POLICY No. (2023-03)

Digital Account Cybersecurity

Originating Department	Innovation & Technology Services		
SMT Approval:	2023-12-14		
Council in Committee:	N/A	**Recommendation #:**	N/A
Council Approval:	N/A	**Resolution #:**	N/A
Revision History:	Click here for revision history		

1. Purpose

This policy seeks to outline Haldimand County's approach to cybersecurity as it relates to digital accounts in alignment with Council Priorities.

2. Scope

This policy has been developed as a component of the Corporate Information Security strategy to ensure cybersecurity is a critical component of Haldimand County's holistic approach to promoting healthy and safe communities and managing risk. This policy applies to all Members of Council, Members of all Boards and Committees, Volunteer Firefighters, and all Employees of Haldimand County including full-time, part-time, casual, unionized, non-unionized, and Library staff.

This policy applies to all Haldimand County information technology assets including computer workstations, laptops, servers, phones, tablets, and Internet of Things (IoT) devices.

This policy supersedes subsection 2.2.3 *User Identification and Passwords* of the *Information-Technology-Security-Policy-2010-03*

3. Definitions

3.1 **Application** refers to a computer program designed for a specific task or use.

3.2 **Desktop** refers to a computing device designed to operate at a single location without ease of relocation of the device.

3.3 **Laptop** refers to a portable computing device which includes a screen and is designed to be operated in multiple locations. This category also includes netbooks, tablets, and Ultrabooks.

3.4 **Multi-factor Authentication (MFA):** Use of two or more factors to validate the identity of a user.

3.5 **Server:** a computing device capable of accepting requests from a client and giving responses accordingly.

4. Legislative Authority

This policy is in alignment with the recommendations put forth by the Canadian Centre for Cyber Security (the Cyber Centre) and the Government of Canada's "*Government in a digital age*" initiatives.

5. Policy Administration

All information technology assets must, at minimum, adhere to the following standards to ensure security and minimize chance of system breach:

- All systems must remain on a supported and recently patched version of their operating system;
- All systems must be protected by anti-virus software, and anti-virus software must be kept up to date;
- All systems must be protected by a user account and password (alphanumerical, token-based, or biometric);
- User accounts, with limited exceptions made for Innovation & Technology Services service accounts, must be named to a single individual and must have a password set;
  - These passwords must not be shared or disclosed to anyone including Innovation & Technology Services staff or other members of County staff;
  - User account passwords must contain at least 16 characters;
  - User account passwords must not contain common phrases such as "password", "123456", "qwerty", "hockey", or "testing".
- User accounts, with limited exceptions made for Innovation & Technology Services service accounts, must use a multi-factor authentication (MFA) type in addition to a password. These may include;
  - MFA Authentication Application;
  - SMS text message;
  - Phone call.

6. Policy Communication

This policy will initially be communicated to all staff, via email from their respective member of the Senior Leadership team. Future communications to new employees will be via the established Human Resources on-boarding processes.

This policy will be posted to the intranet and on the public website.

Upon adoption of this Policy all users out of compliance will be required to comply based on the tenets set out in this Policy.

Innovation & Technology Services will audit user compliance to this Policy and report breaches to the Information Technology Governance Committee.

7. Reference

This policy should be read alongside the Information Technology Acceptable Usage Policy, applicable collective agreements or policies governing non-union employees, various health and safety policies and guidelines, relevant and applicable legislation, and any other policy that may become applicable and/or relevant.

Revision History	
SMT Revision Date	Details