Category: ITS Policy Policy No.: ITS-03-2024 Revisions: February 7, 2024	middlesex centre in the centre of it all	Pages: 5 Effective Date: Feb 7, 2024 Report No.: CPS-06-2024

User Accounts and Passwords

Purpose

Passwords are an important aspect of computer security. A poorly chosen password or a password which is not protected may result in unauthorized access to the Municipality's Network or Information Systems. All users who access the Municipality's Network or Information Systems are responsible for taking the appropriate steps to select and secure their passwords.

It is imperative that anyone who has access to confidential information or information that is protected through privacy legislation, ensure that this policy is followed. This policy defines the use of secure passwords, passphrases, or personal identification numbers to secure sensitive data or information on servers, systems, devices, websites, or software used at Middlesex Centre.

Policy

This policy provides guidelines to Users who access the Municipality's Network and/or Information Systems. It establishes a standard for the creation of strong passwords, the protection of passwords and the frequency of change.

Passwords, passphrases, and personal identification numbers (PINs) shall be used to restrict access to workstations, systems, servers, or services. These passwords, passphrases and PINS shall be designed and utilized in a manner which renders them secure and prevents unauthorized use. Passwords, passphrases, and PINs shall be unique to the account and service for which they have been provisioned.

To add further security, the use of two-factor authentication is encouraged wherever practically possible and/or available.

Scope

This policy applies to Members of Council, all employees of Middlesex Centre including Paid-on-Call Firefighters, and others who perform work or provide services to, or on behalf of, the Municipality, who have a user account and password to access the Municipality's Network or Information Systems.

Definitions

For the purpose of this document, the following terms have the following meanings:

"Biometric Security" is the use of a uniquely identifiable human characteristic for securing sensitive data or information. This includes (but is not limited to) fingerprint, voice, or facial recognition.

"Core Infrastructure" is any device connected to the Middlesex County Network which is responsible for providing a critical service or function, such as a firewall, switch, or server.

"Information Systems" means any computer hardware and/or software system that individuals and organizations use to collect, filter, and process, create and distribute data.

"ITS" means Information Technology Services.

"Middlesex County ITS" is the department at Middlesex County responsible for procurement, maintenance, and support of Information Systems.

"Municipality" is the Municipality of Middlesex Centre.

"Municipal Department" means any categorical division of service delivery or municipal administration of Middlesex Centre which is officially recognized by Middlesex Centre and exercises powers delegated to it by Middlesex Centre, including but not limited to any local board, as defined by the Municipal Act, 2001 as amended or replaced, which exercises powers delegated to it by Middlesex Centre.

"Network" means any computer hardware and/or software that allows computers or other related devices to exchange data.

"Passphrase" is a string of words, traditionally longer than a password, which allows access to a computer system or service.

"Password" is a word or a string of characters which allows access to a computer system or service.

"Personal identification Number (PIN)" is a numerical code which is used to unlock or grant access to a computer system or service.

"Privileged Access Management (System)" is a solution designed to securely store, monitor, and audit privileged credential usage for any device considered to be Core Infrastructure.

"User" means anyone who has an account (username and password) which is used to access the Municipality's Network or Information Systems.

Procedure

1. User Accounts and Passwords

a) All Users are accountable for the acceptable and appropriate use of their assigned user account as outlined in the Acceptable Use of Technology Policy.

b) All Users who have an assigned user account are accountable for the creation and protection of their passwords as outlined in this policy.

2. General Procedures

a) Passwords, passphrases, and personal identification numbers (PIN) shall be stored in a manner which renders them inaccessible by others.

b) Temporary passwords provided by Middlesex County ITS staff shall be changed as soon as possible upon receipt of the temporary password.

c) If a numerical personal identification number (PIN) is used to secure a system or device, the PIN shall not consist of easily guessable combinations (e.g., 0000, 1234, etc.)

d) If a password, passphrase, or PIN is known or suspected to be compromised, it shall be changed immediately.

e) "Remember Password" feature on websites and applications shall not be used.

f) User IDs and Passwords/Passphrases/PINs must not be scripted to enable automatic login on workstations or laptops, except for systems designated as public-access terminals.

g) When configuring password "hints," do not hint at the format of your password (e.g., "postal code + middle name")

h) Passwords must not be inserted into email messages, instant messages, text messages or other related forms of electronic communication.

i) Passwords must not be revealed over the phone to anyone.

j) Do not store your passwords in a file stored on your computer or mobile device. Passwords may be stored in an approved Password Management System (see below).

k) All passwords should be treated as sensitive, confidential information.

l) Users who step away from their computer shall lock or logout of their computer to protect it from unauthorized access or use.

m) Password protected screen-savers will be enabled after no more than 20 minutes of inactivity.

3. Password Protection

a) Passwords or passphrases shall not be shared with anyone (including coworkers and supervisors) and must not be revealed or sent electronically.

b) If a password, passphrase, or PIN must be shared through the course of day-to-day activities, such as granting temporary access of a system or site, it shall be changed once access is no longer required.

c) Passwords shall not be written down or physically stored anywhere in the office.

4. Password Managers

a) Middlesex Centre has approved the utilization of a commercial password management system for staff, which is to be used at all times (e.g., Dashlane).

b) Approved password management systems or solutions may be local or online (cloud) based.

c) An approved/authorized password management system or solution may only be utilized provided its use does not circumvent or negate any policies or procedures outlined in this policy document.

d) The name of such system will be provided by the Director of Corporate Services in collaboration with Middlesex County ITS.

5. Workstations and Laptops

a) All workstations and laptops shall be secured using a password or passphrase consisting of no less than fifteen (15) characters in length.

b) Staff passwords or passphrases utilized for workstation and laptop access shall be unique to the system or service being accessed and not be used for any other purpose.

c) Staff passwords and passphrases used to access Middlesex Centre workstations or laptops do not expire and are only required to be changed if compromised or shared per the General Procedures of this document.

6. Servers, Firewalls, and Core Infrastructure

a) Passwords and passphrases used to access servers, firewalls and other devices defined as Core Infrastructure shall be stored in an approved Privileged Access Management System (PAM) as managed by Middlesex County ITS.

b) Passwords and passphrases stored in an approved PAM shall only be accessible to Middlesex County ITS staff who have been granted access.

c) Passwords and passphrases stored in an approved PAM shall be updated on a regular basis.

7. Mobile Devices

a) Mobile devices shall be secured using a password, PIN, or Biometric Security (or a combination thereof). PINs must be a minimum of 4 characters and shall not follow a sequential format (e.g. 1234, 1111 etc.)

8. Two-Factor Authentication

a) Two-factor authentication (2FA), sometimes referred to as two-step authentication, is a security mechanism where an individual uses two different authentication factors to verify their access to a service, system or information. Two-factor authentication provides a higher level of security than single-factor authentication, which is where the individual only uses one authentication factor, typically a password to access a service, system or information.

b) It is encouraged that wherever practically possible and/or available, individuals implement and leverage two-factor authentication when accessing a sensitive service, system or information.

7. Compliance

Corporate Services and Middlesex County ITS enforce this policy and related standards. Anyone who has reason to suspect a deliberate and / or significant violation of this policy is encouraged to promptly report it to the Middlesex County ITS Service Desk. Policy violations that come to the attention of the ITS Service Desk will be escalated to the Director of ITS and Director of Corporate Services.

Staff in violation of this policy may be subject to disciplinary action up to and including termination.

7.1 Exceptions

Any exception to this policy must be approved by the Director of Corporate Services and the Director of Information Technology Services at the County of Middlesex.

Policy Review

This policy will be reviewed once every four (4) years, or as necessary.