

Information Security Policy

Document Number: Jindal Steel/Info Sec/2025/01
Version: 1.0, Date: 21-08-2025

-Public-

All information contained in this document is proprietary and intended solely for use
by

Jindal Steel Limited's Employees.

Any unauthorized duplication or distribution is strictly prohibited.

Document Control

Document Publication History	
Document Prepared by	Rishi Raj Srivastava
Document Reviewed by	Aditya Vardhan
Document Approved by	Indradyumna Datta
Document Owned by	Corporate – Information Technology
Effective Date	05-12-2025
Review Frequency	Annual
Document Classification	Public

This Transcript is fully **DJSI** compliant.

Document Publication History: DJSI Compliance	
Document Prepared by	Pratik Ghosh
Document Reviewed by	Naveen Ahlawat

Document Distribution List			
#	Name	Organization	Purpose
1	Jindal Steel Limited	Jindal Steel Limited	

Document Approval History				
Version	Date	Name	Role	Comments
1.0	05-12-2025	Indradyumna Datta	CDO	Summary version of detailed Internal Information Security policy.

Jindal Steel is dedicated to a robust implementation of Information Security Management. It strives to ensure the proper confidentiality, integrity, and availability of its data. The principles set out in this policy shall be applied to all physical and electronic information assets for which Jindal Steel holds responsibility. Jindal Steel is particularly committed to safeguarding the confidentiality, integrity, and availability of documentation and data supplied by, generated by, and held on behalf of third parties in connection with work carried out under contract, in accordance with the requirements of data security standards.

This policy applies to, and will be communicated to, all employees, contractors, and third parties who interact with information held by Jindal Steel, as well as the information systems used to store and process it. It covers all systems, both automated and manual, for which Jindal Steel holds administrative responsibility, including those managed or hosted by third parties on behalf of Jindal Steel.

To safeguard our information, we endeavour to adhere to the following aspects:

- We are committed to safeguarding information through strict adherence to data protection standards and maintaining the accuracy and reliability of all data assets.
- The policy promotes the continuous improvement of information security systems through regular reviews, audits, and updates in line with emerging threats and best practices.
- We are committed to implementing active monitoring and prompt responses to information systems to identify potential security threats and vulnerabilities without delay. Our comprehensive threat detection approach is detailed within the full policy, which is accessible internally to all employees and relevant stake holders.

- The risks associated with access to JINDAL STEEL 's information processing facilities by third parties shall be assessed and appropriate security controls implemented. Where there is a need to connect to a third-party location, a risk analysis shall be carried out to identify any requirements for specific security measures.
- All employees of the organization and, where relevant, third-party users shall receive appropriate training and regular updates on organization policies and procedures.

CISO (Chief Information Security Officer) is responsible for overall maintenance of this Information Security Policy at Jindal Steel. Furthermore, the Department/Function Leads are the risk owners of their respective departments and will be responsible for classifying the information within their respective areas with respect to the Confidentiality, Integrity, and Availability (C, I, A) of information and ensuring Information security policy adheres within the function.

All employees, contractors, and vendor staff working for Jindal Steel shall adhere to this Information Security policy.



Indradyumna Datta
Chief Digital Officer