MIRI AFRICA LIMITED

AI ETHICS AND GOVERNANCE POLICY

1. PURPOSE

1.1 Miri Africa Limited ("Miri Africa" or the "Company") is committed to the responsible, lawful, safe and accountable development, procurement, deployment, use and oversight of Artificial Intelligence ("AI").

1.2 This Policy establishes the Company's principles, governance arrangements, control requirements and accountability framework for AI across its operations, products, services, partnerships and business activities.

1.3 The purpose of this Policy is to:

a. ensure that AI is developed and used in a manner consistent with the Company's values, mission and legal obligations;

b. promote innovation while managing risks to individuals, communities, customers, partners, employees, the environment and the Company;

c. provide a clear framework for the ethical and responsible use of AI throughout its lifecycle;

d. support trust, transparency, security, fairness and human accountability in relation to AI; and

e. establish minimum governance standards for the identification, assessment, mitigation, monitoring and escalation of AI-related risks.

1.4 This Policy is intended to provide appropriate safeguards to ensure ethical and responsible development and use of Artificial Intelligence (AI) technologies within the Company.

2. APPLICATION

2.1 This Policy applies to:

a. all directors, officers, employees, secondees, interns, temporary personnel, consultants, contractors and any other persons acting for or on behalf of the Company;

b. all business units, teams, functions, subsidiaries, affiliates and controlled operations of the Company;

c. all AI systems designed, developed, procured, licensed, configured, integrated, deployed, operated, used or retired by the Company or on its behalf;

d. all third-party AI systems, models, tools, platforms, services or application programming interfaces used in connection with the Company's business; and

e. all partnerships, pilots, collaborations, customer solutions, vendor arrangements and other engagements involving the use of AI by or for the Company.

2.2 This Policy applies throughout the full AI lifecycle, including concept development, use-case selection, procurement, design, data sourcing, model development, training, testing, validation, deployment, use, monitoring, maintenance, retraining, decommissioning and retirement.

2.3 This Policy applies whether AI is used for internal productivity, analytics, automation, decision support, content generation, software development, customer interaction, operational control, monitoring, or any other business or technical purpose.

2.4 Supplementary procedures, standards, guidance notes, templates and control documents may be issued from time to time to support the implementation of this Policy.

3. TERM DEFINITION

3.1 For the purpose of this Policy:

"AI Impact Assessment" means the documented assessment undertaken to evaluate the purpose, expected benefits, stakeholders, data sources, risks, safeguards, oversight arrangements, legal considerations and deployment suitability of an AI system.

"AI system" means any software, model, tool, application, service or technical component that uses AI.

"Artificial Intelligence" or "AI" means an engineered or machine-based system that, for explicit or implicit objectives, infers from inputs how to generate outputs such as predictions, content, recommendations, classifications, scores or decisions capable of influencing physical or virtual environments.

"Automated decision-making" means the use of AI to make or materially influence a decision without meaningful human judgement at the point of decision.

"Generative AI" means AI capable of creating, transforming or synthesising text, images, audio, video, code, data or other content.

"High-Risk AI" means any AI system that, by reason of its purpose, context, capability, scale or likely impact, may materially affect health, safety, legal rights, employment, education, financial outcomes, access to opportunities or services, public trust, environmental integrity, vulnerable persons, or the Company's regulatory, operational, financial or reputational position.

"Human Oversight" means meaningful human supervision, review, intervention or control that is appropriate to the nature, context and risk of the AI system and capable of influencing outcomes.

"Material AI Incident" means any event involving an AI system that results in, or is reasonably likely to result in, unlawful conduct, harmful or misleading output, significant error, discrimination, privacy breach, security incident, operational disruption, customer harm, reputational harm or regulatory exposure.

"Sensitive Data" includes personal data, confidential business information, customer data, privileged material, trade secrets, security credentials, regulated information and any other information classified by the Company as confidential, restricted or sensitive.

"Third-Party AI Service" means any externally provided AI model, system, tool, platform, service or API used by or on behalf of the Company.

4. POLICY STATEMENTS

4.1 AI plays a critical role in our organization's operations and future. We recognise the importance of responsible AI-use to uphold our values and mission.

Principles and Values

4.2 We are committed to the following AI principles:

- Ethical Use – AI systems must uphold ethical standards, ensuring fairness, accountability, transparency and the protection of human rights.
- Fairness- AI systems must be intentionally designed and validated to ensure that all types of known bias, be it based on any factor such as but not limited to race, gender, religion, socio-economic status, sexuality or political affiliation, are identified and eliminated.
- Reliability, Safety and Fitness for Purpose - AI systems shall be sufficiently reliable, robust and safe for their intended use and shall not be deployed unless their material

limitations, dependencies and foreseeable failure modes are understood and appropriately managed.

- Privacy, Confidentiality and Responsible Data Stewardship - AI shall be governed in a manner consistent with applicable data protection requirements, confidentiality obligations, data minimisation, purpose limitation, access control and responsible stewardship of information and the source of data used in AI systems shall be verified for consent from data subjects.

- Security and Misuse Prevention - AI systems shall be subject to appropriate technical and organisational safeguards to prevent unauthorised access, compromise, abuse, harmful misuse, data leakage, adversarial manipulation and other security or integrity failures.

- Transparency and Explainability -The Company shall maintain documentation and provide disclosures appropriate to the nature and risk of the AI system, including its purpose, limitations, oversight arrangements and material impacts where relevant.Accountability - AI systems must have a unit that is responsible for ensuring compliance with the principles and relevant governance processes including laws and policies on data security, privacy and integrity. Such unit shall be supervised by the Chief Technology Officer (CTO) in respect of the AI systems deployment and use.

- Lawfulness and Legitimate Purpose - AI shall be used only for lawful, authorised and legitimate purposes and in a manner consistent with applicable law, contractual obligations, internal policy and responsible corporate conduct.

- Human Accountability and Oversight - AI shall not displace accountable human governance. A designated owner shall remain accountable for each material AI system, and appropriate human oversight shall be maintained throughout the lifecycle of the system.

- Human Rights, Dignity and Fairness - AI shall be developed and used in a manner that respects human dignity and fundamental rights. The Company shall take reasonable steps to identify, assess, mitigate and monitor bias, unfairness and unlawful discrimination.

- Proportionality and Risk-Based Governance - AI shall be governed according to its risk profile, context and potential impact. Higher-risk uses shall be subject to enhanced assessment, approval, control and monitoring requirements.

- Continuous Improvement **-** AI governance shall be ongoing. The Company shall review, monitor and improve its AI systems, controls and governance arrangements

in light of operational experience, incidents, legal developments, evolving standards and technological change.

5. GOVERNANCE AND ACCOUNTABILITY

5.1 The Board of Directors, or a Board committee designated by the Board, shall exercise overall oversight of the Company's AI governance framework.

5.2 The Board or designated Board committee shall receive periodic reporting on:

a. material AI initiatives;

b. significant AI-related risks;

c. material AI incidents and remediation;

d. the adequacy and effectiveness of the Company's AI governance framework; and

e. any strategic, legal, regulatory or reputational matters arising from the Company's use of AI.

5.3 Executive management shall be responsible for ensuring that this Policy is implemented effectively and supported by appropriate governance structures, resources, controls, training and reporting mechanisms.

5.4 The Company shall designate an executive owner for AI governance, who shall have responsibility for the implementation, administration and oversight of this Policy.

5.5 The Company shall assign primary responsibility for the implementation and day-to-day oversight of this Policy to the Chief Technology Officer, subject to the oversight of the Chief Executive Officer. Where necessary, the CTO and CEO may obtain input from relevant internal or external advisers on legal, regulatory, privacy, security, operational and risk matters in relation to any material AI initiative.

5.6 The Chief Technology Officer, under the oversight of the Chief Executive Officer, shall be responsible for the implementation and oversight of this Policy and shall, as appropriate:

a. oversee the implementation of this Policy and any related standards, procedures or guidance;

b. review AI Impact Assessments for material AI systems;

c. determine or confirm the risk classification of AI systems;

d. approve, conditionally approve, defer or prohibit High-Risk or Restricted AI uses, subject to escalation where appropriate;

e. oversee material third-party AI arrangements and related risks;

f. review material AI incidents and remediation measures;

g. maintain oversight of the Company's AI systems inventory; and

h. escalate material AI matters to the Chief Executive Officer and, where appropriate, to the Board.

5.7 Each material AI system shall have a clearly designated owner responsible for its business purpose, authorised use, implementation, oversight and ongoing suitability. Depending on the nature, scale and complexity of the system, the same person may perform both the business and technical oversight roles.

5.8 No person may develop, procure, integrate, deploy, materially modify or use any AI system for Company business except in accordance with this Policy and any applicable internal review or approval requirements.

6. RISK CLASSIFICATION

6.1 Every material AI system shall be assessed and classified prior to development, procurement, pilot deployment or production use.

6.2 AI systems shall be classified by reference to their nature, purpose, context, users, data sensitivity, decision impact, operational criticality, legal implications and potential for harm.

6.3 The Company shall maintain a risk-based classification framework that includes, at a minimum:

a. Prohibited AI Uses;
b. Restricted or High-Risk AI Uses;
c. Moderate-Risk AI Uses; and
d. Low-Risk AI Uses.

6.4 An AI system shall ordinarily be treated as Restricted or High-Risk where it:

a. materially influences decisions affecting legal rights, employment, financial outcomes, access to services or other significant interests;

b. may affect health, safety, environmental integrity or operational resilience;

c. processes Sensitive Data at scale or in a particularly sensitive context;

d. involves biometric, surveillance, identity, behavioural or profiling capabilities;

e. is used in relation to vulnerable persons or sensitive contexts;

f. generates or materially supports outputs, advice, instructions, code or representations that may reasonably be relied upon; or

g. is otherwise likely to present significant legal, regulatory, ethical, reputational or societal risk

6.5 Risk classification shall be reviewed and, where necessary, updated whenever there is a material change in the system's purpose, scope, data inputs, users, outputs, underlying model, deployment conditions or risk profile.

7. PROHIBITED AND RESTRICTED USES

7.1 The Company shall not develop, procure, deploy, support or knowingly enable AI systems for any unlawful purpose or in any manner that is inconsistent with this Policy.

7.2 Without limitation, the following shall be treated as prohibited unless expressly required by law and approved at the highest appropriate level of governance:

a. unlawful discrimination or exclusion;

b. deceptive, manipulative or exploitative uses intended to materially distort behaviour or impair informed choice;

c. unlawful surveillance, monitoring or profiling;

d. social scoring of individuals;

e. fully automated decisions with legal or similarly significant effects on individuals without lawful basis and meaningful human oversight;

f. use of AI in a manner that knowingly infringes privacy, confidentiality, intellectual property or other legal rights;

g. use of confidential, customer or regulated data in public or unapproved AI tools; h. creation or dissemination of harmful, false or misleading synthetic content on behalf of the Company without lawful purpose, proper authority and appropriate disclosure where required; and

h. any other use prohibited by applicable law, regulations, contract or Board direction.

7.3 Restricted uses may only proceed where:

a. clear business justification exists;

b. the use has undergone enhanced assessment and review;

c. appropriate safeguards and controls are demonstrably in place; and

d. approval has been granted by the appropriate regulatory authority.

8. AI IMPACT ASSESSMENT AND APPROVAL

8.1 An AI Impact Assessment shall be completed before any material AI system is developed, procured, piloted, integrated or deployed.

8.2 The AI Impact Assessment shall, at a minimum, address:

a. the intended purpose and expected benefits of the system;

b. the use context and affected stakeholders;

c. the proposed risk classification and basis for that classification;

d. the data sources, data categories, provenance and applicable restrictions;

e. legal, regulatory, ethical, privacy, security, safety and fairness considerations;

f. foreseeable misuse, abuse, failure modes and adverse impacts;

g. proposed controls, limitations, human oversight arrangements and escalation measures;

h. validation, testing and monitoring requirements;

i. vendor or third-party dependencies; and

j. whether deployment is justified in view of the identified risks and available safeguards.

8.3 No Restricted or High-Risk AI system may be deployed unless:

a. the required assessment has been completed;

b. all required legal, compliance, privacy, security and risk reviews have been obtaine

c. the system has undergone appropriate validation and testing;

d. accountable owners have been designated; and

e. formal approval has been granted.

8.4 AI Impact Assessments shall be reviewed and updated:

a. before any material change to the system;

b. after any Material AI Incident;

c. where the risk profile materially changes; and

d. at prescribed review intervals, including at least annually for High-Risk AI systems

9. DATA GOVERNANCE, PRIVACY, CONFIDENTIALITY AND INTELLECTUAL PROPERTY

9.1 Data used in connection with AI systems must be relevant, appropriately sourced, suitably governed and used only in accordance with applicable law, contractual obligations, confidentiality duties and Company policy.

9.2 The Company shall maintain appropriate controls relating to:

a. data provenance and source verification;

b. lawful basis or authorisation for use where required;

c. data quality, relevance and suitability;

d. data minimisation and purpose limitation;

e. access control, segregation and least-privilege principles;

f. de-identification, anonymisation or pseudonymisation where appropriate;

g. retention, deletion and secure disposal; and

h. cross-border data handling where applicable.

9.3 No person shall input Sensitive Data, confidential information, customer information, regulated data, trade secrets, privileged material, security credentials or proprietary

source code into a public or unapproved AI tool except where expressly authorised and protected by approved contractual, technical and governance controls.

9.4 The Company shall take reasonable steps to assess and manage intellectual property, licensing and ownership risks associated with training data, prompts, outputs, model use and downstream deployment.

9.5 AI-generated outputs shall be reviewed as appropriate for accuracy, suitability, legal risk, confidentiality risk, harmful content, bias and intellectual property risk before being relied upon for material internal or external use.

10. DEVELOPMENT, PROCUREMENT AND DEPLOYMENT LIFECYCLE CONTROLS

10.1 AI systems shall be governed throughout their lifecycle and shall not be treated as ordinary software without AI-specific control measures.

10.2 The following minimum lifecycle requirements shall apply, as relevant to the system:

a. **Use Case Definition and Feasibility** - The business need, expected value, alternatives, context, intended users and potential risks shall be identified at the outset.

b. **Design and Requirements** - Requirements shall define intended use, prohibited use, performance expectations, oversight requirements, security controls, documentation needs and release criteria.

c. **Data Preparation and Management** - Data shall be assessed for quality, sensitivity, suitability, restrictions and bias-related considerations.

d. **Model Selection, Development or Procurement** - Models and tools shall be selected or developed with regard to reliability, controllability, explainability, security, vendor risk and the appropriateness of the model for the intended purpose.

e. **Testing and Validation** - Testing shall be proportionate to risk and may include performance testing, robustness testing, bias testing, security testing, misuse testing, adversarial testing, red-team exercises and validation against defined acceptance criteria.

f. **Release and Deployment Readiness** - No AI system shall be released into production until required approvals, controls, documentation, user instructions, monitoring mechanisms and rollback arrangements are in place.

g. **Monitoring and Maintenance** - The Company shall monitor material AI systems for performance degradation, drift, harmful outputs, anomalies, abuse, security weaknesses, unfair impacts and other indicators of control failure.

h. **Change Management** - Material changes to use case, data inputs, model capabilities, integrations, operating conditions or outputs shall require reassessment and may require renewed approval.

i. **Retirement and Decommissioning** - AI systems that are no longer appropriate, lawful, licensed, supported or fit for purpose, including systems for which any required licence, subscription, support arrangement or third-party right of use has expired, been terminated or otherwise ceased to be available, shall be retired or decommissioned in a controlled manner. Such retirement or decommissioning shall include, where applicable, discontinuance of use, revocation of access, secure handling or deletion of associated data and logs, management of dependencies and integrations, preservation of required records, and any other steps necessary to ensure legal, operational and information security compliance.

11. HUMAN OVERSIGHT, TRANSPARENCY AND EXTERNAL TRUST

11.1 The Company shall maintain documentation sufficient to explain each material AI system's purpose, approved uses, limitations, oversight model, owners, risk classification, monitoring arrangements and material dependencies.

11.2 Where appropriate to the context, and having regard to legal, commercial and security considerations, the Company shall provide clear information regarding the role of AI in relevant products, services, interactions or materially significant outputs.

11.3 Human Oversight shall be proportionate to risk and may include:

a. pre-use or pre-release review of outputs;

b. review of exceptions, anomalies or flagged outcomes;

c. authority to override, suspend, reject or escalate AI-generated outputs or actions; and

d. enhanced review in relation to decisions or outputs with potentially significant effects.

11.4 AI outputs shall not be presumed to be correct solely because they were generated by an automated system. Users remain responsible for applying judgement, professional standards and Company controls.

11.5 Where the Company uses AI-generated content externally, it shall ensure appropriate review, quality assurance, and disclosure where required or appropriate.

12. THIRD-PARTY AI SERVICES AND VENDOR GOVERNANCE

12.1 Third-Party AI Services shall be subject to due diligence proportionate to the nature and risk of the proposed use.

12.2 Due diligence shall consider, as appropriate:

a. the provider's governance, privacy and security posture,
b. the provider's data use practices and confidentiality safeguards,
c. the quality and sufficiency of model documentation,
d. known limitations, restrictions and safety features,
e. incident response and notification commitments,
f. subcontracting or onward transfer arrangements,
g. audit, access, transparency and exit considerations where appropriate,
h. intellectual property and licensing implications; and
i. jurisdictional and regulatory considerations.

12.3 Contracts involving Third-Party AI Services shall, where appropriate, address data protection, confidentiality, ownership and use of data and outputs, security obligations, restrictions on secondary use, incident reporting, compliance with applicable law, and rights of suspension or termination.

12.4 No third-party AI service may be connected to Company systems, workflows or data outside approved procurement, information security and governance processes.

13. INVENTORY, RECORDS AND AUDITABILITY

13.1 The Company shall maintain and keep up to date an inventory of its material AI systems.

13.2 The inventory shall, at a minimum, record:

a. the name or identifier of the system;
b. the designated owner responsible for the system;
c. the purpose and deployment context of the system;
d. the vendor, model or service provider, where applicable;
e. the applicable risk classification;
f. the relevant review or approval status;
g. the categories of data used by or in connection with the system;
h. the date of the last review; and
i. any material restrictions, incidents, decommissioning or retirement status.

13.3 Records of AI Impact Assessments, approvals, testing, incidents, monitoring, changes and retirement shall be retained in accordance with applicable law and the Company's records management framework.

13.4 AI governance records shall be accessible on a controlled basis to authorised management, legal, compliance, privacy, information security, risk and audit personnel.

14. Incident Reporting, Escalation and Remediation

14.1 All personnel must promptly report actual or suspected AI-related incidents, harmful outputs, anomalies, misuse, security concerns, privacy concerns, system failures or breaches of this Policy.

14.2 The Company shall maintain procedures for the identification, triage, investigation, escalation, remediation and documentation of AI-related incidents.

14.3 Where necessary to prevent or limit harm, the Company may suspend, restrict, disable or withdraw an AI system pending review or remediation.

14.4 Material AI Incidents shall be escalated promptly to the relevant accountable owner, the executive owner for AI governance, and such governance, legal, compliance, privacy, security, risk or management stakeholders as may be appropriate.

14.5 Following a Material AI Incident, the Company shall conduct an appropriate post-incident review, including root-cause analysis, corrective action, control enhancement, record updates and any required regulatory, contractual or stakeholder notifications.

15. Training, Awareness and Acceptable Use

15.1 The Company shall promote an appropriate level of AI literacy across the organisation and provide training proportionate to role and responsibility. Such training may include: general awareness for all personnel; specialised training for developers, product owners, reviewers and governance stakeholders; legal, ethical, privacy, security and confidentiality obligations; risks associated with generative AI, prompts, outputs and model misuse; and reporting and escalation obligations.

15.2 Personnel shall use only approved AI tools and shall comply at all times with applicable Company rules regarding confidentiality, records, intellectual property, information security, communications, regulatory compliance and responsible use of technology.

16. Compliance, Exceptions and Enforcement

16.1 Compliance with this Policy is mandatory.

16.2 Any exception to this Policy must be documented, justified and approved by the appropriate authority designated by the Company. No exception may be granted in respect of a prohibited use save where required by law and approved at the highest applicable governance level.

16.3 Any breach of this Policy may result in disciplinary action, suspension of access, contractual consequences, termination of engagement, legal action, regulatory reporting, recovery of losses, or any other appropriate remedial measure.

16.4 Any business unit, project team or individual that develops, deploys or uses AI outside approved governance channels may be required to suspend such activity immediately and undertake remedial review or corrective action.

17. Review and Continuous Improvement

17.1 This Policy shall be reviewed at least annually and more frequently where necessary to reflect changes in applicable law, regulation, standards or guidance; material changes in the Company's AI activities or risk profile; lessons arising from incidents, audits, assessments or reviews; or material technological developments.

17.2 The Company shall continue to refine its AI governance framework, implementation standards and control environment in line with evolving best practice, regulations, law, or stakeholder expectations.

18. Public Commitment

18.1 Miri Africa recognises that responsible AI governance is fundamental to trust, innovation and long-term corporate accountability. The Company is committed to developing and using AI in a manner that is lawful, ethical, accountable, secure and aligned with the interests of its stakeholders and the broader public.

Effective Date	14th April, 2026
Approver	Board of Directors
Review Cycle	Annually
Authorised Signature	