ISO 27001:2022

Password Policy

**Non-disclosure**

The information contained in this communication is confidential and intended solely for the recipient. Unauthorized disclosure, copying, or distribution of this information is strictly prohibited. Any views or opinions expressed are solely those of the author and do not necessarily represent those of the organization. By receiving this information, you agree to keep it confidential and to use it only for the intended purpose. If you are not the intended recipient, please notify the sender immediately and delete this message. Thank you for your understanding and cooperation in maintaining the confidentiality of this information.

**Table of contents**

[1 Introduction 3](#_Toc198642054)

[2 Disclaimer 3](#_Toc198642055)

[3 Purpose 3](#_Toc198642056)

[4 Scope 3](#_Toc198642057)

[4.1 Password complexity 4](#_Toc198642058)

[4.2 Password Expiration and Reuse 4](#_Toc198642059)

[4.3 Password Storage 4](#_Toc198642060)

[4.4 Password Reset Procedure 4](#_Toc198642061)

[4.5 Failed Login Attempts 5](#_Toc198642062)

[4.6 User Responsibility 5](#_Toc198642063)

[4.7 System and IT Responsibility 5](#_Toc198642064)

[4.8 Multifactor Authentication (MFA) 5](#_Toc198642065)

[4.9 Monitor and Review 5](#_Toc198642066)

[5 Policy requirements 6](#_Toc198642067)

[5.1 Password complexity 6](#_Toc198642068)

[5.2 Password Expiration and Reuse 6](#_Toc198642069)

[5.3 Password Storage 6](#_Toc198642070)

[5.4 Password Reset Procedure 7](#_Toc198642071)

[5.5 Failed Login Attempts 7](#_Toc198642072)

[5.6 User Responsibility 7](#_Toc198642073)

[5.7 System and IT Responsibility 7](#_Toc198642074)

[5.8 Multifactor Authentication (MFA) 7](#_Toc198642075)

[5.9 Monitoring and Review 7](#_Toc198642076)

[6 Non-Compliance 8](#_Toc198642077)

[7 User Agreement Policy 8](#_Toc198642078)

[8 Annex 9](#_Toc198642079)

# Introduction

In today's digital landscape, safeguarding sensitive information is essential for maintaining an organization's integrity and reputation. A strong password policy is a critical component of our information security strategy, designed to protect against unauthorized access and data breaches.

This Password Policy establishes guidelines for the creation, management, and protection of passwords across the organization. By enforcing stringent requirements for password complexity, storage, and expiration, we aim to mitigate risks associated with weak or compromised passwords.

Applicable to all employees, contractors, and vendors, this policy emphasizes the shared responsibility of users in securing our digital assets. By fostering a culture of security awareness and compliance, we can effectively defend against evolving cyber threats and uphold the trust of our clients and stakeholders.

# Disclaimer

This policy is intended to provide guidelines for users to enhance the security of their accounts and the organization’s information systems. However, compliance with this policy does not guarantee complete security against all threats, as cybersecurity is an ever-evolving field.

Users are encouraged to remain vigilant and proactive in their security practices beyond the guidelines provided. The organization reserves the right to modify this policy at any time to address emerging threats or changes in technology. Failure to comply with this policy may result in disciplinary action, including termination of access or employment. By signing this agreement, users acknowledge their understanding of these terms and their commitment to uphold the organization's security protocols.

# Purpose

The purpose of this password policy is to establish a robust framework for the creation, management, and protection of passwords within the organization, in alignment with the requirements of ISO/IEC 27001. Passwords are a critical component of an organization's information security strategy, serving as the first line of defense against unauthorized access to systems, applications, and sensitive data.

This policy aims to:

Protect the confidentiality, integrity, and availability of the organization's information assets by ensuring that only authorized individuals can access them.

Minimize the risk of unauthorized access and potential data breaches by enforcing strong password practices.

Foster a culture of security awareness among employees, contractors, and other stakeholders by emphasizing the importance of password security.

By adhering to this policy, the organization ensures that its information security management system (ISMS) aligns with international best practices, thereby enhancing its overall security posture and reducing vulnerabilities.

# Scope

This password policy applies to all individuals and systems within the organization that interact with or manage sensitive information.

Specifically, it covers:

* Password complexity;
* Password Expiration and Reuse;
* Password Storage;
* Password Reset Procedure;
* Failed Loggin Attempts;
* User Responsibility;
* System and IT Responsibility;
* Multifactor Authentication (MFA);
* Monitoring and Review.

The policy is designed to ensure that:

Passwords are created, stored, and managed securely across all systems.

Users are educated on best practices for password security to reduce the risk of human error.

The organization complies with regulatory and contractual obligations related to information security.

By defining clear guidelines for password management, this policy supports the organization's broader goal of safeguarding its information assets and maintaining trust with stakeholders.

## Password complexity

Password complexity refers to the requirement for passwords to include a diverse mix of characters, such as uppercase letters, lowercase letters, numbers, and special symbols, to enhance security. This diversity increases the number of possible combinations, making it significantly more challenging for attackers to crack passwords through brute force methods. However, while complexity is important, it should be balanced with usability, as overly complex requirements can lead users to create predictable patterns, ultimately undermining security efforts.

## Password Expiration and Reuse

Password expiration is a security measure that requires users to change their passwords after a specified period, typically every 90 days, to reduce the risk of unauthorized access. This practice helps prevent password reuse, as users are encouraged to create new, unique passwords rather than slightly modifying old ones, which can lead to predictable patterns and vulnerabilities. However, it is essential to provide users with guidance on creating strong passwords to ensure that the new passwords are not only unique but also complex enough to withstand potential attacks. By implementing a robust password expiration and reuse policy, organizations can significantly enhance their overall security posture and protect sensitive information from breaches.

## Password Storage

Password storage is the practice of securely saving user passwords within a system to protect them from unauthorized access and potential breaches. Instead of storing passwords in plain text, they should be hashed using strong cryptographic algorithms, such as bcrypt or Argon2, which transform the original password into a fixed-length string that is difficult to reverse-engineer. Additionally, implementing techniques like salting—adding random data to the password before hashing—further enhances security by ensuring that identical passwords yield different hashes. Proper password storage practices are crucial for maintaining user trust and safeguarding sensitive information against cyber threats.

## Password Reset Procedure

The administrator must verify the user's identity, which may involve confirming details such as the user's full name, username, or other identifying attributes to ensure the correct account is selected. Once the user is identified, the administrator on the account and selects the "Reset Password" option. A new password is then entered, adhering to the organization's password policy, and the administrator can optionally enforce the user to change their password at the next logon by setting the "User must change password at next logon" option.

This ensures both security and compliance with organizational policies.

## Failed Login Attempts

A failed login attempt refers to an unsuccessful effort made by a user to access a system or application, typically due to incorrect credentials such as a wrong username or password. These attempts are tracked by the system to enhance security and identify potential unauthorized access attempts. After a specified number of failed attempts, the user's account may be automatically locked to prevent further access and protect sensitive information from potential breaches.

## User Responsibility

Users have a critical responsibility to protect their account credentials by creating strong, unique passwords and keeping them confidential. They must also adhere to the organization's security policies, including regularly updating their passwords and reporting any suspicious activity or potential security breaches. Additionally, users should be proactive in educating themselves about best practices for password management and cybersecurity to minimize risks. By taking these responsibilities seriously, users contribute significantly to the overall security and integrity of the organization's information systems.

## System and IT Responsibility

The IT department is tasked with implementing and maintaining robust security measures, including the enforcement of password policies and the secure storage of user credentials. They are responsible for regularly monitoring system access and conducting audits to identify vulnerabilities and ensure compliance with security standards. Additionally, IT personnel must provide training and support to users, helping them understand best practices for password management and cybersecurity. By fulfilling these responsibilities, the IT team plays a crucial role in safeguarding the organization's data and maintaining a secure computing environment.

## Multifactor Authentication (MFA)

Multifactor Authentication (MFA) is a security mechanism that requires users to verify their identity using multiple factors, such as something they know (password), something they have (a smartphone or token), or something they are (biometric data). This layered approach significantly enhances security by making it harder for attackers to gain unauthorized access, even if one factor, like a password, is compromised. Organizations are strongly encouraged to implement MFA wherever their infrastructure allows, as it is considered a critical cybersecurity measure to protect sensitive data and systems. When implemented effectively, MFA reduces the risk of breaches caused by compromised credentials and strengthens overall organizational security.

## Monitor and Review

Monitoring and review are essential processes that help organizations assess the effectiveness of their security measures and policies, including password management. By continuously tracking user compliance and system performance, organizations can identify potential vulnerabilities and areas for improvement. Regular reviews allow for the evaluation of collected data, enabling teams to reflect on their security practices and make informed decisions about necessary adjustments. This proactive approach not only enhances the overall security posture but also fosters a culture of accountability and continuous improvement among users and IT personnel. Ultimately, effective monitoring and review processes contribute to a more resilient and secure organizational environment.

# Policy requirements

## Password complexity

Complex passwords reduce the likelihood of brute force attacks and unauthorized access.

Passwords must meet the following complexity requirements:

* Minimum length for users: 9 characters.
* Minimum length applications: 14 characters.

Must include at least:

* One uppercase letter (e.g., A–Z).
* One lowercase letter (e.g., a–z).
* One numeric digit (e.g., 0–9).
* One special character (e.g., @, #, $, %, &).

Passwords must not include easily guessable information, such as:

* Usernames.
* Personal information (e.g., names, birth dates, etc.).
* Common dictionary words or patterns (e.g., "password123").

## Password Expiration and Reuse

Regular password changes limit the time an attacker can exploit a compromised password.

* System user’s passwords must be changed every 60 days (or more frequently if required by a risk assessment).
* System application passwords (e.g. SDMS and DB) must be changed every 45 days (or more frequently if required by a risk assessment).
* Users may not reuse any of their last 5 passwords.
* Temporary passwords must be valid for a maximum of 24 hours and require a mandatory change upon first use.

## Password Storage

Storing passwords securely prevents unauthorized access in case of a data breach.

* Passwords must not be stored in plain text and should always be protected using strong hashing algorithms to prevent unauthorized access.
* Specifically, all passwords not related to Active Directory must utilize robust hashing methods such as bcrypt, PBKDF2, or Argon2 to ensure that even if the hashed data is compromised, it remains extremely difficult to reverse-engineer the original passwords.
* Passwords must never be shared via insecure methods such as email, messaging apps, or written notes.

Additionally, any password storage mechanism must be regularly reviewed and updated to incorporate the latest security practices and technologies.

## Password Reset Procedure

Secure password reset processes prevent attackers from exploiting weak recovery mechanisms.

* Identity Verification: Before resetting a password, verify the user's identity using secure methods like security questions, email verification, or multi-factor authentication.
* Lockout Duration: Temporarily lock the account for a set period 30 minutes to deter attackers while minimizing disruption to legitimate users.

## Failed Login Attempts

* Systems must lock user accounts after 5 consecutive failed login attempts.
* Locked accounts should only be unlocked by the IT/security team or through a secure self-service process.

## User Responsibility

* Users are responsible for maintaining the confidentiality of their passwords.
* Users must:
  + Never disclose their passwords to anyone, including IT staff.
  + Avoid using the same password for personal and work accounts.
  + Report suspected password compromises immediately to the IT/security team.
  + If passwords must be written down, they should be stored securely, such as in a locked safe or an encrypted password manager.

## System and IT Responsibility

* The IT department is responsible for:
  + Enforcing password policy settings in all systems using Group Policy Object (GPO) Password Policy in Active Directory.
  + Providing secure mechanisms for password recovery.
  + Performing regular audits to ensure compliance with this policy and identify any gaps.
  + Educating users about password security best practices.

## Multifactor Authentication (MFA)

If overall IT infrastructure allow and support:

* MFA must be implemented for all critical systems and sensitive data access.

## Monitoring and Review

* This policy must be reviewed annually and updated in response to emerging security threats or changes in operational requirements. Results of audit has to deliver to:
  + Managing director
  + CISO
  + Head of
  + Team Leadn

# Non-Compliance

Non-compliance with the password policy can lead to serious security vulnerabilities, increasing the risk of unauthorized access to sensitive information.

Individuals who fail to adhere to the established guidelines may face disciplinary actions, which could include retraining, account suspension, or even termination, depending on the severity of the violation.

Furthermore, persistent non-compliance can undermine the organization's overall security posture, potentially exposing it to data breaches and legal liabilities, thereby affecting its reputation and trustworthiness in the industry.

# User Agreement Policy

All system users must formally agree to this policy by providing their signature, indicating their understanding and commitment to adhere to its rules and guidelines. This agreement serves as a binding acknowledgment that users are aware of their responsibilities regarding security practices, including password management and multifactor authentication.

By signing, users also accept the consequences of non-compliance, which may include disciplinary actions or restricted access to systems. This process not only reinforces accountability but also fosters a culture of security awareness within the organization. Ultimately, requiring a signature ensures that all users are aligned with the organization's security objectives and are actively participating in safeguarding its information assets.

# Annex

**User Agreement**

By signing below, I acknowledge that I have read, understood, and agree to comply with the organization's password policy and security guidelines. I understand my responsibilities regarding password management, multifactor authentication, and the consequences of non-compliance. I commit to following the rules outlined in this policy to help maintain the security and integrity of the organization's information systems.

|  |  |
| --- | --- |
| Company: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Project name: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Name and Surname: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| System username: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Department: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

This signature serves as a formal agreement to uphold the standards set forth in the password policy and to actively contribute to the organization's cybersecurity efforts.