*City of Milwaukee*

# Password Policy

| NIST Reference: | Implementation Date : | Revision Number : |
|---|---|---|
| AC – Access Control<br>AT – Awareness and Training<br>IA – Identity and Authentication | October 12, 2021 | 0.2 |

## PASSWORD POLICY

### PURPOSE

The purpose of this policy is to establish a standard for the creation of strong passwords, protection of those passwords and the frequency of change to effectively protect information systems and data from unauthorized access.

### SCOPE

The scope of this policy includes all personnel who use or are responsible for any form of access that supports information systems which reside at any City of Milwaukee facility; including all contractors, vendors, or agents who have access to the City of Milwaukee network or electronically store any City of Milwaukee information. Any reference in this document to "employee" or "City employee" shall be considered to include any contractor, vendor, or agent working for or representing the City but not in City employ.

### GENERAL POLICY

City information systems and networks are required to enforce strong passwords that meet minimum security standards.

### PASSWORD REQUIREMENTS

All passwords are to be treated as sensitive, confidential information and therefore need to meet the following requirements for AD and applications:

- All passwords must be at least eight characters long.
- Password history is enforced. Number of passwords remembered; 10.
- All passwords must be alphanumeric (Contain at least one (1) letter and number).
- Multi-Factor Authentication is mandatory for all user accounts.
- Passwords are required to be changed when there is reason to believe a password has been compromised or fails to meet our Password Requirements.
- The number of unsuccessful consecutive attempts by a user to enter a password and log into a system or application should be limited to protect against brute force attacks. System administrators should immediately disable passwords for users that change assignments or leave employment with the City.

| NIST Reference: | Implementation Date : | Revision Number : |
|---|---|---|
| AC – Access Control<br>AT – Awareness and Training<br>IA – Identity and Authentication | October 12, 2021 | 0.2 |

- The system administrator should provide an initial password to each user when logging on for the first time. The initial password assigned by the system administrator should be valid only on the user's first session. The user should choose another personal password during the course of the initial session.

## ADDITIONAL USER REQUIREMENTS

Passwords should not be written down. Password managers authorized by the organization, may be used for storing login information.

- Passwords should not be stored in a file on any computer system or device (including hand held devices, flash drives, or similar devices) without encryption.
- Passwords should not be shared with anyone, including supervisors, other City employees or family with the exception of network administrators during maintenance.
- Create passwords that are easily remembered but meet the requirements of a strong password. The use of pass phrase or key board associations can make strong passwords easy to remember.
    - A Common practice to create easy to remember complex passwords is substituting letters for similar numbers or letters. Some examples include; A=@, B=8, S=$, i=!, E=3, O=o and L=7. Using this method passwords can be constructed thusly; Il!k3$tr0ngP@sswords, $p@in1492, US@Ju7y4th, B3tt3rProt3ct!on.
    - A pass phrase can be used to help create a password and use the first letter of each word. A password created with a pass phrase needs to contain a combination of both letters and numbers and can be made stronger through the use of special characters. For example, the phrase might be: "This may be one way to Remember!" and the password could be: "TmB1W2R!" or "TmB1W>r~" or some other variation.
    - Shift row on keyboard. A password includes the use of a memorable word, even a dictionary word, but move the hands up a row from the home row on the keyboard when typing it. This way, "GoFishing?" would become T9R8wy8ht?".
- Weak passwords contain any of the following characteristics and should not be used:
    - Words found in a dictionary (English or foreign), slang, dialect, jargon, etc
    - Names of family, user's job, pets, friends, co-workers, fantasy characters, sport team, etc.
    - Any part of the individual name or username in the password
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The "City of Milwaukee" or any derivation of the City's name (cityofmilw).
    - Birthdays and other personal information such as addresses.
    - Word or number patterns.

| NIST Reference: | Implementation Date : | Revision Number : |
|---|---|---|
| AC – Access Control<br>AT – Awareness and Training<br>IA – Identity and Authentication | October 12, 2021 | 0.2 |

  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit
- A dictionary to blacklist a set of commonly used passwords should be used which includes dictionary words, repetitive or sequential strings, passwords taken in prior security breaches, variations on the site name, commonly used passphrases, or other words and patterns that cybercriminals are likely to guess.
- If the user suspects their password has been compromised or observed by others, the password must be changed immediately.

## POLICY EXCEPTIONS

Some information systems including operating systems applications can not comply with this policy due to system limitations. System owners/administrators of such systems must complete the compensating controls worksheet found on the IT Profiles System within the MINT.

System Accounts (Automated program access) are not required to comply with the Password Policy. Systems used by citizens are not required to comply with the Password Policy.

## ENFORCEMENT

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## REVISION HISTORY

| Revision | Date | Changes |
|---|---|---|
| 0.0 | June 1, 2011 | Initial Release |
| 0.1 | July 8, 2019 | Format Revision, updated password requirements. |
| 0.2 | October 12, 2021 | Added dictionary restrictions to password policy. |