INFORMATION SECURITY POLICY

OF

LLOYDS METALS AND ENERGY LIMITED

(CIN: L40300MH1977PLC019594)

Registered Office: Plot No. A 1-2, MIDC Area, Ghugus, Chandrapur, Maharashtra - 442505

Tel. Nos.: 07172 285103 / 285398

Corporate Office: A-2, 2nd Floor, Madhu Estate, Pandurang Budhkar Marg, Lower Parel, Mumbai 400013

Tel. Nos.: 022 6291 8111

The Policy shall be maintained through the following revision and approval record:

Revision No.	Date of Approval
R0	16-03-2023
R1	03-11-2026

The Policy shall be approved by the Board of Directors and shall be reviewed periodically to ensure its continued relevance and effectiveness.

1. Purpose

Lloyds Metals and Energy Limited ("the Company" / "LMEL") recognizes that information, technology systems, operational technology, digital assets and data are critical assets for business continuity, safety, operations, stakeholders and long-term value creation. The purpose of this Information Security Policy ("Policy") is to establish the principles, standards and governance framework to protect the confidentiality, integrity and availability of information assets and to manage cybersecurity and information security risks in a systematic manner.

This Policy aims to prevent, detect, respond to and recover from information security incidents, data breaches, cyber threats and technology disruptions, while ensuring compliance with applicable laws, contractual requirements and recognized information security practices.

2. Scope and Applicability

This Policy is applicable to the Company, all its locations and all information assets, information systems, operational technology systems, networks, applications, databases, cloud environments, digital platforms, end-user devices, communication systems and information processed by or on behalf of LMEL.

This Policy is applicable to all individuals working at all levels and grades, including directors, senior management, officers, employees, workers, consultants, contractors, service providers, suppliers, vendors, agents, trainees, interns and any other person or entity accessing, processing, storing, transmitting or managing LMEL information or systems.

This Policy applies to information in all forms, including electronic, physical, verbal, confidential, personal, operational, financial, technical, commercial and business information.

3. Information Security Governance

3.1 Board / Executive Oversight

The Board of Directors / Audit Committee / Risk Committee / Executive Management shall have oversight of significant information security and cybersecurity risks, major incidents, privacy incidents, technology resilience and improvement actions, as considered necessary.

3.2 Management Responsibility

The Chief Information Officer / Chief Information Security Officer / designated information security function shall be responsible for defining and implementing the information security governance framework, risk management approach, policies, procedures, security controls, awareness programmes, incident response and reporting mechanisms.

3.3 Information Security Committee

The Company may establish an Information Security / Cybersecurity Steering Committee or equivalent governance forum to provide direction, review security posture, monitor key risks, support resource allocation and track implementation of information security initiatives.

3.4 Integration with Enterprise Risk Management

Information security and cybersecurity risks shall be integrated into the Company's enterprise risk management, internal control and business continuity processes, as applicable.

4. Information Security Principles

4.1 Legal and Regulatory Compliance

The Company shall comply with applicable laws, regulations, contractual obligations, data protection requirements and sectoral requirements relating to information security, cybersecurity, privacy, technology risk and business continuity.

4.2 Alignment with Recognized Standards

The Company shall strive to align its information security management practices with recognized standards and frameworks, including ISO/IEC 27001, NIST Cybersecurity Framework or other equivalent standards, as considered appropriate.

4.3 Confidentiality, Integrity and Availability

The Company shall implement appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of information assets and critical systems.

4.4 Continuous Improvement

The Company shall continually improve its information security practices based on risk assessments, incidents, audits, threat intelligence, technology changes, regulatory developments and business requirements.

4.5 Data and Information Classification

Information assets shall be identified, classified and handled based on sensitivity, criticality, business value and applicable legal or contractual requirements.

4.6 Access Control and Identity Management

Access to information assets and systems shall be granted based on business need, least privilege, role-based access, segregation of duties and periodic access review. User credentials shall be protected and monitored appropriately.

4.7 Secure Configuration and Asset Management

Information assets, hardware, software, networks, operational technology and cloud services shall be inventoried, configured, monitored and maintained in accordance with applicable security requirements.

4.8 Threat Monitoring and Vulnerability Management

The Company shall monitor threats, vulnerabilities and security events and shall implement vulnerability assessments, patch management, penetration testing or other security testing based on risk and criticality.

4.9 Incident Response and Escalation

The Company shall establish procedures for identifying, reporting, escalating, containing, investigating, remediating and recovering from actual or suspected information security incidents, cyber incidents and data breaches.

4.10 Business Continuity and Disaster Recovery

The Company shall maintain business continuity and disaster recovery arrangements for critical systems, data and processes and shall periodically test such arrangements.

4.11 Workforce Responsibilities

Employees, workers and contractors shall protect information assets, follow security requirements, protect credentials, avoid unauthorized disclosure and promptly report actual or suspected security incidents.

4.12 Third-Party Requirements

Third parties accessing, processing, storing or transmitting LMEL information or systems shall comply with applicable confidentiality, data protection, information security and incident reporting obligations.

4.13 Operational Technology Security

The Company shall consider cybersecurity requirements for operational technology, industrial control systems and connected digital systems, including access control, segmentation, monitoring and incident response, wherever applicable.

4.14 Secure Development and Change Management

Technology changes, applications, systems and digital solutions shall be developed, configured, tested and changed using appropriate security and change-management controls, as applicable.

4.15 Awareness and Training

The Company shall provide periodic information security and cybersecurity awareness training to employees, workers, contractors and relevant third parties.

4.16 Internal / External Audits and Certification

The Company may conduct internal and/or external reviews, audits or certifications of information security controls, including ISO/IEC 27001 or equivalent verification, as appropriate.

4.17 Breach Disclosure and Reporting

Material information security incidents, data breaches or cyber incidents shall be escalated and reported internally and externally where required under applicable laws, regulations, contractual obligations or reporting frameworks.

5. Information Security Management Programme

The Company shall maintain an information security management programme covering governance, asset management, risk assessment, security policies and procedures, access management, security operations, network security, endpoint security, application security, cloud security, operational technology security, vulnerability management, incident response, business continuity, third-party security, security awareness, audits and performance monitoring.

The programme shall be risk-based and shall prioritize critical assets, sensitive information, operational technology, business-critical systems and regulatory requirements.

6. Roles and Responsibilities

6.1 Board of Directors / Executive Management

The Board of Directors / Executive Management shall oversee significant information security risks, major incidents and programme effectiveness, as considered necessary.

6.2 CIO / CISO / Information Security Function

The CIO / CISO / designated information security function shall be responsible for implementing this Policy, defining controls, monitoring risks, coordinating incident response, reporting to management and supporting continuous improvement.

6.3 Business and Functional Heads

Business and functional heads shall ensure that information security requirements are implemented within their areas of responsibility and that employees and third parties comply with this Policy.

6.4 Employees, Workers and Contractors

Employees, workers and contractors shall comply with this Policy, protect information and systems, complete required training and report actual or suspected security incidents promptly.

6.5 Third Parties

Third parties shall comply with contractual and policy requirements relating to information security, privacy, confidentiality, access control, cybersecurity and incident reporting.

7. Reporting and Concerns

Any actual or suspected information security incident, cyber incident, unauthorized access, data breach, malware infection, phishing attempt, loss of device, misuse of credentials, policy violation or weakness in controls shall be promptly reported to the IT / Information Security function, reporting manager or designated reporting channel.

No person who in good faith reports an information security concern shall suffer harassment, retaliation or adverse consequences.

8. Monitoring, Metrics and Disclosure

The Company may monitor information security performance through indicators such as number and nature of security incidents, phishing simulation results, user awareness coverage, vulnerability closure,

audit findings, access review completion, business continuity test results, third-party security reviews and corrective action closure.

The Company shall disclose material information security governance, incidents, controls, certifications or programme information through annual report, sustainability report, BRSR, website or other applicable disclosures, where required or appropriate.

9. Documentation and Records

The Company shall maintain appropriate documentation and records relating to information security policies, risk assessments, asset inventories, access reviews, vulnerability assessments, penetration tests, incidents, investigation reports, corrective actions, business continuity tests, audits, certifications, training and third-party reviews, as applicable.

10. Review of Information Security Policy

This Policy shall be reviewed periodically by third-party auditors or earlier in case of changes in applicable laws, technology, business operations, threat landscape, incidents, risk profile, stakeholder expectations or information security requirements.