[Organization logo]

[Organization name]

BACKUP POLICY

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

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

Commented [270012]: To learn how to manage backup, read this article:

Backup policy – How to determine backup frequency
https://advisera.com/27001academy/blog/2013/05/07/backup-policy-how-to-determine-backup-frequency/

Commented [270013]: There is no need to write a separate document for the Backup Policy if the same rules are prescribed by the Security Procedures for IT Department.

Commented [270014]: 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. BACKUP 3

3.1. BACKUP PROCEDURE 3

3.2. TESTING BACKUP COPIES 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 3

5. VALIDITY AND DOCUMENT MANAGEMENT 4

1. 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].

2. Reference documents

- ISO/IEC 27001 standard, clause A.8.13
- Information Security Policy
- [Business Continuity Strategy]

Commented [27A5]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "05_General_Policies".

3. Backup

3.1. Backup procedure

Backup copies must be created for all systems identified in the [Business Continuity Strategy] and

for storing backup copies, physical protection for backup copies, encryption, passwords, etc.]

Commented [270016]:

Commented [270017]:

3.2. Testing backup copies

Backup copies and the process of their restoration must be tested at least [once every three months]

Commented [270018]: Adjust frequency in accordance with assessed risks.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for	Controls for record protection	Retention time

Commented [270019]:

		storage		
[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 1 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 1 year

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 [2700110]: 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]

[job title]
[name]

_____
[signature]

Commented [2700111]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.