CYBER SECURITY POLICY

OF

S.J.S. ENTERPRISES LIMITED

1. INTRODUCTION

A cyber security policy is essential for protecting an organization's digital assets from cyber threats. It outlines measures to secure information systems, networks and data, defines roles and responsibilities and establishes procedures for incident response and recovery. A robust cyber security policy builds trust with stakeholders and ensures business continuity.

In view of the above, **S.J.S. Enterprises Limited** ("**Company**") has formulated the Cyber Security Policy ("Policy").

The Board had adopted this Policy at its meeting held on 27th March, 2023.

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

Confidential data:

- Unpublished financial information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 will give our employees instructions on how to avoid security breaches.

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 both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- 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 monthly or as soon as updates are available.
- 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.

When new hires receive company-issued equipment they will receive instructions for:

- Password management
- Installed antivirus / anti-malware software
- Domain account
- Email account
- ERP account (if applicable)

They should follow instructions to protect their devices and refer to our IT Team if they have any questions.

Keep emails 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, vouchers.).
- 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.).

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

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 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 two months.

Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

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 the IT Team for help.
- 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 scams, privacy breaches and hacking attempts

The IT Team needs 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 team in writing or in person.

The IT Team must investigate promptly, resolve the issue and send a companywide alert when necessary.

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.

The System Administrator 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.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Remote employees:

Remote employees must 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 the IT Team.

Firewalls:

a. This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to SJS' network and information systems.

b. The firewall will (at minimum) perform the following security services:

i. Access control between the trusted internal network and untrusted external networks
ii. Block unwanted traffic as determined by the firewall ruleset
iii. Hide vulnerable internal systems from the Internet
iv. Hide information, such as system names, network topologies, and internal user IDs, from the Internet
v. Log traffic to and from the internal network
vi. Provide robust authentication
vii. Provide virtual private network (VPN) connectivity

c. All network firewalls, installed and implemented, must conform to the current standards as determined by SJS' IT Department. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

d. The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this policy.

e. Outbound – allows all Internet traffic to authorized groups

f. All traffic is authorized by Internet Protocol (IP) address and port The firewalls will provide:

i. Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.
ii. Application proxy – every packet is stopped at the proxy firewall and examined and compared to the rules configured into the firewall.
iii. Stateful Inspection – a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.
iv. The firewalls will protect against:
v. IP spoofing attacks – the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
vi. Denial-of-Service (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets.

g. Any network information utility that would reveal information about the SJS domain.

h. A change control process is required before any firewall rules are modified. Prior to implementation, SJS network administrators are required to have the modifications approved

by the Chief Information Officer. All related documentation is to be retained for three (3) years over email or in writing.

i. All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.

j. The IT Department is responsible for implementing and maintaining SJS' firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and designees as assigned. Password construction for the firewall will be consistent with the strong password creation practices outlined in the SJS Password Policy.

k. The specific guidance and direction for information systems security is the responsibility of IT.

l. This IT dept. will be responsible for:

i. Retention of the firewall rules
ii. Patch Management
iii. Review the firewall logs for:
iv. System errors
v. Blocked web sites
vi. Attacks
vii. Sending alerts to the SJS network administrators in the event of attacks or system errors
viii. Backing up the firewalls

Disciplinary Action:

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 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 behaviour hasn't resulted in a security breach.