CYBER SECURITY POLICY

PREFACE

TITLE	**CYBER SECURITY POLICY**
VERSION NUMBER	**2.00**
EFFECTIVE DATE	**05.05.2026**
AUTHORISED BY	**BOARD OF DIRECTORS**

At JSW Group, Information is our most valuable asset and protecting this is mission-critical for our business operations.

Management at JSW demonstrates strong commitment towards cybersecurity. It strives to continuously review and provide the necessary means to strengthen the cyber security posture and safeguard JSW assets.

Cyber Security Scope

The policy applies to all businesses operations at JSW including information and business assets. This is applicable to employees, consultants, contractors, associates, suppliers / third-party personnel having access to JSW information assets.

Cyber Security policy broadly covers following three areas as:

1. Physical security: It mandates what protection should be wielded to safeguard the physical asset for both employees and management, applies to the prevail facilities including doors, entry point, etc.

2. Personnel management: Tell employees how to conduct or operate day to day business activities in a secure manner, for instance, password management, confidential information security, etc., applies to individual employees.

3. Hardware and software: It directs the administrator what type of technology to use and what and how network control should be configured and applies to system and network administrators.

Policy brief & Purpose:

Cyber Security Policy outlines guidelines and provisions for preserving the security of its 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 our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks.

Policy Elements:

- Confidential Data
- Protect personal and company devices
- Keep Emails Safe
- Manage passwords properly
- Transfer data securely
- Additional Measures

Confidential Data

Confidential data is secret and valuable. Common examples are:

- Software & Applications
- Unpublished financial information
- Data of vendors

All employees are obliged to protect this data.

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 computers, tablets and mobile phones secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade 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. They should follow instructions to protect their devices and refer to the IT Support Team if they have any questions.

Keep Emails Safe

Emails often host scams and malicious software (e.g. worms / ransomware). 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", "Account is locked").
- Be suspicious of clickbait titles (e.g. offering prizes, advice).
- Check email addresses 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 the IT Support 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 confidential. For this reason, we have group policy and 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.

Transfer Data Securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. Software & Applications, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, employees should seek assistance from the IT Support Team.
- Share confidential data only over the company network/system and not over public Wi-Fi or private connections.
- Ensure that recipients of the data are properly authorized individuals or organizations and have adequate security policies in place.

Report Scams, Privacy Breaches and Hacking Attempts

The IT Support Team must be informed about scams, breaches, and malware incidents so that they can effectively protect the Company's infrastructure. Employees are advised to report any perceived attacks, suspicious emails, or phishing attempts as soon as possible.

The IT Support Team shall promptly investigate reported incidents, take necessary corrective actions, and issue company-wide alerts where required. Employees are encouraged to reach out to them with any questions or concerns.

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. We have applied group policy in server to lock screen after 3 minutes of inactivity.
- Report stolen or damaged equipment as soon as possible to the IT Department.
- Change all account passwords at once when a device is stolen.
- Report any 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.

Cyber Security Policy Statement
JSW will

- Consistently thrive to upgrade technology, systems and processes to be ahead of the curve from cyber security perspective.
- Continuously protect internal information and information related to suppliers, customers, business partners and other stakeholders from unauthorized access, disclosure and/or modification.
- Ensure compliance with applicable regulatory, and legal requirements and information security management system.
- Apply effective risk management framework to identify and treat current and emerging risks to JSW's business with potential to disrupt operations and/or brand reputation.
- Ensure that all Business Heads / Department Heads are directly responsible for ensuring compliance with JSW's Information security policy in their respective business domains.
- Ensure that information is protected against known and future cyber security threats by designing, implementing, and continually improving security controls.
- Shall periodically review the effectiveness of the cyber security controls deployed and take corrective and preventative actions to improve the posture.