Title: Cyber Security

Policy No: 1031

Effective Date: March 23, 2021

Motion Number: 21.03.132

Supersedes Policy No:

Review Date: March 23, 2024

Purpose: The purpose of this policy is to detect, describe and educate users about cyber security in order to prevent cyber-attacks and maximize Greenview's online security. The cyber security policy of Greenview outlines guidelines to protect data and technology infrastructure against human errors, hacker attacks and system malfunctions.

1. DEFINITIONS

1.1. **CAO** means the Chief Administrative Officer.

1.2. **Corporate Technology** means any computer hardware or software, network service, and any electronic or digital device supported by the Information Systems, including (but not limited to): laptops, desktops, VoIP, smartphones, etc.

1.3. **Cybersecurity** means the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

1.4. **Common Threats** means Phishing, Pharming, Spoofing, Botnets, Distributed denial-of-service, Hacking, Malware, Ransomware, Spam, Spyware, Trojan Horses, Viruses, Wi-Fi Eavesdropping, Worms.

1.5. **Greenview** means the Municipal District of Greenview No. 16.

1.6. **IS** means Information Systems.

1.7. **IT** means Information Technology.

1.8. **Users** means all individuals authorized by Greenview to use Greenview's corporate technology, which includes access to the Internet.

2. POLICY

2.1. Guiding Principles:

A) Cyber Security is everyone's responsibility.
B) Cyber Security is a process, not a product.
C) Cyber Security requires a multi-layered defence strategy.

2.2. The Internet has become an essential part of everyday life, but it is also a breeding ground for criminal activity, where corporate technology can be monitored and information compromised. Corporate technology is frequently used in critical operations to collect and store sensitive and personal information.

2.3. Greenview corporate technology users must be aware of common threats, risks, and implement IT procedures. The IS Department will maintain cyber security to the best of their ability; however, it is every user's responsibility to maintain and maximize cyber security.

3. PROCEDURE

3.1. Corporate devices that access Greenview email are automatically configured to require passwords.

3.2. Corporate user account passwords expire every ninety (90) days.

3.3. Workstations will lock and logout after thirty (30) minutes of inactivity.

3.4. Meeting room workstations will lock themselves after sixty (60) minutes of inactivity.

3.5. The IS Department may change an employee's password (with proper notification) to perform system maintenance and support.

4. EMPLOYEE AND COUNCILLOR RESPONSIBILITIES

4.1. Be aware of and adhere to this policy.

4.2. Reset passwords when prompted.

4.3. Report any activity to the IS Department that seems suspicious, such as spam emails.

4.4. Ensure the off-site physical security of Greenview issued technology.

4.5. Promptly report the loss or theft of corporate devices, or personal devices configured to access Greenview's email, to a Supervisor or manager, or in the case of a Council Member, to the CAO.

4.6. Do not share passwords with anyone for any reason. Any request for an employee password should be reported to the IS Department or the contracted support team.

4.7. Do not write passwords in a place that is easy to find.

4.8. Do not apply any unauthorized applications, functionality, or components to corporate technology.

4.9. Do not tamper with corporate technology, such as modifying the operating system or installing software to circumvent security controls.

4.10. Do not use compromised technology to connect to the corporate network or information systems.

4.11. Do not connect personal devices or network equipment to the wired network.

4.12. Do not use unfamiliar storage devices, click on links or open attachments from unfamiliar emails, as these activities may result in Viruses or other digital threats.

4.13. Lock corporate devises when leaving equipment unattended for any period.

4.14. Corporate devices must be restarted or logged off versus shutdown to enable IS to provide remote support and maintenance.

4.15. Corporate information must be stored on the network storage options provided to employees, and not locally on any device.

5. MANAGER AND DIRECTOR RESPONSIBILITIES

5.1. Ensure employees are aware of their responsibilities to manage cyber security.

6. IS DEPARTMENT RESPONSIBILITIES

6.1. Protect the corporate environment from abuse and security breaches to maintain the safety, effectiveness, stability, as well as the confidentiality of Greenview's information.

6.2. Develop corporate technology security and put protocols and procedures in place to protect the IT environment.

6.3. Secure, manage and monitor Greenview technology infrastructure to guard against inappropriate use, system intrusion or failure.

6.4. Approve, document, and maintain any exception to this policy.