JINDAL STAINLESS LIMITED

CIN: L26922HR1980PLC010901
Corporate Office: Jindal Centre, 12, Bhikaiji Cama Place, New Delhi – 110066
Registered Office: O.P. Jindal Marg, Hisar, Haryana-125005
T: +91 11 41659169, 26101562
E: info@jindalstainless.com Website: www.jindalstainless.com

Title	Information Security Policy
Effective Date	**29.01.2025**
Approved by	**Board of Directors**
Last revision Date	**-**

1. OBJECTIVE:

This Information Security Policy explains how Jindal Stainless Limited (hereinafter referred to as "JSL" or "We" or "Our" or "Us") recognizes information as one of the most valuable asset belonging to our business and operations, contributing significantly to maintaining and enhancing our competitive edge. This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility to:

- Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets.
- Manage the risk of security exposure or compromise.
- Assure a secure and stable information technology (IT) environment.
- Identify and respond to events involving information asset misuse, loss or unauthorized disclosure.
- Monitor systems for anomalies that might indicate compromise; and
- Promote and increase the awareness of information security.

2. SCOPE AND APPLICABILITY:

This policy applies to JSL and all its affiliated companies including, employees, contractors, consultants, auditors, third-party vendors and others who have access to JSL's information and information systems.

3. POLICY GUIDELINES:

- The achievement of our business goals depends on our ability to safeguard the information; we create or possess by ensuring its confidentiality, integrity and availability at all times.
- Information assets shall be classified based upon their business value, risk exposure and accordingly adequate controls shall be applied aligned to the business requirements. The Information Security Management System Framework ['ISMS'] will furnish necessary measures such as policies, procedures, and suitable solutions to facilitate this process.
- This policy ensures supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners.
- Direct responsibility for ensuring compliance with our information security policy within their respective business domains lies with the Business Heads/ Department Heads.
- Our employees shall understand the value of information and exercise their individual and collective responsibility to protect it.
- JSL shall establish need to know internal controls related to who has access to third-party information and procedures for employees to obtain access to include the reasons of their access.
- JSL shall establish formal timelines for which third-party information will be retained in order to prevent exposing substantial levels of information and data to breaches.
- JSL shall provide periodic ISMS training to all the stakeholders including employees, contractors, suppliers, customers, third-party service providers.
- Access to information and information systems at JSL will be regulated by the JSL's Information Security Policy. This policy extends to inter alia visitors, guests, business associates, consultants, vendors, suppliers, and contractual employees who are on JSL premises or have access to JSL's information and information systems.
- Respect for individual is central to the ethos of our organization and hence, the Information Security Framework will ensure that sufficient mechanisms are established to address the protection of privacy of employees within JSL.
- JSL shall implement procedures to respond data breaches rapidly and to consult customers prior transferring or sharing their Personally Identifiable Information (PII) to third parties.

- JSL shall continuously strive to improve and strengthen our Information Security initiative and integrate it as a part of our identity and business action.

4. Grievance Management

All reported incidents will be investigated thoroughly by the appropriate personnel aiming to determine the cause of the incident, assess the extent of the damage, and implement corrective actions to prevent future occurrences. Any breaches/ grievance against the policy can be reported at the email id: **cyberincidents@jindalstainless.com/**.

5. Review and Amendment

The Policy will be periodically reviewed and updated as required. Any amendments to the Policy would be undertaken with the approval from the Board of Directors.