POLICY NO. XX
CYBERSECURITY POLICY

1.0 PURPOSE

1.1 The purpose of the policy is to provide guidelines and provisions for preserving the security of the Municipality's data and technology infrastructure.

2.0 SCOPE

2.1 This policy applies to all employees, elected officials, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

3.0 CONFIDENTIAL DATA

3.1 Confidential data is secret and valuable. Common examples are:

3.1.1 Unpublished financial information
3.1.2 Data of taxpayers or residents/partners/vendors

3.2 All users are obliged to protect this data. In this policy, we will give users instructions on how to avoid security breaches.

4.0 PERSONAL AND MUNICIPAL DEVICES

4.1 Users must keep both their personal and municipally issued device secure. They can do this if they:

4.1.1 Keep all devices password protected.
4.1.2 Choose and upgrade a complete antivirus software.
4.1.3 Ensure they do not leave their devices exposed or unattended.
4.1.4 Install security updates of browsers and systems monthly or as soon as updates are available.
4.1.5 Log into municipal accounts and systems through secure and private networks only.

4.2 Users should also avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

5.0 EMAILS

5.1 Emails often host scams and malicious software (e.g. worms). To avoid virus infection or data theft, users should:

- **5.1.1** Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- **5.1.2** Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- **5.1.3** Check email and names of people they received a message from to ensure they are legitimate.
- **5.1.4** Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

6.0 PASSWORDS

6.1 Passwords must be secure and should remain secret. Users should:

- **6.1.1** Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- **6.1.2** Remember passwords instead of writing them down. If users need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- **6.1.3** Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, users should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- **6.1.4** Change their passwords every two months.

6.2 Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Users are obliged to create a secure password for the tool itself, following the abovementioned advice.

7.0 SECURE DATA TRANSFERRING

7.1 Transferring data introduces risk. Users must:

- **7.1.1** Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary.
- **7.1.2** Share confidential data over the municipality's network/ system and not over public Wi-Fi or private connection.
- **7.1.3** Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- **7.1.4** Report scams, privacy breaches and hacking attempts

7.2 Users should report perceived attacks, suspicious emails or phishing attempts as

soon as possible to their supervisor or direct contact. Our network administrator must investigate promptly, resolve the issue and send an alert when necessary.

8.0 ADDITIONAL MEASURES

8.1 To reduce the likelihood of security breaches, we also instruct users to:

- **8.1.1** Turn off their screens and lock their devices when leaving their desks or personal space.
- **8.1.2** Report stolen or damaged equipment as soon as possible to their supervisor or direct contact.
- **8.1.3** Change all account passwords at once when a device is stolen.
- **8.1.4** Report a perceived threat or possible security weakness in municipal systems.
- **8.1.5** Refrain from downloading suspicious, unauthorized or illegal software on their municipal equipment.
- **8.1.6** Avoid accessing suspicious websites.

9.0 REMOTE EMPLOYEES

9.1 It is imperative that remote users follow this policy's instructions. Since they could access municipal accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secured by password.

10.0 DISCIPLINARY ACTION

10.1 All users should always follow this policy and those who cause security breaches may face disciplinary action:

- **10.1.1** First-time, unintentional, small-scale security breach may result in a verbal warning and training on security.
- **10.1.2** Intentional, repeated, or large-scale breaches (which cause severe financial or other damage) will result in more severe disciplinary action up to and including termination.
- **10.1.3** Each incident will be investigated on a case-by-case basis.
- **10.1.4** Users who are observed to disregard security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.