Information Security Policy

1. Scope

This policy applies to all information assets, information processing systems, networks, applications of Hindustan Zinc Limited (HZL). It covers all individuals who access or manage HZL's information resources including employees, contracted staff, business partners, vendors, and any other third party associated with HZL.

2. Purpose

To ensure Security, Confidentiality, Availability, Processing Integrity and Privacy of HZL's information assets and processing systems to establish a framework for governance, accountability, and resilience against cybersecurity and data risks.

3. Compliance Reference

HZL Information Security Policies and Standards are designed to address protections required by existing laws, regulations, and frameworks (NIST, COBIT, ISO 27001, ISO 27701, ISO 31000, ISO 22301, Digital Personal Data Protection Act (DPDPA) 2023, India IT Act 2000) and are updated as necessary.

4. Information Security Governance & Oversight

a. **Board Oversight:** Cybersecurity governance is overseen by the **Audit & Risk Committee of the Board**, ensuring cyber risks are integrated into enterprise risk management.

b. **Executive Management Committee:** HZL Executive Committee (EXCO) sets up expectations, providing direction and support; reviewing and monitoring the progress and maturity of the cybersecurity posture of HZL and approving exceptions to the enforced policies, if any.

c. **Cyber Security Operations Committee:** Chief Information Officer (CIO), Chief Information Security Officer (CISO) and Data Governance & Privacy Officer (DGPO) are responsible for driving cybersecurity strategy, policies, operational activities and reviews with internal and external experts.

d. **Policy Review:** Information security policies must be reviewed annually, supporting best-in-class industry standards and regulatory requirements.

e. **Approval:** All security policies are prepared and reviewed by CISO/DGPO and are approved by the CIO.

5. Policy Statement

HZL commits to ensure that all information security policies, procedures, and standards are managed, controlled, and aligned with business objectives, conducting risk assessments across business processes to identify threats and vulnerabilities, classifying and handling all data/assets as per HZL classification standards, enforcing disciplinary action for policy violations; establishing secure design, resilience, and controls across physical, technical, and organizational domains.

6. Cybersecurity Goals

a. Align security with business and sustainability objectives.
b. Build resilient security architecture across Information Technology (IT), Operational Technology (OT), and Digital Platforms.
c. Ensure compliance with best-in-class industry frameworks, practices and applicable regulatory requirements.
d. Establish measurable metrics to evaluate and improve security maturity.

7. Information Security Objectives

a. **Leadership Commitment** – Ensure top management's active involvement and commitment by establishing a governance framework aligned with business objectives, contractual, legal, and regulatory requirements.
b. **Risk Management** – Identify risks and threats to business processes using a structured risk assessment process and implement mitigation strategies.
c. **Integrity & Data Protection** – Safeguard confidentiality, integrity, and availability of information assets.
d. **Threat Monitoring & Response** – Proactively monitor, detect, and respond to threats and vulnerabilities.
e. **Security Incident & Breach Management** – Implement mechanisms to report, investigate, and resolve security incidents and weaknesses; ensure corrective and preventive actions are taken.
f. **Third-Party Security Requirements** – Ensure vendors, suppliers, and partners meet HZL security requirements.
g. **Training & Awareness** – Build and sustain a security-conscious culture through regular information security & privacy awareness programs for employees and relevant third parties.
h. **Individual Responsibilities** – Define and enforce responsibilities for all employees, contractors, and partners.
i. **Management Review & Governance** – Adhere to timelines for management review meetings and audits, with prompt closure of gaps; ensure suppliers/third parties maintain equivalent data protection standards.

j. **Continuous Improvement** – Continuously improve the Information Security Management System (ISMS) to address evolving risks, technologies, and business needs, leveraging audits, reviews, and metrics for sustained maturity.

8. Cybersecurity Approach

a. Governance & Strategy

I. Cybersecurity embedded into enterprise governance, risk, and compliance (GRC).
II. Annual framework review by external experts.
III. Adoption of **security-by-design** and **privacy-by-design** principles in all systems.

b. Cyber Resilience

I. Continuous monitoring of information assets, incident response, and recovery protocols aligned with crisis management.
II. **Cyber insurance**, **incident response retainers**, and **executive cyber drills** for preparedness.
III. **Purple teaming** and penetration testing for continuous resilience improvement.
IV. Implement **Disaster Recovery & Business Continuity Plan (DR/BCP)** for critical business processes**.**

c. Awareness & Social Engineering

I. Mandatory security training for all employees and relevant business partners.
II. Social Engineering simulations and regular awareness campaigns.
III. Monthly and quarterly updates tied to employee performance reviews.

d. Privacy & Data Protection

I. Adoption of a **Privacy Information Management System (PIMS)** aligned with ISO 27701.
II. Compliance with DPDPA covering data discovery, privacy impact assessments, consent management and other provisions.

e. Operational Technology (OT) Security

I. Strengthening security of SCADA, PLC, and Laboratory systems.
II. Continual upgrades of legacy OT infrastructure to prevent exploitation.

f. Network and Infrastructure Security

I. Implementation of Zero Trust Security Architecture.
II. Multi-layered security controls considering defense-in-depth model.
III. Define and comply with Minimum Baseline Security Standards (MBSS) for information assets, as defined by HZL.

g. Cloud, Data Protection & Third-Party Risk

I. Secure cloud adoption aligned with industry standards.
II. Implementation of **Data Loss Prevention (DLP)** and monitoring.
III. Vendor security assessments and contracts embedding cybersecurity clauses.
IV. Integration of third-party risk management with GRC framework.

h. Physical Security, Environment and Safety

I. Implementation of physical access controls for employees, business partners and visitors using biometric, fencing, barriers, gates and turnstiles, as required.
II. CCTV coverage of all critical areas (such as perimeter, entrances, parking, server rooms, engineering control rooms).
III. Implementation of fire detection and suppression systems and emergency preparedness plan.

i. Audit, Assessment and Review

I. Define and drive comprehensive Vulnerability Management Program.
II. Period assessment of information assets through internal and external experts.
III. Review and measure the effectiveness of cyber security controls.

9. Roles and Responsibilities

I. All business heads/department heads are directly responsible for ensuring compliance with information security policy in their respective business domains.
II. Our employees are entrusted to understand the importance of information and safeguard it with responsibility at both individual and organizational levels.

10.Document Control

This document shall be reviewed as and when required or at least once a year in line with evolving threats & vulnerabilities, changing cyber security landscape, emerging technology standards and applicable regulatory requirements.

Arun Misra

Mr. Arun Misra
Chief Executive Officer