(Document last revision 2022/8/01)

VILLAGE ISLAND CO LTD – Cyber Security Policy

POLICY BRIEF & PURPOSE

Our company cyber security policy outlines our 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 severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize the trust our customer have in our company. For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

SCOPE

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access (hereafter called "*company members*") to our systems and hardware.

IT SPECIALIST/NETWORK EXPERT

Our company has assigned a specific IT specialist (hereafter called "IT Specialist"), network expert and responsible person, ready to advise and act on any cyber security concern. Feel free to confirm his contact details whenever relevant.

POLICY ELEMENTS

Confidential data

It is mandatory that company members sign our standard Non-Disclosure Agreement (NDA) to enforce protection of secret and valuable data. Data (hereafter called "data") may be internal and external information of various type: financial, product road map, marketing, technical, customer contact information, etc..
Our standard NDA template can be made available to any legitimate inquiring party.

Protect Personal and company devices

When company members use their digital devices to access company emails or accounts, they introduce security risk to data. We advise our company members to keep both their personal and company issued computer, tablet and cell phone secure, by the following recommendations:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.

- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems periodically or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only

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

Keep email safe

Emails often host scams and malicious software (e.g. worms.). To avoid virus infection or data theft, we instruct 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 they are legitimate, and from the right domain name.
- Look for inconsistencies

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

Manage passwords properly

Password leaks are dangerous since 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 company members 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 two months.

Transfer data securely

Transferring data introduces security risk. Our company members 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 Specialist for advice and help.
- Whenever possible, share confidential data over the company network/ system and 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 and share internally identified scams, privacy breaches and hacking attempts.

Our IT Specialist needs to know about scams, breaches and malware so he can better protect our infrastructure. For this reason, we advise our company members to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our IT specialist. Our IT specialist must then investigate promptly, resolve the issue and send a companywide alert when necessary. Our IT specialist can also advise our company members on how to detect scam emails.

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 IT Specialist.
- 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 company members to refrain using the company network for social media and personal internet usage.

Our IT Specialist should:

- Install firewalls, as well as other physical and digital shields to protect company network and data.
- Make sure anti-malware, anti-virus software is installed on devices
- Access authentication is in place whenever relevant
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other company members would do.

Employees working remotely

Employee working remotely must follow this policy's instructions too. They must ensure their private network is secure, and their device is kept free from disruptive element, with same care as if it would be a device inside the company network.

We encourage them to seek advise to our IT Specialist

Disciplinary Actions

We expect all our employees to always 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 the member contract termination. We will examine each incident on a case-by-case basis.

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

Take security seriously

Everyone, including our customers and partners, 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.