

[4. Managing records kept on the basis of this document 8](#_Toc454538952)

[5. Validity and document management 8](#_Toc454538953)

# 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].

# Reference documents

* ISO/IEC 27001 standard, clauses A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
* ISO/IEC 27017 standard, clause 15.1.2Information Security Policy
* Risk Assessment and Risk Treatment Report
* Statement of Applicability
* Inventory of Assets
* List of Legal, Regulatory and Contractual and Other Obligations
* Incident Management Procedure
* [Operating Procedures for Information and Communication Technology] / [Disposal and Destruction Policy]
* Acceptable Use Policy

# Classified information

## Steps and responsibilities

Steps and responsibilities for information management are the following:

|  |  |
| --- | --- |
| ***Step name*** | ***Responsibility*** |
| 1. Entering the information asset in the Inventory of Assets | [job title] |
| 2. Classification of information | Asset owner |
| 3. Information labeling | Asset owner |
| 4. Information handling | Persons with access rights in accordance with this Policy |

If classified information is received from outside the organization, [job title] is responsible for its classification in accordance with the rules prescribed in this Policy, and this person becomes the owner of such an information asset.

If classified information from outside the organization is received and handled as part of the business operation activities (e.g.: customer’s data on provided cloud services), the information classification, as well as the definition of the owner of such information, must be made in accordance with the specifications on the respective service agreement and other legal requirements.

## Classification of information

### 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 information item during risk assessment
* legal and contractual obligations – based on the [List of Legal, Regulatory and Contractual and Other Obligations]

### 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 |
| Internal use | INTERNAL USE | Unauthorized access to information may cause minor damage and/or inconvenience to the organization | Information is available to all employees and selected third parties |
| Restricted | RESTRICTED | Unauthorized access to information may considerably damage the business and/or the organization's reputation | Information is available only to a specific group of employees and authorized third parties |
| Confidential | CONFIDENTIAL | Unauthorized access to information may cause catastrophic (irreparable) damage to business and/or to the organization's reputation | [organization name]’s information is available only to specific individuals in the organization |

The basic rule is to use the lowest confidentiality level ensuring an appropriate level of protection, in order to avoid unnecessary protection costs.

### List of Authorized Persons

Information classified as "Restricted" and "Confidential" must be accompanied by a List of Authorized Persons in which the information owner specifies the names or job functions of persons who have the right to access that information.

The same rule applies to the confidentiality level "Internal use" if people outside the organization will have access to such a document.

### Reclassification

Asset owners must review the confidentiality level of their information assets every [two years] and assess whether the confidentiality level can be changed. If possible, the confidentiality level should be lowered.

For provided cloud services to customers, asset owners under [organization name]’s responsibility must also review the confidentiality level of their information assets after service agreement changes or after a customer’s formal notification. Where allowed by service agreements clauses, the confidentiality level should be lowered.

## Information labeling

Confidentiality levels are labeled in the following way:

* **paper documents** – the confidentiality level is indicated in the top right corner of each document page; it is also indicated on the front of the cover or envelope carrying such a document as well as on the filing folder in which the document is stored
* **electronic documents** – the confidentiality level is indicated in the top right corner of each document page
* **information systems** – the confidentiality level in applications and databases must be indicated on the system access screen, as well as in the top right corner of each consecutive screen displaying confidential information
* **electronic mail** – the confidentiality level is indicated in the first line of the e-mail body
* **electronic storage media** (disks, memory cards, etc.) – the confidentiality level must be indicated on the top surface of such a medium
* **information transmitted orally** – the confidentiality level of confidential information to be transmitted in face-to-face communication, by telephone or some other means of communication, must be communicated prior to the information itself

## Handling classified information

All persons accessing classified information must follow the rules listed in the following table. [job title] must initiate disciplinary action each time the rules are breached or if the information is communicated to unauthorized persons. Each incident related to handling classified information must be reported in accordance with the Incident Management Procedure.

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

The method for secure erasure and destruction of media is prescribed in the document [Operating Procedures for Information and Communication Technology] / [Disposal and Destruction Policy].

Considering provided cloud services, besides the rules listed in the following table, cloud service customers’ data must be handled according rules specified in the respective cloud service agreement.

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***Internal use*** | ***Restricted\**** | ***Confidential\**** |
| **Paper documents** | * only authorized persons may have access * if sent outside the organization, the document must be sent as registered mail * documents may only be kept in rooms without public access * documents must be frequently removed from printers or fax machines | * the document must be stored in a locked cabinet * documents may be transferred within 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 removed from printers or fax machines * only the document owner may copy the document * only the document owner may destroy the document | * the document must be stored in a safe * the document may be transferred within and outside the organization only by a trustworthy person in a closed and sealed envelope * faxing the document is not allowed * the document may be printed out only if the authorized person is standing next to the printer |
| **Electronic documents** | * only authorized persons may have access * when files are exchanged via services such as FTP, instant messaging, etc., they must be password protected * access to the information system where the document is stored must be protected by a strong password * the screen on which the document is displayed must be automatically locked after [number] minutes of inactivity | * only persons with authorization for this document may access the part of the information system where this document is stored * when files are exchanged via services such as FTP, instant messaging, etc., they must be encrypted * only the document owner may erase the document | * the document must be stored in encrypted form * the document may be stored only on servers which are controlled by the organization * the document must not be exchanged via services such as FTP, instant messaging, etc. |
| **Information systems** | * only authorized persons may have access * access to the information system must be protected by a strong password * the screen must be automatically locked after [number] minutes of inactivity * the information system may only be located in rooms with controlled physical access | * users must log out of the information system if they have temporarily or permanently left the workplace * data must be erased only with an algorithm which ensures secure deletion | * access to the information system must be controlled through an authentication process using smart cards or biometric readers * the information system may only be installed on servers controlled by the organization * the information system may only be located in rooms with controlled physical access and identity control of people accessing the room |
| **Electronic mail** | * only authorized persons may have access * the sender must carefully check the recipient * all rules stated under "Information systems" apply | * e-mail must be encrypted if sent outside the organization | * all e-mails must be encrypted |
| **Electronic storage media** | * only authorized persons may have access * media or files must be password protected * if sent outside the organization, the medium must be sent as registered mail * the medium may only be kept in rooms with controlled physical access | * media and files must be encrypted * media must be stored in a locked cabinet * if sent outside the organization, the medium must be mailed with a return receipt service * only the medium owner may erase or destroy the medium | * media must be stored in a safe * media may be transferred within and outside the organization only by a trustworthy person in a closed and sealed envelope |
| **Information transmitted orally** | * only authorized persons may have access to information * unauthorized persons must not be present in the room when the information is communicated | * the room must be sound proof * the conversation must not be recorded | * conversation conducted through a means of communication must be encrypted * no transcript of the conversation may be kept |

\*Controls are implemented cumulatively, meaning that controls for any confidentiality level imply the implementation of controls defined for lower confidentiality levels – if stricter controls are prescribed for a higher confidentiality level, then only such controls are implemented.

# 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 |

# 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.

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

* number of incidents related to unauthorized access to information
* number of information assets classified with an inappropriate confidentiality level

Previous versions of this policy must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]