LAST UPDATE DATE	04-24-2025
OWNER	JEFF LILLIBRIDGE
STATUS	APPROVED

PASSWORD POLICY

Approval History

Version	Approved By	Approved On
1.0	Not Present	04-24-2025

Purpose

The purpose of the Password Policy is to outline procedures to securely manage passwords and ensure strong authentication mechanisms for all information management systems in City of Madeira Beach.

Scope

Password policy applies to the following:

- All Employees of City of Madeira Beach
- All Contractors of City of Madeira Beach
- All vendors / third-party/visitors
- All information systems
- All 3rd party applications

Background

Strong passwords for an application are the first line of defense against malicious actors. This policy is intended to define the rules of how City of Madeira Beach employees can maintain strong and secure passwords when using multi-factor authentication and also how all information systems can enforce best practices for strong passwords.

Policy

Password complexity and strength

- All passwords must be at least 8 characters, including upper case, lower case, number, and a special character.
- Passwords should not allow personal information such as birthdates, full names, or city of birth.
- Common patterns such as QWERY12345 should not be allowed.
- The last 5 passwords should not be recycled.

Password Rotation

- All system and user-level passwords should be rotated on at least a quarterly basis.
- If a credential is suspected of being compromised, the password in question should be rotated immediately, and the Engineering/Security team should be notified.

Recommended practices for secure password management

- All passwords are treated as confidential information and should not be shared with anyone. If you receive a request to share a password, immediately report to your manager or information security team.
- 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 IT. If you genuinely must share a password, do so through a designated password manager or grant access to an application through a single sign-on provider.
- Do not use the 'Remember Password' feature of applications and web browsers.
- Avoid using the same password for multiple products or services.

Multifactor Authentication

- Multifactor authentication aims to provide added protection to systems beyond password authentication.
- All publicly accessible systems such as Google Workplace should be secured using a multifactor authentication method.
- Multifactor authentication can include password and token/device verification, password and email verify, password and MFA app verification, and password and SMS/text code verification, among other methods.

Password Failed Limits

- The purpose of password limits is to protect against dictionary attacks or password guessing attempts.
- A limit should place on the number of failed password entries to 5 wrong password entries on production systems.

Enforcement

Information security team and each employee is responsible and accountable for enforcing password policy requirements.