Password Policy

Full Council Approved:	3 June 2026
Last Reviewed:	June 2026
Due for next Review:	June 2029

1. Purpose

The purpose of this policy is to define the requirements for creating strong passwords, the protection of those passwords and the frequency of change. Usernames (for identification) used in combination with passwords (for authentication) are countermeasures for preventing unauthorised users from accessing sensitive information/facilities and for maintaining audit trails to facilitate accountability.

2. Scope

The scope of this policy applies to all personnel who have or are responsible for an account on any information systems, services (e.g. email), secure areas, equipment, and network.

3. Policy

- Passwords must never be shared, unless confirmed by the Executive Officer.
- All default passwords must be changed immediately. Users must create their own password from the first time they are granted access.
- Passwords must never appear in plain text on computer screens, written down on paper (e.g., yellow stickers), or stored on a location for fast access (e.g., Slack, Outlook etc.).
- Passwords must be stored in an encrypted format.
- Usernames and passwords must not be scripted to enable automatic login.
- Passwords should not be stored in browsers (autofill).
- Employees must never use the same password on Fleet Town Council resources as for non-Fleet Town Council resources (e.g. Facebook).
- Employees must make use of strong passwords that use a combination of upper/lowercase letters, numbers, and symbols, and have in mind that the longer they are in length, the more time it takes to an intruder to guess them.
- A password history must be maintained to ensure that the new password will not be the same as any of the previous twenty-four (24) that have been used.
- System configuration settings are set to require that system/session idle time out features have been set to a period of fifteen (15) minutes (or less).
- Administrators must verify a user's identity before performing any password resets.

- Group or shared accounts/passwords must not be used, and generic accounts must be disabled. Accounts should be set up using employee names and emails, not in generic accounts.
- Accounts must be locked for at least thirty (30) minutes or require an administrator to unlock them after six (6) failed login attempts.
- Access for terminated users must be revoked immediately.
- Inactive user accounts must be removed or disabled at least every three months.
- Any accounts used by vendors for remote support or maintenance must be enabled only during the period needed and then are disabled.
- Any vendor accounts that are enabled for remote support or maintenance to any system component must be monitored when in use.
- Two Factor Authentication (2FA) should be enabled where available.
- Passwords should be stored in a password manager – The approved password manager is Keeper.
- All system level passwords e.g. root, admin accounts, must be changed at least every 90 days. (Within Keeper's notification centre you can set it to send alerts for time-sensitive items).
- If an account or password is suspected to have been compromised, the password should be changed immediately.

4. Mandatory Requirements

USERNAMES

- Each user must be assigned a unique and personal username that is derived from their first and last name.
- Usernames must be logged when accessing a system's resources.
- Usernames must not be available for selection from a list at the log-on screen of any information system. Additionally, usernames used for accessing an information system by a user must not be displayed or, where possible, be available to another user.
- Usernames must be treated as internal information.

PINS

- A personal identification number (PIN) is a numeric password shared between a user and system that can be used to authenticate a user to a system.
- Avoid using predictable patterns such as "1111" or "1234" and avoid using your day/month/year that you were born (i.e. 1102) for 11th of February.
- One way to create a PIN is to create it from a word. For instance, think of the keypad of your mobile phone. The word "word" would be converted to the PIN 9673 (the W is on the 9, the O is on the 6, the R is on the 7 and the D is on the 3).
- PINS must be treated as confidential information.
- It is the responsibility of each user not to disclose a PIN he/she owns to anybody else and to change it immediately upon a suspected or confirmed disclosure.

PASSWORDS

- The following password formation shall meet the following complexity requirements:
- • The password must be no less than eight (8) characters.

- The password must contain characters from at least three of the following four categories:
    - Uppercase characters (A-Z).
    - Lowercase characters (a-z).
    - Base 10 digits (0-9).
    - Non-alphanumeric (i.e. !,%,@ etc.).
- The password must be a non-dictionary word.
- The password must not be based on family names, friends, pets etc.
- It is strongly recommended to use passphrases. A pass phrase is a sequence of words that provide a bigger entropy in terms of guessing a password. A good passphrase example: I love to play squash becomes IL0ve2Play$qua£h

5. Related Documents

- Access Control Procedure
- Acceptable Use Policy
- Anti-Malware Policy
- Information Security Awareness Policy