INFORMATION TECHNOLOGY POLICY/PROCEDURE/PROCESS

Title:	**PASSWORD POLICY**	Policy Number: APP 706
Effective:	July 13, 2022	
Supersedes:	December 14, 2018	
Approval:	Tom Shewchuk, IT Director	Page 1 of 2

1.0 Scope

☒ Full-time
☒ Part-time
☒ Temporary/Contract
☒ Salaried
☒ Union
☒ Independent Contractors
☒ Visitors and Vendors
☒ Volunteers/Unpaid Interns

Employees who are covered under the provisions of a collective bargaining agreement will follow the standards as contained in their respective contracts if this policy conflicts with the language in the contract.

This policy is applicable Citywide. All users of City computer and technology resources are expected to comply with this policy as a condition of continued employment or contracted services.

The provisions of this Policy are subject to, and may be superseded by (in the event of a conflict), relevant provisions of applicable collective bargaining agreements between the City and the various collective bargaining associations of the City

2.0 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of the City of Ann Arbor's resources. All users, including contractors and vendors with access to the City of Ann Arbor systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

4.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City of Ann Arbor facility, has access to the City of Ann Arbor computing network, or stores any non-public City of Ann Arbor information.

5.0 Policy

5.1 General

5.1.1 Password Aging

All City of Ann Arbor employees (fulltime, part-time and temporary) will be required to change their passwords every 90 days when logging onto the City of Ann Arbor computing network.

5.1.2 System Administrator Passwords

All system-level passwords (e.g., root, domain administrator, application administration accounts, etc.) must be changed promptly after a staff member who had administrative level access to City IT computing assets leaves the organization.

5.1.3 System Administrator Password Protection

All production system-level passwords used by Information Technology staff must be stored in a separate, secure system for password management (e.g. KeePass).

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

All employees with a network password, as well as individuals with system-level passwords, must conform to the guidelines described below for all City of Ann Arbor employees accessing the City's computing network.

5.2 Guidelines

5.2.1 General Password Construction Guidelines

All users at The City of Ann Arbor should be aware of how to select strong passwords. Strong passwords have the following characteristics and must be constructed using the criteria below:

- **Minimum Password Length** determines how short passwords can be. The minimum password length is fifteen (15) alphanumeric characters.
- **Password Complexity Requirements** determines whether password complexity is sufficient. User passwords must meet the following requirements:
    - The password contains characters from at least three of the following four categories:

        - English uppercase characters (A - Z)
        - English lowercase characters (a - z)
        - Base 10 digits (0 - 9)
        - Non-alphanumeric (For example: !, $, #, or %)
- **Password History** determines the number of unique new passwords a user must use before the user may reuse a prior password. Password history is set at 10 for all City of Ann Arbor employees.

5.2.2 Weak Passwords

Weak passwords will no longer be allowed for logging onto the City's computing network. Weak passwords exhibit the following characteristics:

- The password contains less than eight characters;
- The password is a word found in a dictionary (English or foreign);
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "The City of Ann Arbor" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

5.2.3 Password Protection Standards

- Passwords should not be shared unless explicitly approved by a manager as part of an approved business process. The IT Director should also be notified when this is necessary. If someone demands access to a password for which they are not explicitly approved, refer them to this document and direct them to the Information Technology Services Unit.
- Always decline the use of the "Remember Password" feature of applications. If an account or password compromise is suspected, report the incident to the Information Technology Services Unit.
- Always use different passwords for City of Ann Arbor accounts from other non-City of Ann Arbor access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various City of Ann Arbor access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.

- Do not share the City of Ann Arbor passwords with anyone, including administrative assistants, secretaries, co-workers or supervisors. All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored on-line without encryption.
- Staff should not reveal passwords in email, chat, or other electronic communication. System administrators may provide initial or reset passwords electronically, but they will do so via secure means such as encrypted email or Microsoft Teams communications.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including discharge. Password cracking or guessing may be performed on a periodic or random basis by the Information Technology Services Unit or its delegates in order to ensure the security of the system. If a password is guessed or cracked during these exercises, the user/owner will be notified and will be required to change it immediately.