[organization logo]

[organization name]

**BACKUP 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](#_Toc454542820)

[2. Reference documents 3](#_Toc454542821)

[3. Backup 3](#_Toc454542822)

[3.1. Backup procedure 3](#_Toc454542823)

[3.2. Testing backup copies 3](#_Toc454542824)

[3.3. Backup information to cloud service customers 3](#_Toc454542825)

[4. Managing records kept on the basis of this document 4](#_Toc454542826)

[5. Validity and document management 4](#_Toc454542827)

# Purpose, scope and users

The purpose of this document is to ensure that backup copies are created at defined intervals and regularly tested.

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

Users of this document are employees of [organizational units for information and communication technology].

# Reference documents

* ISO/IEC 27001 standard, clause A.12.3.1
* ISO/IEC 27017 standard, clause 12.3.1
* ISO/IEC 27018 standard, clauses 12.3.1 and A.9.2
* Information Security Policy
* [Business Continuity Strategy]

# Backup

## Backup procedure

Backup copies must be created for all systems identified in the [Business Continuity Strategy] and with the frequency specified in that document.

[job title] is responsible for backing up the information, software and system images. [If necessary, describe the technology used for making backup copies, specify responsibilities for individual activities, locations for storing backup copies, physical protection for backup copies, encryption, passwords, etc.]

Logs of the backup process are automatically created on systems where the backup copy is made.

## Testing backup copies

Backup copies and the process of their restoration must be tested at least [once every three months] by implementing the data restore process on [identify the server where the data restore is carried out], and checking that all data has been successfully recovered.

[job title] is responsible for testing backup copies. Records on testing backup copies are kept [describe record form – on paper or in electronic form, is there is a prescribed form, etc.].

## Backup information to cloud service customers

[job title] is responsible to provide to the cloud service customers the following information regarding the backup of their information:

* customer responsibilities on backup and restore procedures
* scope and schedule of backups performed on customer’s data
* time schedule and conditions for data restore
* technology used for making backup copies
* locations for storing backup copies
* physical and logical protection applied on backup copies
* any capabilities that are available to allow cloud service customers to perform backup operations by themselves
* [list here other information the organization deems as relevant or is required by contract]

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [Backup process logs] – electronic form | System executing the backup procedure | [job title] | Logs are read-only; they cannot be deleted or edited | Logs are stored for a period of 5 year |
| [Records of backup testing] – 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 year |

# 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 unsuccessful backup tests

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]