Policy: Information Security Policy

Policy Number: CP-A-11.5

Effective Date: October 16, 2023

Revised Date:

PURPOSE:

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

DEFINITIONS:

"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.

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

“Passphrase” is a string of words, traditionally longer than a password, 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)

“Thames Centre” is the Municipality of Thames Centre.

POLICY:

a) Access to Middlesex County ITS systems and services shall be controlled via unique user accounts / user ID's.

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

c) Staff shall report security incidents to Management 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 Thames Centre staff shall be provisioned by Middlesex County ITS, or by a Middlesex County ITS authorised third-party. All hardware and software in the care of Middlesex County staff shall be always kept secured.

PROCEDURE:

1. User Accounts

a) Unique user accounts will be provided for each Thames 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 Thames Centre Password Policy (CP-A-11.3).

2. Incident Reporting

Staff must promptly report harmful events or policy violations involving Middlesex County ITS Assets or information to their manager or a member of the Middlesex County ITS team. 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 County Information Resources.

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

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

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

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

2. Clean Desk

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

b) Staff should 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 Thames Centre network or system.

3. Data Security

a) Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.

b) Confidential information requiring physical transport must be transported either by a Thames Centre employee or a courier approved by Middlesex County ITS or the Thames Centre Clerk’s Department.

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 the current Thames Centre Records Retention By-law.

4. Hardware and Software

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

b) Software installed on Thames Centre-provided laptops and workstations must be approved by Middlesex County Assets and installed by Middlesex County ITS

staff.

c) Staff wishing to take any Thames Centre ITS off-site may only do so with the prior approval of their Department Head.

d) All Thames Centre ITS Assets taken off-site shall be physically secured at all times.

e) Thames Centre ITS 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 Thames Centre ITS Assets.

5. Malware Protection Policy

Mitigations are in place to protect against unwanted software (such as Grayware, Malware, Ransomware, and Viruses) and are covered under the Thames Centre Malware Protection Policy (CP-A-11.6)

6. Incident Response and Data Breach

Any malicious (both internal or external, and willful or accidental) incident which may affect Thames Centre 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 which also applies to Thames Centre. Any required remedial actions or steps shall be determined by the Incident Response Plan.

7. Compliance

Thames Centre, along with Middlesex County ITS, enforces this Policy and the related standards at all times. Anyone who has reason to suspect a deliberate and/or significant violation of this Policy is encouraged to promptly report it to their Department Head, CAO, and 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.

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