[organization logo]

[organization name]

**DISPOSAL AND DESTRUCTION 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](#_Toc454746675)

[2. Reference documents 3](#_Toc454746676)

[3. Disposal and destruction of equipment and media 3](#_Toc454746677)

[3.1. Equipment 3](#_Toc454746678)

[3.2. Mobile storage media 3](#_Toc454746679)

[3.3. Paper media 4](#_Toc454746680)

[3.4. Cloud computing environment 4](#_Toc454746681)

[3.5. Erasure and destruction records; commission for the destruction of information 4](#_Toc454746682)

[4. Managing records kept on the basis of this document 4](#_Toc454746683)

[5. Validity and document management 4](#_Toc454746684)

# Purpose, scope and users

The purpose of this document is to ensure that information stored on equipment and media is safely destroyed or erased.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all the information and communication technology as well as to the documentation within the scope.

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

# Reference documents

* ISO/IEC 27001 standard, clauses A.8.3.2, A.11.2.7
* ISO/IEC 27017 standard, clause 11.2.7
* ISO/IEC 27018 standard, clauses 11.2.7, A.10.7 and A.10.13
* Information Security Policy
* [Information Classification Policy]
* [Inventory of Assets]

# Disposal and destruction of equipment and media

All data and licensed software stored on mobile storage media (e.g. on CD, DVD, USB flash drive, memory card, etc.; but also on paper) and on all equipment containing storage media (e.g. computers, data storage, mobile phones, network equipment, etc.) must be erased or the medium destroyed before it is disposed of or reused.

The person responsible for erasing data / destroying media must inform the owner of the asset in question about erasing /destroying data, and the asset owner must update the Inventory of Assets.

## Equipment

[job title] is responsible for checking and erasing data from equipment, unless the [Information Classification Policy] prescribes differently. Data must be erased [describe the technology used for erasing data from media in the equipment], but if the process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed. In situations where there is no certainty that equipment stores Personally Identifiable Information (PII) or not, the equipment must be handled as if it does store PII.

## Mobile storage media

[job title] is responsible for erasing data from mobile storage media, unless the [Information Classification Policy] prescribes differently. Data must be erased [describe the technology used for erasing data from media], but if the erasure process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed. In situations where there is no certainty that equipment stores Personally Identifiable Information (PII) or not, the mobile storage media must be handled as if it does store PII.

## Paper media

Employees of the organization handling individual documents are responsible for destroying paper documents, unless the [Information Classification Policy] prescribes differently. Paper documents are destroyed in paper shredders.

## Cloud computing environment

Considering cloud computing environments (e.g., virtual applications, databases, etc.), data must be erased [describe the technology used for erasing data in cloud computing environment], but if the erasure process is not secure enough considering the sensitivity of the data, then the procedures for erasing data from equipment in section 3.1 must be followed.

In situations where there is no certainty that a cloud computing environment stores Personally Identifiable Information (PII) or not, the virtual storage media must be handled as if it does store PII.

## Erasure and destruction records; commission for the destruction of information

Records of erasure/destruction must be kept for all data classified as "Restricted" and "Confidential." Records must include the following information: information about the media, date of erasure/destruction, method of erasure/destruction, person who carried out the process.

All information classified as "Confidential" must be erased/destroyed in the presence of a commission consisting of persons authorized to access the information in question.

All information classified as "PII" must be erased/destroyed according the documents [list the procedures agreed between the organization and it cloud service customers].

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [Erasure/destruction records] – in paper form | [name of filing folder/cabinet] | [job title] | The cabinet is locked, the keys are kept by [job functions] | Records are stored for a period of 5 years |

# 

# 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 arising from failure to erase or destroy information in a manner specified in this document
* number of destruction processes for information with higher confidentiality levels for which no record is kept

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]s