RESPONSIBLE ARTIFICIAL INTELLIGENCE 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:

Date of Approval

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 Artificial Intelligence ("AI") can support productivity, operational efficiency, safety, innovation, decision-making and stakeholder value. At the same time, AI may create ethical, legal, social, environmental, cybersecurity, privacy and reputational risks if not governed responsibly.

The purpose of this Responsible Artificial Intelligence Policy ("Responsible AI Policy" / "Policy") is to establish the principles, standards, governance and control framework for responsible, safe, transparent, accountable and ethical development, procurement, deployment and use of AI systems by or on behalf of the Company.

2. Scope and Applicability

This Policy applies to AI systems developed, procured, deployed, accessed or used by LMEL or on behalf of LMEL, including machine learning, predictive analytics, generative AI, computer vision, optimization models, autonomous or semi-autonomous systems, automated decision-support tools, chatbots, AI-enabled software, AI-enabled operational technology and third-party AI products or services.

This Policy is applicable to all directors, senior management, officers, employees, workers, consultants, contractors, service providers, suppliers, business partners and any other persons or entities involved in designing, developing, procuring, deploying, operating, monitoring or using AI systems for or on behalf of LMEL.

Where legal or regulatory requirements applicable to AI are more stringent than this Policy, such requirements shall prevail. This Policy shall be read together with LMEL's Code of Conduct, Data Privacy Policy, Information Security Policy, Human Rights Policy, Supplier Code of Conduct and other relevant policies and procedures.

3. Responsible AI Principles

3.1 Legal and Ethical Use

AI systems shall be developed, procured, deployed and used in accordance with applicable laws, regulations, contractual obligations, Company policies and ethical business conduct requirements.

3.2 Data Privacy

AI systems shall comply with applicable data protection and privacy laws. Personal data shall be collected, processed, retained, shared and deleted only for lawful, legitimate, necessary and authorized purposes.

3.3 Cybersecurity and Resilience

AI systems shall be protected through appropriate cybersecurity controls, including secure design, secure configuration, access controls, encryption, monitoring, vulnerability management, incident response and business continuity measures, where applicable.

3.4 Fairness and Bias Mitigation

The Company shall strive to identify, assess and mitigate bias, discrimination and unfair outcomes in AI systems through appropriate data governance, testing, validation, diverse and representative datasets where feasible, and periodic review.

3.5 Human Oversight

AI systems that support or influence significant decisions, safety-critical processes, employment-related matters, stakeholder outcomes or high-risk activities shall include appropriate human oversight, review, intervention and escalation mechanisms.

3.6 Transparency and Explainability

The Company shall strive to ensure that AI use, purpose, limitations, assumptions, risks and outputs are transparent and explainable to relevant users and stakeholders, as appropriate to the context and risk level.

3.7 Accountability

Roles and responsibilities shall be defined for AI system owners, developers, users, reviewers and approving authorities. Errors, misuse, incidents, unintended outcomes or policy violations shall be investigated and addressed.

4.8 Boundaries and Guardrails

AI systems shall be used only within approved business purposes, defined scope, authorized data sources, applicable laws and Company policies. High-risk or sensitive AI use cases shall be subject to enhanced review and approval.

4.9 Ecological Footprint

The Company shall consider energy, water, computing and carbon impacts of AI systems and shall strive to optimize AI use, model efficiency, infrastructure utilization and sustainability of AI deployment, wherever feasible.

4.10 Prohibited Uses

The Company shall not permit AI uses that are manipulative, exploitative, unlawful, discriminatory, unsafe, deceptive, socially harmful, unauthorized biometric surveillance, social scoring or otherwise prohibited under applicable laws or Company policies.

5. Responsible AI Governance

5.1 Board / Executive Management Oversight

The Board of Directors / Executive Management shall oversee material AI governance, risks, opportunities, incidents and responsible AI implementation, as considered necessary.

5.2 AI Governance Forum

The Company may establish a cross-functional AI governance forum or equivalent mechanism involving Information Technology, Information Security, Data Privacy, Legal, Compliance, Human Resources, Sustainability, Operations, Risk and relevant business functions.

5.3 AI System Owner

Each material AI system shall have an identified business owner accountable for intended use, risk assessment, compliance, monitoring and ongoing performance of the AI system.

5.4 Risk-Based Approach

AI systems shall be governed based on their risk level, including data sensitivity, operational criticality, safety relevance, stakeholder impact, human rights impact, cybersecurity exposure, legal risk and environmental impact.

5.5 Approval and Review

High-risk AI systems and sensitive AI capabilities shall be subject to appropriate review and approval prior to deployment and periodically thereafter.

6. Responsible AI Programme

6.1 AI Inventory and Risk Classification

The Company shall maintain, where feasible, an inventory of material AI systems and classify them based on purpose, owner, data sensitivity, user impact, business criticality and risk level.

6.2 Access Controls for Sensitive AI

Access to sensitive or high-risk AI systems, datasets, models, prompts, outputs and administration privileges shall be restricted to authorized personnel and monitored based on business need and least privilege.

6.3 Labeling and Disclosure of AI Use

AI-generated content, AI-supported decisions or AI interactions shall be clearly labelled or disclosed where appropriate and feasible, particularly where users or stakeholders may reasonably need to know that AI has been used.

6.4 Model Testing, Validation and Monitoring

Material AI systems shall be tested and validated before deployment and monitored for performance, accuracy, robustness, security, model drift, degradation and unintended outcomes.

6.5 Fairness and Bias Assessments

Relevant AI systems, particularly those affecting people, employment, safety, communities, customers or stakeholder outcomes, shall be subject to fairness, bias or impact assessments.

6.6 Model Drift Detection and Correction

The Company shall establish mechanisms, where feasible, to detect, review and correct model drift, performance degradation or unintended AI behaviour.

6.7 Human Review and Appeals

Where AI outputs materially affect individuals or stakeholders, appropriate human review, escalation, correction or appeal mechanisms shall be provided, where feasible and required. The Company shall keep humans “in the loop” for all critical decisions by ensuring meaningful human oversight, review, and accountability. Automated systems and AI tools shall assist decision-making but shall not independently make or implement critical decisions without appropriate human authorization. Employees shall have the ability to review, intervene, modify, or override automated outputs where necessary to manage risks, ensure fairness, and achieve responsible outcomes.

6.8 Sustainability and AI Impact

The Company shall strive to monitor and reduce the ecological footprint of material AI systems and may track relevant sustainability indicators such as energy consumption, computing intensity, cloud resource use or avoided environmental impact, where applicable.

6.9 Employee Training and Awareness

The Company shall provide awareness or training to relevant employees, users, developers and decision-makers on responsible AI, ethical use, data privacy, cybersecurity, bias, limitations and reporting of concerns.

6.10 External Verification

The Company may seek independent review, external assurance or certification of its AI governance or AI management system, including ISO/IEC 42001 or equivalent standards, where appropriate.

7. Data Governance and AI Inputs

AI systems shall use data that is obtained lawfully, processed for authorized purposes, suitably protected and appropriate for the intended AI use. Sensitive, confidential, personal, operational, safety-critical or regulated data shall be subject to additional safeguards and approvals, as applicable.

Employees and third parties shall not upload LMEL confidential information, personal data, trade secrets, source code, unpublished price sensitive information or sensitive operational data into public or unauthorized AI tools without approval.

8. Third-Party AI and Procurement

AI systems procured from vendors or embedded in third-party services shall be assessed, where applicable, for data privacy, cybersecurity, bias, explainability, intellectual property, sustainability, contractual safeguards, subcontracting, data use, audit rights, incident reporting and compliance with this Policy.

Suppliers and business partners providing AI-enabled products or services shall be expected to comply with responsible AI, data protection, cybersecurity, confidentiality and ethical conduct requirements.

9. Information Security, Incidents and Breach Management

Actual or suspected misuse of AI, unauthorized AI use, AI-enabled data leakage, security compromise, harmful output, model manipulation, prompt injection, privacy incident, intellectual property concern or other AI-related incident shall be reported promptly to the designated IT / Information Security / Compliance / Legal function, as applicable.

AI-related incidents shall be assessed, escalated, contained, investigated, remediated and reported internally or externally where required under applicable laws, regulations, contracts or reporting frameworks.

10. Reporting, Metrics and Disclosure

The Company may monitor responsible AI performance through appropriate indicators, which may include number of material AI systems inventoried, number of AI risk assessments completed, high-risk AI systems reviewed, employees trained, AI incidents reported, bias assessments completed, model monitoring reviews conducted, appeal requests handled and external verification status, where applicable.

The Company shall disclose material responsible AI governance, policy commitments, programme elements, risks, incidents or performance information through annual report, sustainability report, BRSR, website or other applicable disclosures, where required or appropriate.

11. Responsibilities

11.1 Executive Management

Executive Management shall support implementation of this Policy and may review material AI risks, high-risk AI use cases, significant incidents and improvement actions.

11.2 AI Governance Forum / Designated Function

The AI governance forum or designated function shall coordinate responsible AI governance, risk assessment, approvals, monitoring, training, reporting and policy implementation.

11.3 AI System Owners

AI system owners shall ensure that AI systems under their responsibility have defined purpose, approval, risk assessment, documentation, monitoring and controls.

11.4 Employees and Users

Employees and users shall use AI systems responsibly, comply with this Policy, protect information, verify AI outputs before use, avoid unauthorized AI tools and report concerns.

11.5 Suppliers and Business Partners

Suppliers and business partners shall comply with applicable responsible AI, privacy, cybersecurity and confidentiality requirements when providing AI-related products or services to LMEL.

12. Reporting and Concerns

Employees, contractors, suppliers and other stakeholders may report actual or suspected misuse of AI, bias, unsafe outcomes, privacy concerns, unauthorized AI use, inaccurate or harmful outputs, cybersecurity concerns or breach of this Policy through reporting managers, IT / Information Security, Compliance, Legal or other designated reporting mechanisms.

No person who in good faith reports a concern under this Policy shall suffer harassment, retaliation or adverse consequences.

13. Documentation and Records

The Company shall maintain appropriate records relating to AI inventory, risk assessments, approvals, data sources, testing, validation, monitoring, model drift reviews, bias assessments, human oversight, incidents, training, third-party assessments, corrective actions and external verification, where applicable.

14. Review of Responsible AI Policy

This Policy shall be reviewed periodically or earlier in case of changes in applicable laws, AI use cases, technology, risk profile, cybersecurity threats, stakeholder expectations, business operations or responsible AI requirements.