Hanover
Ontario, Canada

Policy and Procedure Manual

SECTION: Administration	**POLICY #: ADM-014**
Date Approved: August 21, 2017	Network System Passwords
Revision Date:	**Review Date:**
Authority: Report DCS-16-17	

PURPOSE

Passwords are a very important aspect of computer security. A poorly designed password or a password that is not effectively protected may result in unauthorized access to the Town of Hanover's confidential information. The purpose of this policy is to establish a standard for strong passwords, the protection of those passwords and the frequency of change of passwords. This policy outlines the responsibility of the account holder to create and protect a password that meets security best practices in an effort to prevent unauthorized access to the network or information systems.

SCOPE

This policy applies to all Town of Hanover or other personnel who have, or are responsible for, an account or any device that provides access of any part of the municipality's network, including council members. The user, to whom a unique account or access to the municipality's network has been assigned, is responsible for the creation, protection and maintenance of their passwords. It is imperative that this policy is followed by anyone who has access to confidential information or information that is protected through privacy legislation.

POLICY

1. All system users must utilize a password that conforms to the Password Creation Guidelines below.

2. Users must not use the same password for company network access that they use for other non-company account access.

3. When possible, users must not use a common password for access to multiple company related accounts. Other town internal information system passwords must be different than the network access password and should comply within the password rules as set for each town internal information system component (e.g. Keystone, Activenet, Insync) as some of these components passwords are limited to the number of characters available.

4. All network system passwords will expire within 365 days of creation. Users can change passwords as frequently as they wish with a minimum one day lifespan, but the maximum life span of a password on the network system will be 365 days. Users will be notified 10 days in advance of password expiration on the network system. This update is required for ALL network system devices (computer, iphone or blackberry, ipad, etc.).

5. Network system passwords will have a lockout threshold allowing for up to 10 failed attempts within 30 minutes before the account will be locked out.

Definitions

"Information Systems" means any computer hardware and/or software system that people and organizations use to collect, filter, process, create, and distribute data.

"Network" means any computer hardware and/or software that allows computers or other related devices to exchange data.

"User" means anyone who has an account (username and password) which is used to access the Town of Hanover's Network or Information Systems.

Password Protection

- Passwords must not be shared with others, including employees of the company. They are considered confidential business information.
- Passwords shall not be inserted into email messages, instant messages, text messages or other related forms of electronic communication.
- Passwords shall not be relayed over the phone to anyone.
- Passwords must not be written down or stored on a computer file or mobile device unless the file is encrypted.
- Do not use the "remember password" options provided by software applications.
- Report any occurrence to Corporate Services when there is a suspicion that a password has been compromised as soon as that suspicion is realized.
- Users who step away from their computer shall lock or logout of their computer to protect it from unauthorized access or use.
- All passwords should be treated as sensitive, confidential information.

Password Creation Guidelines

All users shall be aware of how to create **strong** passwords. Strong passwords have the following characteristics:

- Contain at least three of the four following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Special characters such as @#$%^&*()!

- Contain at least 12 alphanumeric characters

Weak passwords have the following characteristics:

- Contain less than 12 alphanumeric characters
- Contains a common usage word such as:
  - Name of family member, pet, friend, co-worker or fantasy character
  - Computer or device name, command, hardware, software
  - The company's name or any abbreviation of it
  - Birthdays of users, family members, pets or co-workers
  - Word or number patterns such as "aabb", 1234,
  - Any of the above spelled backwards

Policy Compliance

An employee found to have violated the policy by allowing access to any confidential information or any information that is protected by privacy legislation may be subject to disciplinary action, up to and including termination of employment.