CORPORATE POLICY

Responsible AI

Version: 1.0 | Issue Date: 26 November 2025

Revised Responsible AI Policy

1. Introduction & Scope

MicroSourcing and Beepo (hereafter "the Company") acknowledge the transformative potential of Artificial Intelligence (AI) to revolutionize client experiences and optimize both our managed outsourcing solutions and internal operations. As AI and Machine Learning (ML) are increasingly integrated into our services and offerings, we commit to a framework of responsible, ethical, and lawful development and deployment.

This Policy governs all activities within the Company related to the design, development, deployment, procurement, and use of AI systems and the data that fuels them, encompassing traditional ML, advanced analytics, and emerging Generative AI (GenAI) technologies. This includes interactions with our clients, their customers, employees, partners, and stakeholders.

2. Guiding Purpose and Vision

The purpose of this policy is to establish clear principles and governance structures to ensure that our pursuit of AI-driven innovation is aligned with our commitment to societal welfare, human rights, and business integrity.

Our vision is to unlock new levels of innovation and excellence for our clients while maintaining the highest standards of safety, fairness, and accountability. This Policy guides the decisions and behaviors of all personnel and partners across the entire AI lifecycle—from initial ideation and data curation to commercialization and decommissioning.

3. Core Responsible AI Principles

The Company's approach to Responsible AI is grounded in the following comprehensive principles:

- **Fairness and Non-Discrimination:** We are committed to designing, developing, and deploying AI systems that treat all individuals and groups equitably. We will proactively identify and mitigate sources of algorithmic bias in data, algorithms, and system outputs to prevent unfair or discriminatory outcomes, particularly for protected characteristics.
- **Transparency and Explainability (XAI):** We strive to ensure that the workings and outputs of our AI systems are appropriately transparent and understandable relative to the potential impact. For high-impact systems, we will provide meaningful explanations (interpretability) regarding how decisions or recommendations are reached, enabling effective human review.
- **Privacy and Data Protection:** We will collect, process, and use data in conjunction with AI systems in strict adherence to applicable privacy laws (e.g., GDPR, CCPA) and client agreements. We will employ techniques like federated learning or differential privacy where appropriate to safeguard personal and sensitive information.
- **Security and Robustness:** Our AI systems will be designed to be resilient against adversarial attacks, manipulation, and unauthorized access. We will implement robust security controls and processes throughout the AI lifecycle to ensure their continuous availability, integrity, and operational safety.
- **Accountability and Governance:** Clear roles and responsibilities for the development, deployment, and oversight of AI systems will be established. We commit to maintaining comprehensive documentation and audit trails to verify compliance with these principles and regulatory requirements. Effective human oversight will be a mandate for all high-risk or high-impact decisions.
- **Societal and Environmental Benefit:** We prioritize the use of AI to drive positive outcomes for our clients, their customers, our employees, and the broader community. We are mindful of the potential environmental impact of large-scale AI models and will seek energy-efficient solutions.

4. Risk Management and Mitigation

We adopt a proactive, risk-based approach to the use of AI, scaling mitigation efforts according to the potential severity and likelihood of harm.

4.1 High-Priority AI Risks

We systematically assess and strive to mitigate risks including, but not limited to:

- **Bias and Fairness Risks:** The potential for AI outputs to reflect or amplify societal biases, leading to unfair or discriminatory treatment.
- **Generative AI (GenAI) Specific Risks:**
  - **Hallucination/Factual Accuracy:** AI generating false or misleading information.
  - **Copyright/IP Infringement:** Training data containing copyrighted material or outputs infringing on intellectual property.
  - **Data Leakage/Confidentiality:** Employees or clients inputting sensitive data into external GenAI tools.
- **Model Drift and Performance Degradation:** The AI system's performance deteriorating over time due to changes in real-world data distributions.
- **Privacy Violations:** The inadvertent exposure or inference of sensitive personal data.
- **Safety and Harm:** The potential for a deployed AI system to cause physical, psychological, or financial harm.

4.2 Risk Mitigation Strategy

We systematically assess and strive to mitigate risks including, but not limited to:

- **Risk Tiers:** AI use cases will be categorized (e.g., High, Medium, Low Risk) based on industry standards (e.g., EU AI Act) and a formal risk matrix.
- **Impact Assessments:** Mandatory **AI Impact Assessments (AIIAs)** will be conducted for all high-risk AI deployments before implementation.
- **Testing and Validation:** Rigorous, multi-faceted testing, including stress testing for security vulnerabilities and adversarial examples, will be mandatory.

5. Governance and Oversight

5.1 The AI Risks and Ethics Committee (AIREC)

The Company has established the **AI Risks and Ethics Committee (AIREC)** to serve as the highest oversight body for Responsible AI practices.

- **Membership:** Comprised of cross-functional experts including Heads of Technology, Information Security, Legal and Shared Services, People Strategy and People and Partnership Cluster Leaders.
- **Responsibilities:**
  - Review and approve **High-Risk AI Impact Assessments (AIIAs).**
  - Monitor evolving AI regulations and ensure policy compliance.
  - Define and approve remediation plans for policy violations or system failures.
  - Establish standards for vendor due diligence in the AI Partner Ecosystem.

5.2 Continuous Monitoring and Training

- **System Monitoring:** Comprehensive monitoring and alerting mechanisms will be deployed to track AI system performance, fairness metrics, and potential drift in real-time.
- **Continuous Learning:** All employees involved in the AI lifecycle will receive mandatory, recurring training on this Policy, emerging AI risks, and techniques for bias mitigation and security.

5.3 Trusted Partner Ecosystem

We expect all third-party suppliers, vendors, and subcontractors to demonstrate a clear commitment to Responsible AI principles that are consistent with this Policy. Our procurement and vendor management processes will include specific due diligence to validate their adherence to data security, privacy, and ethical AI standards.