Cybersecurity Policy

1. Policy brief & purpose

This policy outlines guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become to security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. Security measures and instructions have been drawn up to help mitigate security risks which are hereby outlined.

2. Scope

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

3. Policy elements

3.1 Confidential data

Confidential data is secret and valuable which employees are obliged to protect. Common examples are:

- Unpublished financial information.
- Data of customers/members/employees/partners/sellers.
- Sensitive corporate information.
- Customer lists (existing and prospective).

3.2 Protect personal and company devices

When employees use their digital devices to access company emails etc. they may introduce security risks to our data. They must keep personal and company-issued computer/mobiles secure by:

- Keeping all devices password protected.
- Choosing and upgrading to a complete antivirus software.
- Ensuring they do not leave their devices exposed or unattended.
- Installing security updates of browsers and systems monthly or as soon as updates are available.
- Logging into company accounts and systems through secure and private networks only.

Employees are advised to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Prior being granted use of company-issued equipment, new hires must sign the company's Information Security Policy and follow instructions to protect their devices.

3.3 Keep emails safe

Emails may host scams and malicious software. To avoid virus infection or data theft, employees must:

- 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 they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

The company routinely provides cybersecurity awareness training. This training is mandatory for all employees having systems/email access. If an employee isn't sure whether an email they received is safe, they are advised to refer to our IT department, prior to taking any further action with the suspicious email communication.

3.4 Manage passwords properly

Password leaks are dangerous as they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, 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.
- Passwords should never be exchanged.
- Change passwords every two months or when it's suspected that a password was compromised.

3.5 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 absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT department for help.
- Share confidential data over the company network, not over public Wi-Fi or private 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.

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

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

3.6 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.
- 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/illegal software on company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media & internet usage policy.

Our company will have all physical and digital shields to protect information and our IT department should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them (employees should all be aware through cybersecurity training).
- Investigate security breaches thoroughly (may need to be outsourced).

- Follow these policies provisions as other employees do.
- Consider deploying an MDM (Mobile Device Management) solution.

3.7 Remote employees

Remote employees follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage them to seek advice from HR and the IT department.

3.8 Disciplinary Action

Employees must follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior hasn't resulted in a security breach.

3.9 Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.