POLICY

Title: CYBER SECURITY POLICY

Policy No: 1031

Effective Date: June 10, 2019

Motion Number: 19.06.446

Supersedes Policy No: (None)

Review Date: June 10, 2022

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.

DEFINITIONS

IS means Information Systems.

IT means Information Technology.

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.

Cybersecurity is 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.

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

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

Guiding Principles:

1. Cyber Security is everyone's responsibility.
2. Cyber Security is a process, not a product.
3. Cyber Security requires a multi-layered defence strategy.

POLICY STATEMENT

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

PROCEDURES

1. Corporate and personal devices configured to access Greenview email are automatically configured to require passwords.

2. Corporate user account password expires every year.

3. Workstations will lock and logout after 30 minutes of inactivity.

4. Meeting room workstations will lock themselves after 60 minutes of inactivity.

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

RESPONSIBILITIES

6. **Employees and Council Members**
   - 6.1. Be aware of and adhere to the cyber security policy.
   - 6.2. Reset your passwords when prompted.
   - 6.3. Report any activity to the IS Officer or delegate that seems suspicious, such as spam emails.
   - 6.4. Ensure the off-site physical security of Greenview issued technology.
   - 6.5. Promptly report the loss or theft of corporate devices, or personal devices configured to access Greenview's email.
   - 6.6. Do not share your password with anyone for any reason. Any request for your password should be reported to the IT Officer or delegate.
   - 6.7. Do not write passwords in a place that is easy to find.
   - 6.8. Do not apply any IS unauthorized applications, functionality, or components to corporate technology.
   - 6.9. Do not tamper with corporate technology, such as modifying the operating system or installing software to circumvent security controls.
   - 6.10. Do not use compromised technology to connect to the corporate network or information systems.
   - 6.11. Do not connect personal devices or network equipment to the wired network.
   - 6.12. 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.
   - 6.13. Lock corporate devices (CTR-Alt-Delete) when leaving equipment unattended for any period.
   - 6.14. Corporate devices must be restarted or logged off versus shutdown to enable IS to provide remote support and maintenance.
   - 6.15. Corporate information must be stored on the network storage options provided to employees, and not locally on any device.

7. **Department Managers**
   - 7.1. Ensure all employees are aware of their responsibilities to manage cyber security.

8. **Information Systems Officer:**
   8.1. Protect the corporate environment from abuse and security breaches to maintain the safety, effectiveness, stability, as well as the confidentiality of Greenview's information.
   8.2. Develop corporate technology security and put protocols and procedures in place to protect the IT environment.
   8.3. Secure, manage and monitor Greenview technology infrastructure to guard against inappropriate use, system intrusion or failure.
   8.4. Approve, document, and maintain any exception to this policy.