CYBER SECURITY POLICY

GEM Enviro Management Ltd.

CYBER SECURITY POLICY

Document Name	Cyber Security Policy
Organization	GEM Enviro Management Ltd.
Last Updated on	1st December, 2023
Version approved by	Mr. Sachin Sharma
Effective Date	1st April, 2022

Introduction

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize GEM's business and reputation. Our 'Cyber Security Policy' outlines the guidelines and provisions for preserving the security of our data and technology infrastructure.

We have implemented several security measures to guard against possible data-security threats. We have also prepared instructions to mitigate security risks. The provisions in this policy have been outlined below.

1. Scope

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

2. Definitions

- **"Organization"** means "GEM Enviro Management Ltd."
- **"Policy"** shall mean this "Cyber Security Policy" adopted by the organization.

3. Policy elements

i. Confidential data

Confidential data is secret and valuable. Data could be of following types:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we have laid down the right practices and guidelines on how to avoid security breaches.

ii. Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep their company-issued computer, tablets and cell phones secure. To ensure this, they should;

- Keep all devices password protected.
- Install and upgrade a corporate antivirus software.
- Ensure they do not leave their devices exposed or unattended.

- Install security updates of browsers and systems periodically.
- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

iii. Keep emails safe

Emails often host scams and malicious software. To avoid virus infection and subsequent data theft, we advise employees to:

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

If an employee isn't sure that an email they received is safe, they can refer to our IT Support.

iv. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure to be hacking proof, but they should also remain secret. For this reason, we advise our employees to:

- 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.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every month.

v. Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless necessary.

- Share confidential data over the company network/ system and not over public network/Wi-Fi connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts.
- Limit use of external storage drives, only company's authorised device must be used.
- Use Google Drive for transfer of bulk data.

IT department needs to know about scams, breaches, and malware so they can protect our infrastructure better. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible. IT department would investigate promptly, resolve the issue, and send a companywide alert when necessary.

IT department is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

vi. Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to HR/ IT department.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to access the internet cautiously. IT support team would:

✓ Install firewalls, anti-malware software and access authentication systems.
✓ Arrange for security training of all employees.
✓ Inform employees regularly about new scam emails/viruses and ways to combat them.
✓ Investigate security breaches thoroughly.

vii. Remote employees

Remote employees must also follow this policy's guidelines. They would be accessing our company's system from a distance; hence, they are obliged to follow all data encryption and data protection settings. They should ensure that their private network is secure. We encourage them to seek advice from the IT department to ensure the same.

4. Reference to Other Policies

Relevant sections of GEM's following policies shall also be applicable, as required;

i) Policy for preservation of Documents
ii) Risk Management Policy

GEM ENVIRO MANAGEMENT LTD.

Unit no. 203, Central Square, Plaza 3

M.L. Khurana Marg, Bara Hindu Rao

Delhi – 110006

https://gemrecycling.com