Responsible Artificial Intelligence Policy

1. Purpose

In response to the rapid advancement of Artificial Intelligence (AI) technologies and their growing impact on business operations, products, and society, the Company establishes governance principles and management requirements covering the entire AI lifecycle, including AI adoption, development, procurement, usage, oversight, and decommissioning.

This policy aims to:

- Ensure that AI applications foster innovation while effectively managing associated risks.
- Systematically manage information security, privacy, regulatory compliance, and operational risks.
- Uphold the principles of fairness, transparency, explainability, and ethical use of AI.
- Strengthen corporate governance and support sustainable business development.

2. Scope

This policy applies to the Company and all of its global subsidiaries and covers all AI-related activities, including but not limited to:

- AI systems developed in-house
- Commercially purchased or third-party AI services
- Generative AI and Agentic AI

The scope of this policy encompasses the entire lifecycle of AI systems, including data processing, model development, testing, deployment, operation, and decommissioning.

3. Core Governance Principles

Based on the principles of Risk-Based and Human-Centric governance, the Company establishes the following AI governance foundations:

1. Respect for Data Privacy

The Company shall respect data privacy throughout the use and/or development of AI systems. During the AI lifecycle, the principles of lawfulness, legitimacy, and data minimization shall be ensured. Appropriate data classification, access controls, and protection mechanisms shall be implemented to safeguard personal data and sensitive information. All data processing activities must comply with applicable laws, regulations, and the Company's internal data governance requirements, and data shall only be used for approved purposes and within authorized scopes.

2. Protect the cybersecurity and information security of AI systems throughout their use and/or development.

AI systems and their supporting infrastructure shall be incorporated into the Company's information security governance framework. Risk-based technical and administrative controls shall be implemented, including:

- Identity and access management controls
- Data encryption and protection

- Vulnerability management and continuous monitoring
- Protection against AI-specific threats (e.g., prompt injection and model misuse)
- Prevention of abnormal or unauthorized behaviors
- Prevention of inappropriate or harmful outputs

3. Avoid Potential Bias Throughout the Use and/or Development of AI Systems

AI systems shall be designed and operated to prevent unfair or discriminatory outcomes resulting from data bias or model design. Through testing, monitoring, and continuous improvement mechanisms, the Company shall ensure that AI-driven decisions and outputs are reasonable, reliable, and trustworthy.

4. Maintain Human Oversight and Decision-Making

For decisions that may have a significant impact on individuals, customers, or business operations, a Human-in-the-Loop (HITL) mechanism shall be implemented to ensure that:

- AI-generated decisions are subject to human review and validation.
- Final decision-making authority remains with designated personnel.

This approach helps reduce the uncertainty and risks associated with high-impact automated decision-making.

5. Ensure Transparency and Explainability of AI Systems and AI-Generated Outcomes

AI systems shall disclose their intended purpose, operating principles, and limitations to a reasonable extent, and provide appropriate explanation mechanisms to enable users and stakeholders to understand the basis of relevant decisions or outcomes. Furthermore, users shall be able to recognize when they are interacting with an AI system.

6. Establish Clear Governance Mechanisms for AI-Generated Outputs

The Company shall clearly define AI governance roles and responsibilities, including the respective duties of governance functions, system owners, and relevant business units. The following management mechanisms shall be established:

- Establish or designate a dedicated function, committee, or responsible unit for AI governance and risk management.
- Clearly define system ownership, accountability, and responsibilities for the use of AI systems.
- Establish processes for incident reporting, investigation, corrective actions, and continuous improvement.

These measures are intended to ensure the traceability, accountability, and continual improvement of AI applications.

7. Define Clear Boundaries for AI Capabilities and Authorities

AI systems shall be used only for their approved purposes and within their authorized scope. They shall not be applied beyond their intended design objectives or extended to unauthorized use cases. The Company shall establish:

- Controls governing the permitted boundaries of AI usage.

- Review and approval mechanisms for high-risk AI use cases.
- Exception management and approval processes.

These measures are intended to ensure that AI systems operate within approved objectives, maintain appropriate oversight, and effectively manage risks arising from unauthorized or unintended use.
To prevent misuse and compliance risks.

8. Promote Sustainable Development

AI development and deployment shall take environmental sustainability and resource efficiency into consideration. Sustainability principles shall be integrated into AI governance and risk management processes. Where reasonably practicable, the Company shall prioritize the adoption of energy-efficient architectures and technologies to reduce computational resource consumption and carbon emissions.

9. Prohibit the Use of AI Systems Prohibited under the EU AI Act

The Company's AI applications shall comply with applicable laws, regulations, and internationally recognized standards in all jurisdictions where it operates. The following AI practices are strictly prohibited:

- AI systems designed to manipulate or distort human behavior.
- AI systems that exploit vulnerabilities of individuals or vulnerable groups.
- Social scoring systems.
- Biometric identification or surveillance activities conducted without lawful authorization.

The Company shall further comply with the prohibited AI practices defined under the European Union Artificial Intelligence Act (EU AI Act) and other applicable regulatory requirements, ensuring that AI technologies are not used in a manner that infringes upon fundamental human rights, human dignity, or social fairness.

Arthur Yu-Cheng Chiao
Chairman
July 2026