**<Your Company Logo>**

**Password Management Policy**

# ***Version Control Table***

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Reviewed |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

|  |  |
| --- | --- |
| **Date of Next Revision** | **<date>** |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status and at yearly intervals after that.

The version control table will show the published update date and provide a thumbnail of the significant change. CAUTION: the thumbnail is not intended to summarize the difference and is not a substitute for reading the full text.

# 

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_arxqdy8knprl)

[**Table of Contents 5**](#_cj9vnfyr0ye6)

[**Purpose 6**](#_xwg0fms4e2gq)

[**Scope 6**](#_e8vmszom3kxt)

[**Policy 6**](#_54buvhmopnd1)

[Strong passwords must have the following characteristics: 6](#_s5k0ix4004ji)

[Confidentiality 6](#_kfgb4jo0m47j)

[Password Security 6](#_wxq4e07pxbcb)

[MFA 7](#_8e109gda3gb5)

[Password rotation 7](#_ni62umbecxm6)

[**Disciplinary actions 7**](#_oo4pebgvtuk2)

[**Change, Review, and Update 7**](#_6cu0cv3y3y7n)

[**Responsibility 7**](#_fxvzxllev4xj)

[**Reference 7**](#_1ksv4uv)

[**Related Documents 7**](#_fdh46p3e88r)

# 

# Purpose

The purpose of these guidelines is to provide best practices for creating strong passwords and provide reliable protection of passwords.

# Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third party that uses <Company> information assets or information resources and services.

# Policy

The organization mandates that users adhere to the following guidelines on password construction.

This policy is partially based on the National Institute of Standards and Technology (NIST) Special Publication 800-63B Digital Identity Guidelines, which provide best practices related to authentication and password lifecycle management.

## Strong passwords must have the following characteristics:

* The passwords contain both upper- and lower-case characters (e.g., a-z, A-Z).
* Passwords contain at least one punctuation character (ex. !#$^&\*()\_+|~-=\`{}[]:";'<>?,./)
* Passwords contain numeric characters (0-9)
* The password is at least twelve alphanumeric characters long.
* The password is not a word in any language, slang, dialect, jargon, etc.
* The password is not based on personal information, names of family, etc.

## Confidentiality

The following guidelines apply to the confidentiality of company passwords:

* Users must not disclose their passwords to anyone.
* Users must not share their passwords with others (co-workers, supervisors, family, etc.).
* Users must not write down their passwords and leave them unsecured.
* Users must not check the “save password” box when authenticating to applications.
* Users must not use the same password for different systems and accounts.
* Users must not reuse passwords.

## Password Security

All <Company> employees must use Password Manager to store their credentials securely. It’s recommended to use Random Password Generator to create unique and strong passwords.

Passwords must not be shared in plain text. <Company> employees must use Password Managers or Secure password-sharing services <Name of Service> for this purpose.

## MFA

Multi-Factor Authentication must be enabled on all systems processing <Company> and clients' information if it’s supported.

## Password rotation

Users must change passwords every 90 days at a minimum. Automatic password rotation must be configured on the following system:

1. Google Workspace
2. AWS
3. <Other systems>

# Disciplinary actions

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Management will determine how severe an employee’s offense is and take the appropriate action.

# Change, Review, and Update

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 Annex A.9.2.4 Management of Secret Authentication Information of Users
* ISO 27001 Annex A.9.4.3 Password Management System

# Related Documents

* <Company> Access Management Policy