Password Policy

| Reference | ISO 27001:2022 A.5.17 |
| --- | --- |
| Version | 1.0 |
| Document Classification | CONFIDENTIAL (see Information Classification Policy) |
| Document Owner | CISO (see Roles and Responsibilities) |
| Approved by |  |
| Approval date |  |
| Release date |  |

**Change Control**

Requests for changes to this document must be sent to the Cybersecurity Steering Commitee at xxx@xxx, providing details and reason.

**Document History**

The log of the changes to this document is available from the Governance Change Log.

**Review Period**

The review period for this document is *twelve months after the issue date and every twelve months thereafter*. It may be subject to ad-hoc review and changes as dictated by business needs or legal and regulatory requirements.

# Introduction

Passwords are crucial in protecting sensitive data and systems from unauthorized access. This policy aims at minimizing the cybersecurity risks associated with weak and compromised passwords.

# Objective

* 1. Promoting a secure use, change, delete, and share of passwords, compliant with ISO 27001 A.9.4.
  2. Defining the policies to protect assets against malicious activities, such as unauthorized access or data breaches, exploiting weak passwords.

# Scope Statement

* 1. Any Staff member must comply with the Password Policy and adopt the Password Management Procedure in this manual for any business related account and for any personal account which, in case of data breach, may have a negative impact on the business.
  2. Any third-party supplier must be compliant to the Password Policy in this document.
  3. Any on-premise or cloud-based system or service must be compliant to this document or provide evidence that the cyber-risk of non-conformity is acceptable.

# Responsibilities

* 1. The CISO is Responsible for:
     1. the definition of the security requirements for the Password Policy,
     2. the definition of the Password Management Procedure and the technologies used for the enforcement of the policy in the procedure,
     3. the analysis of the quantitative or qualitative risk (likelihood and impact) of potential and actual non-conformities, in the business operations, to this document,
     4. to properly disseminate this document and to raise awareness to any other role listed in the following of this section.
  2. Company department managers (CIO, CFO, HR Manager, CTO, etc.) are responsible for:
     1. the adoption of the Password Policy and Password Management Procedure within their departments,
     2. report to the CISO any non-conformity with, or change request to, this document.
  3. All staff shall be Informed of this policy and take responsibility for maintaining the security of their passwords to foster a robust cybersecurity culture.

# Password Policy

## **Password Storage (Confidentiality At-Rest)**

* + 1. Passwords must be stored securely using strong encryption and never stored in plain text.
    2. Company Staff
       1. Must store passwords using a password management software configured to enforce the requirements contained in this policy.
       2. Must never store Passphrases.
  1. **Secure Share (Confidentiality In-Transit)**
     1. Passphrases must never be shared.
     2. Passwords must be shared:
        1. Generating a link from which the recipient can obtain the password such that:
           1. The link is not available after 1 day.
           2. The link is not available after 1 click.
        2. Over an authenticated and encrypted channel offered by a trusted password management software.

## **Complexity**

* + 1. Passwords:
       1. Must be at least 16 characters long.
       2. Must contain a combination of uppercase letters, lowercase letters, numbers, and special characters.
    2. Passphrases must be at least 4 words long separated by one special character.

## **Strength**

* + 1. Passwords:
       1. Must be generated randomly.
       2. Must not contain easily guessable information, such as personal names, common words.
       3. ~~Must not contain repeated symbols.~~
    2. Passphrases:
       1. Must not contain personal information (such as name, surname, date of birth etc).
       2. Must not contain information related to the user (such as friend’s names, dog’s name, usual or latest vacation place etc).

## **Uniqueness**

* + 1. Any password and passphrase must be different from any other business or personal password and passphrase.

## **Rotation**

* + 1. Passwords must be changed at least every 6 months.
    2. Passphrases must be changed at least every year.
    3. Passwords and passphrases must not be intentionally reused (i.e., passwords and passphrases cannot be changed into a password or passphrase previously used, unless this happens due to the randomness of the choice of passwords).

## **Multi-Factor Authentication (MFA)**

* + 1. MFA must be implemented for all accounts.
    2. MFA options must include one or more of the following factors: one-time passwords, biometrics, hardware tokens.

## **Password Recovery**

* + 1. There must be a process for the:
       1. Recovery of the passphrase used for the password management tool
       2. Recovery of the passwords used for the business products and services

# Password Management Procedure

* 1. The CISO
     1. identifies the password management tool
     2. Creates the **Company Password Vault**
     3. Creates all the **Personal Password Vaults**, within the Company Password Vault, for the company Staff members.
     4. Creates **Shared Password Vaults** and is responsible for handling the access control of users and Shared Password Vaults, compliant with the Access Control Policy.
  2. Every Staff member (internal or external) must use the Personal and Shared Password Vaults to use, create, update, share, and delete business credentials.

# Control Process

* 1. A conformance checklist shall be maintained by the CISO to keep track of compliance and non-conformities to the requirements listed in the password policy with respect to the roles, and IT/OT systems and services directly involved in one of the processes (e.g., business or management) of the company.
  2. A threat assessment must be maintained by the CISO to regularly assess the threats to the password policy and password management procedure.

# Violations

Without prejudice to any civil and criminal liability profiles, failure to comply with or violation of the aforementioned rules is punishable with disciplinary measures and compensation provided for by the current labor contract for employees; for collaborators, consultants and external suppliers, verified the seriousness of the violation, with the termination or withdrawal from the agreement relating to them.