# City of Milwaukee
# Information Technology Systems
# Password Policy

## I. Overview

All City departments that have information systems and networks need to ensure that access to these systems is restricted to safeguard the City's assets and data. Passwords are an important aspect of computer system security. Passwords help protect the integrity of City data and safeguard City assets and data against fraud, misuse, and theft. Employees with administrative and regular access to Active Directory and City applications are responsible for taking the appropriate steps to select and secure strong passwords.

## II. 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.

## III. 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.

## IV. Policy

City information systems and networks are required to enforce strong passwords that meet the minimum security standards outlined in Section V. Password strength should reflect the environment that the information system is deployed in, and the likely threats it will face. However, minimal password requirements as outlined in Section V are required to provide baseline protection of City data and information systems.

Information Systems administrative personnel charged with the management of **Active Directories** and **applications** should configure the end user passwords to enforce strong password requirements as outlined in Section V.

Administrative accounts like the Domain Administrator, Application administrator and Database Administrator must also comply with the strong password requirements as outlined in Section V.

The default manufacturer passwords for administrative system and hardware management accounts must be changed at setup.

Some production legacy systems may not be able to comply with this Policy due to system limitations. These systems are discussed in section VI, Policy Exceptions.

System compliance status with the password policy must be reported annually by August 30th through the IT Profiles System on the MINT (www.milwaukee.gov/ITProfile).

## V. 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.
- All passwords must be alphanumeric (Contain at least one (1) letter and number).
- All passwords must set to change at least every 90 days.
- The number of unsuccessful consecutive attempts by a user to enter a password and log into a system or application should be limited to no more than five (5) attempts.
- System administrators should immediately disable passwords for users that change assignments or leave employment with the City.
- 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 but if it is necessary they should be kept in a secure location like a locked drawer.
- 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. Refer to Appendix A for tips and guidelines.
- If the user suspects their password has been compromised or observed by others, the password must be changed immediately.

## VI. 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.

Systems that are not limited in their ability to enforce given password requirements and are functionally able to enforce the password requirements in section V do not qualify for exception status.

Document files from applications like Excel, Word or Adobe PDF are not required to be password protected under this policy.

## Appendix A. Tips and Guidance on Creating Strong Passwords

Creating and remembering strong passwords can be constructed using one of the following techniques:

- 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.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit

## Appendix B. Considerations for Compensating controls

- Implementing dual factor authentication through an RSA token (http://www.webopedia.com/TERM/R/RSA.html)
- Monthly review of system activity log signed off by management
- Manually enforce password changes by generating a stale password report and asking non compliant users to update their passwords.