Policy: IT Access Control Policy

Policy Number: CP-A-11.8

Effective Date: October 16, 2023

Revised Date:

PURPOSE:

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

DEFINITIONS:

“Administrator Account(s)” are any user ID’s which can access Endpoints, Servers and Network Devices at a functional level which permits the user to perform tasks such as configuration and user account changes, reset passwords, system modification, and application installation.

“Corporate Information” is any information, files, or communications which could be considered sensitive, privileged, or confidential, stored within ITS Assets owned by Thames Centre.

"Endpoint" any device which connects to a computer network, such as a server, workstation, or laptop.

"ITS" means Information Technology Services.

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

“Network Device(s)” are physical devices capable of connecting multiple devices together on a wired or wireless network.

“Thames Centre” is the Municipality of Thames Centre.

“Virtual Private Network (VPN)” is a method in which an approved staff member can securely access Corporate Information from a remote location, using approved software, hardware, or a combination thereof.

"Workstation" A desktop computer used by one or more individuals for the purposes of conducting day-to-day business or providing a service.

POLICY:

All systems capable of accessing, storing, or modifying corporate data shall be configured in a manner which renders them inaccessible to unauthorized individuals, as defined in the Procedures section of this policy.

Users or resources shall be granted access to systems or services with the minimum privileges necessary to fulfil their roles and responsibilities.

All systems and services provided by or managed through Middlesex County ITS shall be subject to review under this policy to ensure they are compliant with the Procedures in this policy.

PROCEDURE:

1. Access Control Requirements

All users must use a unique user ID to access Thames Centre systems and applications, defined in the Thames Centre Information Security Policy (CP-A-11.5). This user ID shall be secured with a password or passphrase as defined in the Thames Centre Password Policy (CP-A-11.3). Alternative authentication mechanisms which do not rely on a unique ID and password may be formally approved by the Director of ITS.

2. Administrator Accounts

Administrator accounts shall only be granted to Thames Centre staff who require such access to perform their job function. Administrator accounts shall be strictly controlled, and their use shall be logged and reviewed as required.

Thames Centre staff with administrator access shall only access sensitive data if required in the performance of a specific task.

Thames Centre staff with administrator access shall also have an unprivileged account, which shall be used for all purposes not requiring administrator access, including but not limited to electronic mail.

3. Vendor & Contractor Remote Access

Where required, contractors and vendors may be granted remote access to Thames Centre resources for the purposes of providing setup, configuration, and support. To facilitate this access, Middlesex County ITS should be contacted as soon as possible upon learning of such a request.

Middlesex County ITS shall:

a) Provide access to the system or resource using approved remote support software

b) Monitor remote access while the vendor or contractor performs their work

c) Provide temporary user accounts and passwords where required for a vendor or contractor

d) Terminate/remove temporary user accounts once the vendor or contractor has completed their work

Vendors or Contractors shall not be granted unattended remote access to any corporate connected system or service without written approval of the Middlesex County Director of Information Systems or Manager of IT Infrastructure and Technical Services.

4. Account Termination

Middlesex County ITS shall be notified if a staff member has left the organization or has provided notice to leave the organization.

Upon the staff member's departure, Middlesex County ITS shall:

a) Disable access to the Thames Centre network, systems, and server(s) by resetting the user account password and disabling the account.

b) Disable access to online services and portals such as email web-access or mapping websites by resetting the user account password and disabling the account or deleting the account for these services. Any licenses associated with these services will be unassigned from these accounts during this process.

c) Disable remote VPN access for the user account.

d) Redirect inbound email to an alternate destination as requested by the staff member's Department Head or Manager.

e) Provide access to the departed staff members files and emails to alternate staff as requested by the staff member's department head.

After a period of thirty (30) days has lapsed, any access to the departed staff member's account should be reviewed by Middlesex County ITS staff, along with the Thames Centre staff member's Department Head/Manager and/or CAO. to determine if this access is still required.

Should this access no longer be required, the departed staff member's account(s) shall be archived and removed from the system(s).

5. Account Termination Exceptions

If a departure is pre-scheduled (notice given, or a permanent full-time contract is transitioned into a temporary contract), the staff member's account may remain active and operational for a period of time as determined by the Thames Centre staff member's Department Head/Manager and/or CAO. Once the staff member's departure has been finalized, the staff member's account shall be disabled per this policy.

6. Additional or Modified Permissions

Middlesex County ITS shall be notified by a Thames Centre Department Head/Manager if a staff member requires additional or modified permissions to perform a task or as part of their job role. Staff may request additional or modified permissions directly with Middlesex County ITS, should their job duties require these additional or modified permissions. All additional or modified permission requests shall be subject to approval of the Thames Centre staff member's Department Head/Manager and/or CAO.

Upon approval, Middlesex County ITS staff will make the appropriate additions or modifications and confirm their operation with the Thames Centre staff member.

Additional or modified permissions which have the potential to cause harm to the security or integrity of the Middlesex County Network or related infrastructure, shall be subject to a security review and risk assessment prior to being provisioned by Middlesex County ITS.

7. Auditing and Logging

a) User account names and actions performed may be automatically recorded using audit logging capabilities of the system(s) or server(s) accessed. Where possible these logs shall be automatically exported to a Middlesex County ITS logging server for backup purposes. See the Thames Centre Electronic Monitoring Policy (CP-A-5.6) for further information.

b) Any access request changes and approvals shall be logged by Middlesex County ITS staff, including the nature of the request, the requester's name, date of the request, and all approval(s) obtained.

8. Data Centre Access

a) Only authorized personnel shall be given access to secure areas at Thames Centre's premises and any third-party premises where sensitive information is processed or maintained, or physical assets are held.

b) All access to areas hosting systems that store, process, or transmit sensitive data (e.g. server rooms) shall have physical access controls, monitored by cameras, and access shall be logged.

Staff shall challenge and/or report any visitors found unsupervised or acting suspiciously at any site where sensitive Thames Centre data is processed or maintained.

9. 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.