AI Security Policy

Document Control:

Document Title	AI Security Policy
Document Number	A05-1-1-JSL-ISMS-POL-AI Security Policy-V1.0
Document Version	V1.0
Date	01-Jan-2025
Document Classification	Internal

Version History:

Version	Date	Reviewed By	Approved By	Comments
V1.0	01-Jan-2025	CISO	CDIO	Reviewed and Approved
V1.1	14 Jan 2026	CISO	CDIO	No change made

Document Distribution

Digital & IT Department is responsible for communicating the latest version of the document to all the functions of Jindal Stainless Limited (JSL) The Corporate Communication function shall ensure distribution of the document to all employees and relevant third parties respectively.

Contents

1. Purpose

The purpose of this policy is to establish Jindal Stainless Limited's (JSL) high-level direction and commitment toward the secure, ethical, and compliant use of Artificial Intelligence (AI) technologies.
This policy ensures that all AI-related initiatives protect data confidentiality, integrity, and availability while aligning with applicable laws, regulations, and ethical standards.

2. Scope

This policy applies to all JSL business units, employees, contractors, partners, and third parties involved in the design, development, procurement, deployment, or use of AI-based systems, whether developed internally or externally.

3. ISO/IEC 27001:2022 Alignment

- Clause A.5 – Organizational Controls
    - A.5.1 Policies for Information Security.

4. Policy

4.1 Governance and Accountability

- JSL shall maintain governance oversight for the ethical and secure use of AI technologies through defined roles and responsibilities approved by management.
- AI systems shall undergo appropriate risk and impact assessments prior to deployment, considering potential effects on individuals, business operations, and society.
- All AI initiatives must be approved through established digital transformation and information security governance processes.

4.2 Data Security and Privacy

- AI systems must comply with JSL's data protection and privacy policies to ensure lawful, fair, and transparent processing of data.
- Sensitive or confidential data shall not be used with publicly accessible AI systems.
- Personally Identifiable Information (PII) used in AI training or operations shall be protected using approved anonymization or pseudonymization methods and handled under defined retention and access control procedures.

4.3 Intellectual Property Protection

- JSL's proprietary or confidential information shall not be shared with or uploaded to external or public AI tools without explicit management authorization.
- All AI solutions shall respect third-party intellectual property and licensing rights.

4.4 Compliance and Ethics

- All AI deployments shall comply with applicable laws, regulatory requirements, and organizational codes of ethics.
- AI shall be used responsibly, avoiding bias, discrimination, or unethical outcomes in decision-making processes.
- Compliance monitoring shall form part of the periodic ISMS review process.

4.5 Incident Management and Awareness

- Any suspected or actual data leakage, misuse, or breach involving AI systems shall be reported immediately to location IT/Security team.
- Awareness programs shall be conducted periodically to educate employees on AI security, privacy, and responsible use.