Meeting Date: **February 7, 2024**

Prepared By: **Tiffany Farrell, Director of Corporate Services, and Heather Kepran, Manager of Strategic Communications**

Report No: **CPS-06-2024**

Subject: **Information Technology Policies**

Recommendation:

THAT Report CPS-06-2024 re: Information Technology Policies be received;

AND THAT Council endorse the updated policies attached as Appendices A1–A7;

AND FURTHER THAT Council endorse the new policies attached as Appendices A8–A11.

Purpose:

The purpose of this report is to seek Council's endorsement of the new and updated information technology (IT) policies for the municipality.

Background:

Middlesex Centre uses corporate IT policies to provide overall direction and guidance to the organization relating to the proper, acceptable, and secure use of technology and information systems.

In 2022, Council adopted the municipality's Information Technology (IT) Master Plan. The IT Master Plan outlines many recommendations, one being to update the current IT policies and to add new IT policies. In addition, these policies should now be reviewed on a four-year cycle.

Middlesex Centre has been working with the Director of Information Technology Services at the County of Middlesex to update our existing four policies and develop four new policies for the municipality's adoption.

The municipality’s existing IT policies are:

- Acceptable Use of Technology Policy
- Cellphone and Mobile Device Policy
- User Accounts and Passwords Policy
- Information System Disaster Recovery and Business Continuity Policy

The municipality’s proposed new IT policies are:

- Wireless Access Policy
- Information Security Policy
- Malware Protection Policy
- Information Technology Access Control Policy

Additionally, as presented to Council on November 1, 2023, the municipality undertook a full human resources policy review in 2023. Staff engaged consultants at HRdowloads to review and update all human resources policies. Three of the policies included in that review had aspects relating to information technology. Due to this, the following three policies were included in this group of policy revisions. These policies are:

- Social Media Policy
- Electronic Monitoring Policy
- Right to Disconnect Policy

Analysis:

As recommended as part of our IT Master Plan in 2022, staff began the process of updating out IT policies in 2023, working collaboratively with the County of Middlesex Information Technology department.

Once the draft policies were created, the municipality created an IT policy working group to review, discuss and finalize the policies for Council adoption. The working group included the CAO, senior management team and a selection of the managers in the organization.

As noted above, the municipality is recommending approval of eleven policies. Each of these eleven policies will be discussed below.

In addition to these eleven policies, there are three policies that have been adopted at the County of Middlesex that cover Middlesex Centre owing to our agreement with the County for the provision of IT services. These three policies are:

- Back-up Policy
- Patch Management Policy
- Secure Configuration Policy

Middlesex Centre will maintain copies of these policies, however they will not be adopted by the municipality separately from the County of Middlesex.

For all policies the following was amended:

- Policy review date added to all policies
- Updated to a standard template
- Employee titles updated
- Standard policy naming and numbering conventions applied
- Update to departments instead of position when possible
- Removal of acknowledgment of policy within the policy, except for the required Security Officer acknowledgment in the Information System Disaster Recovery and Business Continuity Policy
- Added compliance section

Social Media Policy

This policy is put into place to identify responsibilities and standards for the establishment and administration of corporate social media sites.

This policy provides rules on the acceptable participation in social networks by Members of Council and municipal employees. This policy is to be read in conjunction with the Middlesex Centre Employee Code of Conduct, Council Code of Conduct, Acceptable Use of Technology, R-Zone, and Respect in the Workplace policies.
This policy serves to provide direction to those managing and administering corporate social media sites, protect the municipality's reputation, provide employees and Members of Council with clear usage guidelines, and provide protocol around monitoring, administration, acceptable use and privacy.

This policy applies to Members of Council, all employees of Middlesex Centre including paid-on-call firefighters. This policy applies to usage during and outside work hours. Changes made were minor administrative updates.

Right to Disconnect Policy

The Municipality of Middlesex Centre understands that due to work-related pressures, the current landscape of work, or an employee's work environment or location, employees may feel obligated or choose to continue to perform their job duties outside their normal working hours. Work-related pressure and the inability to disconnect from the job can lead to stress and deterioration of mental health and overall well-being. This policy has been established to support employee wellness, minimize excessive sources of stress, and ensure that employees have the right to disconnect from work outside their regularly scheduled hours.

Under the Employment Standards Act, 2000, a written Right to Disconnect Policy is required for employers that employ 25 or more employees.
This policy applies to all employees of the Municipality of Middlesex Centre.
This policy was recently adopted in 2022 by the municipality. Only minor administrative updates were completed.

Electronic Monitoring Policy

Middlesex Centre values trust, discretion, and transparency and believes employees deserve to know when and how their work is being monitored. This policy is to be used in addition to other Middlesex Centre policies, including but not limited to the Acceptable Use of Technology Policy, the Video Surveillance Policy and the Cellphone and Mobile Device Policy. It is intended to establish guidelines for company practices and procedures related to electronic monitoring of employees.

Electronic monitoring is an essential part of ensuring compliance with Municipal policies, maintaining a respectful workplace environment, and ensuring ITS assets that are owned and managed by the municipality are used safely and appropriately. By monitoring municipal assets, the municipality is protecting its employees from liability and/or performance challenges caused by the improper or unauthorized use of the systems made available to facilitate the business of the municipality.

This policy applies to all employees of the Municipality of Middlesex Centre including paid-on-call firefighters. Aspects of the policy also apply to the municipality’s Information Technology Services (ITS) provider, Middlesex County ITS.

This policy also applies to consultants, contractors, volunteers and any other individual who may use the municipality’s electronic resources.

This policy was recently adopted by the municipality due to legislative requirements. Only minor administrative updates were completed and a new appendix to log and tracking was created.

Cellphone and Mobile Device Policy

The purpose of the Cellphone and Mobile Device Policy is to provide direction, terms, conditions and procedures for department directors and staff who use a corporate issued mobile device or a personally owned mobile device for the purposes of conducting Middlesex Centre business, and to ensure the protection of personal information, confidential information and any other information in the custody and control of Middlesex Centre while being transmitted and/or stored on mobile devices.

This policy applies to all authorized persons who may conduct Middlesex Centre business using a mobile device.

This policy contains multiple updates. Some of the more notable changes include:

a) Assigning detailed roles and responsibilities to specific departments and positions.

b) For staff using a personally owned mobile device:

    a. Approval of department director and Director of Corporate Services must be obtained before use.

b. Personally owned mobile devices must be no more than four generations old, and still receive regular security updates and support from the device manufacturer or vendor.

c. Staff are responsible for ensuring their personally owned mobile device is kept up to date with current operating system patches and updates.

d. Staff are responsible for any recurring service plans, warranty or maintenance fees, and any over-usage fees for the device; there will be no pre-arranged reimbursement agreements for the usage of the device.

e. Middlesex County ITS will remove access to any corporate data upon completion of employment or during mobile device upgrades.

f. Any cost associated with acquiring and maintaining a personally owned mobile device, including any charges or monthly fees incurred while using the device, is the sole responsibility of the authorized person.

c) Any information on a mobile device which is accessible by the mobile device management software may be subject to monitoring as defined in Middlesex Centre's Electronic Monitoring policy.

User Accounts and Password Policy

Passwords are an important aspect of computer security. A poorly chosen password or a password that 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.

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.

This policy contains multiple updates. Some of the more notable changes include:

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

b) 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.

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

Information System Disaster Recovery and Business Continuity

The purpose of this policy is to establish processes to ensure the availability of all information systems required for essential business operations in the event of an equipment failure, service disruption, or a loss of operational capacity resulting from a fire, natural disaster, or other emergency.

This policy addresses business continuity for information systems and recovery of information systems.

This policy applies to Members of Council, all employees of Middlesex Centre including paid-on-call firefighters and volunteers. It applies to all IT assets of the municipality.

Changes made were minor administrative

Acceptable Use of Technology Policy

To conduct business, Middlesex Centre provides access to technology in the form of hardware (such as laptops, workstations, and portable devices) and software (such as productivity tools). The purpose of this policy is to outline Middlesex Centre's expectations regarding the acceptable use of technology when using networks, email, internet, and all other technology and information systems.

All staff of Middlesex Centre have access to Middlesex Centre's network and its services ("Information Systems") provided it is for business purposes. occasional use of information systems for personal activities is allowed so long as it does not interfere with the security of the network, their productivity, or the productivity of other users of the network.

Middlesex Centre staff shall use technology in a manner that supports the organization, maintains the confidentiality of protected information, and ensures the integrity of all systems, servers, and networks of Middlesex Centre.

This policy applies to Members of Council, all employees of Middlesex Centre including paid-on-call firefighters and volunteers.

This policy contains multiple updates. Some of the more notable changes include:

a) Staff shall not use TikTok on any municipally-owned device.

b) Staff must take care when using artificial intelligence (AI) software (e.g., ChatGPT, among others) to ensure confidential or sensitive information is not put into unsecure systems. Further, staff must review any outputs from AI software to ensure accuracy and truthfulness.

Wireless Access Policy

This is a new policy for the municipality.

The purpose of this policy is to outline the secure and appropriate use and configuration of wireless networks (e.g., Wi-Fi in public spaces, among others).

This policy applies to Members of Council, all employees of Middlesex Centre including paid-on-call firefighters and volunteers.

Information Security Policy

This is a new policy for the municipality.

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

This policy applies to Members of Council, all employees of Middlesex Centre including paid-on-call firefighters and volunteers.

Malware Protection Policy

This is a new policy for the municipality.

The purpose of this policy is to outline the implementation and configuration of endpoint protection tools, user security awareness, early detection and mitigation security systems and ensure staff are aware of security policies in place on their IT assets.

This policy applies to Members of Council, all employees of Middlesex Centre including paid-on-call firefighters and volunteers.

Information Technology Access Control Policy

This is a new policy for the municipality.

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

This policy applies to Members of Council, all employees of Middlesex Centre including paid-on-call firefighters and volunteers.

Financial Implications:

None.

Strategic Plan:

This matter aligns with following strategic priorities:

- Responsive Municipal Government

This report aligns with maintaining accountability through compliance with legislative changes and requirements.

Attachments:

A1 – CPS-06-2024 Social Media Policy

A2 – HRS-05-2024 Right to Disconnect Policy

A3 – HRS-15-2024 Electronic Monitoring Policy

A4 – ITS-02-2024 Cellphone and Mobile Device Policy

A5 – ITS-03-2024 User Accounts and Passwords Policy

A6 – ITS-04-2024 Information System Disaster Recovery and Business Continuity Policy

A7 – ITS-05-2024 Acceptable Use of Technology

A8 – ITS-06-2024 Wireless Access Policy

A9 – ITS-07-2024 Information Security Policy

A10 – ITS-08-2024 Malware Protection Policy

A11 – ITS-09-2024 Information Technology Access Control Policy