[organization logo]

[organization name]

**PASSWORD 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](#_Toc454540047)

[2. Reference documents 3](#_Toc454540048)

[3. User obligations 3](#_Toc454540049)

[4. User password management 4](#_Toc454540050)

[5. Validity and document management 5](#_Toc454540051)

# 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].

# Reference documents

* ISO/IEC 27001 standard, clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
* ISO/IEC 27017 standard, clause 9.2.4
* ISO/IEC 27018 standard, clauses 9.2.1 and A.9.2
* Information Security Policy
* Statement of Acceptance of ISMS documents

# User obligations

[organization name]’s users must apply good security practices when selecting and using passwords:

* passwords must not be disclosed to other persons, including management and system administrators
* passwords must not be written down, unless a secure method has been approved by [job title]
* user-generated passwords must not be distributed through any channel (by oral, written or electronic distribution, etc.); passwords must be changed if there are indications that passwords or the system might be compromised – in that case a security incident must be reported
* strong passwords must be selected, in the following way:
  + using at least twelve characters
  + using at least one numeric character
  + using at least one uppercase and at least one lowercase alphabetic character
  + using at least one special character
  + a password must not be a dictionary word, dialectal or jargon word from any language, or any of these words written backwards
  + passwords must not be based on personal data (e.g. date of birth, address, name of family member, etc.)
  + the last three passwords must not be re-used
* password must be changed every 3 months
* password must be changed at first log-on to a system
* passwords must not be stored in an automated log-on system (e.g. macro or browser)
* passwords used for private purposes must not be used for business purposes

For cloud services provided for third parties, the cloud service customers’ user obligations concerning selection and use of passwords must be in compliance with [specify the documents].

# User password management

Considering [organization name]’users, when allocating and using user passwords, the following rules must be followed:

* by signing the Statement of Acceptance of ISMS Documents, users also accept the obligation to keep passwords confidential, as prescribed by this document
* each user may use only his/her own uniquely allocated username
* each user must have the option to choose his/her own password, where applicable
* the temporary password used for first system log-on must be unique and strong, as prescribed above
* temporary passwords must be communicated to the user in a secure manner, and user’s identity must be previously checked
* the password management system must require the user to change the temporary password at first log-on to the system
* the password management system must require the user to select strong passwords
* the password management system must require the users to change their passwords every three months
* if the user requests a new password, the password management system must determine the identity of the user by [specify how]
* the user has to confirm the receipt of the password by [specify how]
* the password must not be visible on the screen during log-on
* if a user enters an incorrect password three consecutive times, the system must block the user account in question
* passwords created by the software or hardware manufacturer must be changed during initial installation
* files containing passwords must be stored separately from the application's system data

For cloud services provided for third parties, the allocation and use of cloud service customers’ user passwords must be in compliance with least these minimal requirements:

* [List here all password allocation and usage rules that all cloud service customers must follow]

Stricter rules defined by cloud service customers are described in [specify the documents]. [job title] must inform cloud service customers’ users about the rules for password management.

In case of cloud service customers’ user password being compromised, cloud service customers’ staff must proceed according to [specify document], which is made available to them by [job title].

# 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:

* number of incidents related to misuse of passwords by unauthorized persons
* number of incidents related to inadequate handling of passwords

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]