Committee of the Whole

Meeting Date: **February 14, 2023**

Submitted by: **Chris Bailey, Director of Information Technology Services and Greg Marles, Manager of IT Infrastructure and Technical Services**

Subject: **Information Technology Services - Policy Updates**

BACKGROUND:

Middlesex County Information Technology Services (ITS) uses policies to maintain the security and integrity of County information technology infrastructure, and ensure ITS assets are used safely and appropriately.

The Middlesex ITS Strategic Plan includes recommendations for enhancements to IT governance. These enhancements incorporate reviewing and refreshing existing ITS policies and procedures and developing new ones.

Initially, four ITS policies have been reviewed and updated to better align with industry standards and best practices.

These policies include:

- ITS Asset Management Policy (IT Policy 1.01)
- Acceptable Use of Technology Policy (IT Policy 2.01)
- Cellphone and Mobile Device Policy (IT Policy 5.01)
- Password Policy (IT Policy 7.01)

The ITS department continues to work through the Strategic Plan recommendations, including developing and implementing new policies and procedures to strengthen our cyber security program and provide guidance to staff on the appropriate and safe use of technology.

ANALYSIS:

The following four policies were reviewed and updated to better align with industry standards and best practices. Significant updates to these policies have been outlined below.

IT Policy 1.01 – ITS Asset Management Policy

- Formerly called "Network Equipment" – has been renamed to ITS Asset Management as it properly describes the nature of the policy
- The new policy covers updated purchasing, reporting and lifecycle guidelines for equipment procured through Middlesex County ITS
- Language updates which better align with structural changes in the Middlesex County ITS department

IT Policy 2.01 – Acceptable Use of Technology

- Updated to include reference to the Electronic Monitoring Policy (HR Policy 1.17).
- Includes new language related to moving/reassigning technology, and reporting obligations if a device is lost/damaged or stolen

IT Policy 5.01 – Cellphone and Mobile Device Policy

- Updated to better define the obligations regarding Corporate devices versus Bring-Your-Own (BYOD) devices
- Includes new language to better describe Mobile Device Management and its impact on Cellphones and Mobile devices
- Includes updated language surrounding corporate data vs personal data
- Updated to include reference to the Electronic Monitoring Policy (HR Policy 1.17).

IT Policy 7.01 – Password Policy

- Formerly called "User Accounts and Passwords" – has been renamed to Password Policy as it better captures the intent of the policy
- Updates previous password standards to align them with current best practices
- Includes language regarding Password Managers
- Introduces the use of a Privileged Access Management (PAM) system

RECOMMENDATION:

THAT ITS Asset Management Policy (IT Policy 1.01), Acceptable Use of Technology Policy (IT Policy 2.01), Cellphone and Mobile Device Policy (IT Policy 5.01) and Password Policy (IT Policy 7.01) revisions be approved, and that the Corporate Administrative Policy and Procedure Manual be updated.

Attachments:

1. 1.01 - ITS Asset Management Policy (DRAFT)
2. 2.01 - Acceptable Use of Technology Policy (DRAFT)
3. 5.01 - Cellphone and Mobile Device Policy (DRAFT)
4. 7.01 - Password Policy (DRAFT)