



Cyber Security Policy

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 hosted across all geographies. This is applicable to employees, consultants, contractors, associates, suppliers / third-party personnel having access to JSW information assets.

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 including ISO/IEC 27001:2013 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.

Seshagiri Rao MVS

Jt. Managing Director & Group CFO

Date: 14th July 2022

