Password Policy

Doorway

SOC 2 Criteria: CC6.1
ISO 27001 Annex A: A.9.2.4, A.9.3.1

Keywords: Password requirements, Password Manager, Complex passwords, 2FA, MFA

Purpose

This policy describes the procedure to select and securely manage passwords at Doorway.

Scope

This policy applies to all Doorway employees, contractors, and any other personnel who have an account on any system that resides at any company facility or has access to the company network.

Roles and Responsibilities

The Security Officer is responsible for updating, reviewing, and maintaining this policy.

Policy

If a password is suspected of being compromised, the password in question should be rotated and the Security Officer should be notified immediately.

Password Requirements

- Complex passwords are required where possible. Complex passwords have at least 10 characters, 1+ uppercase letter(s), 1+ lowercase letter(s), 1+ non-alphanumeric character(s)
- Passwords must have at least 8 characters
- Do not reuse previously used passwords or their variants
- Do not use commonly used passwords

MFA Requirements

- MFA must be enabled for any and all systems that provide the option for Multi-Factor Authentication (MFA)

Password Protection

- All passwords are treated as confidential information and should not be shared with anyone. If you receive a request to share a password, deny the request and contact the system owner for assistance in provisioning an individual user account.
- If you are required to maintain your own secret authentication information, you will be provided initially with a unique, individual, and secure temporary secret authentication information in a secure manner, which you must acknowledge its receipt, and change on first use.
- Do not write down passwords, store them in emails, electronic notes, or mobile devices, or share them over the phone. If you must store passwords electronically, do so with a password manager that has been approved by Doorway:
- Doorway's approved Password Manager: 1Password.
- If you absolutely must share a password, do so through the approved password manager or grant access to an application through a single-sign-on (SSO) provider.
- If you suspect a password has been compromised, rotate the password immediately and notify the Company's Security Officer.
- Passwords stored in systems must be stored with a unique salt and as a one-way hash using an approved password hashing algorithm (pbkdf2, bcrypt, scrypt) and an HMAC-SHA256

Enforcement

- An employee or contractor found to have violated this policy may be subject to disciplinary action.

Revision History

Version	Date	Editor	Description of Changes
1.0	24.02.2022	Henry Sinclair	Initial Creation