Category: ITS Policy Policy No.: ITS-07-2024 Revisions: February 7, 2024	middlesex centre in the centre of it all	Pages: 5 Effective Date: Feb 7, 2024 Report No.: CPS-06-2024

Information Security Policy

Purpose

The purpose of this policy is to protect system resources against inappropriate or undesired user access and/or data loss.

Scope

This policy applies to Members of Council, all employees of Middlesex Centre including Paid-on-Call Firefighters and volunteers.

Definitions

"(ITS) Asset" means any physical electronic device owned by Middlesex Centre, which may contain or have access to sensitive information such as files and emails or has considerable value and is uniquely identifiable via a serial number or other means.

"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.

“Confidential or Sensitive Information” includes any data which may be damaging should it be exposed to unauthorized individuals, including (but not limited to) credit card numbers, social insurance numbers, personally identifiable information, or personal health information.

"ITS" means Information Technology Services.

"Malware" is catch-all term for software which is designed to disrupt, damage, or gain unauthorized access to a computer system.

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

“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” is a numerical code which is used to unlock or grant access to a computer system or service. Also known as a PIN.

Procedure

1. General Procedures

a) Access to Middlesex Centre’s ITS systems and services shall be controlled via unique user accounts / user IDs.

b) All unique accounts shall be secured with a password or passphrase, or another appropriate security control.

c) Staff shall report security incidents to their supervisor or manager and/or Middlesex County ITS staff upon learning of the incident.

d) Staff shall maintain security by logging out of systems and services when not in use and keeping their passwords or passphrases secure.

e) Hardware and software for use by Middlesex Centre staff shall be provisioned by Middlesex County ITS, or by a Middlesex County ITS authorized third-party. All hardware and software in the care of Middlesex Centre staff shall be always kept secure.

2. User Accounts

a) Unique user accounts will be provided for each Middlesex Centre staff member.

b) User accounts shall not be shared between staff members unless specifically required for the function of the organization, or the provision of a unique account is not possible.

c) User accounts will be protected by means of password or passphrase, PIN, or biometric security (or a combination hereof).

Further information regarding the use of passwords and passphrases can be found in the Middlesex Centre’s User Accounts and Password Policy.

3. Incident Reporting

Staff must promptly report harmful events or policy violations involving Middlesex Centre IT Assets or information to their manager or a member of the Middlesex County ITS team. All data-related incidents or unauthorized access incidents must be reported to the Municipal Clerk. Events include, but are not limited to, the following:

a) Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to Middlesex Centre Information Resources.

b) Data incident: any potential loss, theft, or compromise of Middlesex Centre information.

c) Unauthorized access incident: any potential unauthorized access to a Middlesex Centre Information Resource.

d) Facility security incident: any damage or potentially unauthorized access to a Middlesex Centre owned, leased, or managed facility.

e) Policy violation: any potential violation to this or other Middlesex Centre policies, standards, or procedures.

4. Clean Desk

a) Staff should log off from applications or network services when they are no longer needed.

b) Staff shall log off or lock their workstations and laptops when their workspace is unattended.

c) Staff shall not maintain any confidential information at their physical workspace such as passwords, passphrases, personal identification numbers, or any other sensitive information which could be used to access any Middlesex Centre network or system.

5. Data Security

a) Microsoft 365 OneDrive may be used for sharing, storing, and transferring confidential or internal information. Any other external application must be reviewed and approved by Corporate Services in consultation with Middlesex County ITS.

b) Confidential information requiring physical transport must be transported either by a Middlesex Centre employee or a courier approved by a Middlesex Centre department director.

c) All portable electronic media containing confidential information must be securely disposed. Please contact Middlesex County ITS for guidance or assistance.

d) Confidential or Sensitive Information stored on a shared resource such as a server or cloud computing application shall be secured in a manner which restricts access from unauthorized users (such as folder permissions, passwords, or a combination thereof).

e) When no longer required, Confidential or Sensitive Information shall be security destroyed, unless subject to retention under Middlesex Centre Records Retention By-law.

6. Hardware and Software

a) All hardware must be formally approved by Middlesex County ITS before being connected to Middlesex Centre networks.

b) Software installed on Middlesex Centre provided laptops and workstations must be approved by department director and installed by Middlesex County ITS staff.

c) Staff wishing to take any Middlesex Centre IT Assets off-site may only do-so with the prior approval of their department director.

d) All Middlesex Centre assets taken off-site shall be physically secured at all times.

e) Middlesex Centre assets taken off-site shall not be left visible in a vehicle or stored within unattended luggage. Should an ITS Asset require storage in a vehicle it shall be stored in the trunk or another otherwise inaccessible area and removed from the vehicle as soon as possible.

f) Staff shall not allow family members or other non-employees to access Middlesex Centre assets.

7. Malware Protection Policy

Mitigations are in place to protect against unwanted software (such as Grayware, Malware, Ransomware, and Viruses) and are covered under the Middlesex Centre's Malware Protection Policy.

8. Incident Response and Data Breach

Any malicious (both internal or external, and willful or accidental) incident which may affect Middlesex Centre's Information Systems Assets, including any hardware, databases, software applications, and networked devices, shall be subject to review under the Incident Response Plan (IRP) maintained by Middlesex County ITS on behalf of Middlesex Centre. Any required remedial actions or steps shall be determined by the Incident Response Plan.

Any breach of personal data information must be reported to the Municipal Clerk.

9. 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.

Policy Review

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