[Organization logo]

[Organization name]

PASSWORD 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]: There is no need to write a separate document for the Password Policy if the same rules are prescribed in the IT Security Policy and in the Access Control Policy.

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

The purpose of this document is to prescribe rules to ensure secure password management and secure use of passwords.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all workplaces and systems located within the ISMS scope.

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

Commented [270014]: Include the name of your company.

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.16, A.5.17, and A.5.18
- Information Security Policy
- Statement of Acceptance of ISMS documents

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

3. User obligations

Commented [270016]: Delete this whole section if the rules are already prescribed in the IT Security Policy.

Users must apply the following good security practices when selecting and using passwords:

Commented [270017]: These are only best practices examples; you can adapt these rules according to assessed risks.

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- strong passwords must be selected, in the following way:
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
- [illegible]
- [illegible]
- [illegible]
- passwords used for private purposes must not be used for business purposes

strongest practices available must be used.

4. User password management

When allocating and using user passwords, the following rules must be followed:

- the temporary password used for first system log-on must be unique and strong, as prescribed above
- the password management system must require the users to change their passwords every three months
- files containing passwords must be stored separately from the application's system data

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.

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

Commented [270018]: Delete this whole section if the rules are already prescribed in the Access Control Policy.

Commented [270019]: Adapt these rules according to assessed risks and system features.

Commented [2700110]: Separate rules may be prescribed for administrator and user passwords.

Commented [2700111]: More details may be provided here.

Commented [2700112]: E.g. by sending an e-mail instructing the user to perform an action, etc.

Commented [2700113]: E.g., last three previous passwords.

Commented [2700114]: E.g. by logging on to the system within a time interval, etc.

Commented [2700115]: This is only a recommendation; adjust frequency as appropriate.

[job title]
[name]

_____
[signature]

Commented [2700116]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.