

Yihai Kerry Arawana Holdings Co., Ltd.

Responsible Artificial Intelligence Policy

With the vigorous development of the digital economy and the acceleration of the new generation of technological revolution, Artificial Intelligence (AI) is reshaping business logic and social forms in an unprecedented depth. Yihai Kerry Arawana Holdings Co., Ltd. (hereinafter referred to as "the Company") regards safe, controllable, and responsible AI governance as an important component of the company's digital transformation. Therefore, the Company has formulated this policy to clarify the ethical boundaries and action guidelines of the Company in the field of AI, ensuring that technological progress always goes in the same direction as safeguarding personal rights, enhancing public trust, and promoting environmental friendliness.

1. Scope of application

This policy applies to the Company and its subsidiaries, as well as suppliers and partners who provide AI-related products or services on behalf of the Company.

2. Data privacy

The Company respects and protects personal information, important data, trade secrets, intellectual property, and other protected data throughout the entire lifecycle of AI development and deployment, following the principles of legality, legitimacy, necessity, clear purpose, minimization, and security protection. The Company implements data classification and hierarchical management during the development, training, and application of AI systems. Without necessary security assessments and explicit authorization, it is strictly prohibited to input user privacy, trade secrets, core algorithms, and legally protected business data into public AI tools or unauthenticated third-party models to ensure the security of data assets in the AI era.

3. Cybersecurity

The Company has established an information security management system that complies with ISO27001, and continuously manages and improves AI-related infrastructure, systems, and services in line with information security management requirements and following the PDCA cycle. In response to AI-specific risks such as prompt injection, data poisoning, model theft, sensitive information leakage, unsafe output, and inappropriate content, the Company has established input and output barriers, content filtering, security testing, and monitoring measures that are appropriate to the risks. The Company implements identity authentication, minimum permissions, penetration testing, incident response, encryption and secure coding practices, vulnerability management, log auditing, and business continuity management based on AI risks. When significant vulnerabilities, out-of-control behaviors, or unacceptable risks are discovered, the Company has the right to immediately restrict, roll back, suspend, or deactivate the relevant AI systems.

4. Fairness and Prevention of Bias

When designing, developing, and using AI, the Company should avoid unfair, discriminatory, or exclusionary effects based on race, ethnicity, nationality, gender, age, disability, religion, health status, or other protected characteristics.

The Company should identify potential biases in training data, feature selection, labeling, model design, and application scenarios, and prioritize the use of sufficient, accurate, diverse, and representative datasets. For important scenarios that may affect personal rights and interests, subgroup performance testing, bias audits, and adverse impact assessment should be conducted, and corrective measures such as data correction, parameter adjustment, retraining, manual review, restricted use, or cessation of use should be taken based on the evaluation results.

5. Human supervision and intervention

The Company firmly believes that AI is a tool to assist decision-making. In highly sensitive and high-risk areas involving major business decisions, financial disclosures, quality and safety, talent evaluation, and life and health, the output of AI is used only as auxiliary reference. The Company promises to maintain an effective and documented Human-in-the-loop mechanism in the aforementioned critical business processes, ensuring that humans always have the final decision-making power to review, intervene, veto, and suspend the use of AI systems.

6. Transparency

According to applicable laws, regulations, and specific scenarios, the Company will use clear and easily recognizable methods to identify text, images, audio, and videos generated or substantially synthesized by AI, to avoid users mistaking AI-generated content for real person creations or objective facts. For AI-assisted decision-making that affects personal rights or key issues, the participation mode, main influencing factors, capacity limitations, and manual review arrangements of AI should be explained within a reasonable range, and necessary records such as system or model versions, important inputs, output results, manual review, and final decisions should be retained.

7. Responsibility and Accountability

The business leader is the first person responsible for specific AI scenarios, and is accountable for business purpose, legality, appropriateness, output usage, and impact management. The technical team is responsible for technical control of architecture, data, models, testing, deployment, monitoring, change, and exit. Functional departments independently review, supervise, and propose rectification requirements according to their responsibilities. AI does not assume legal or managerial responsibility; personnel who approve, develop, deploy, supervise, or use AI are responsible for their actions, decisions, and consequences. In addition, if AI is used in violation of regulations or has adverse effects due to inadequate management, the Company will pursue

accountability in accordance with internal accident management regulations.

8. Capability Boundary and Acceptable Use

The Company clarifies the scope of relevant users, data scope, capabilities and performance limitations, manual supervision requirements, abnormal escalation, suspension and exit conditions for each AI system. AI shall not intervene beyond the intended scope in key matters that should be independently judged by humans, and shall not be applied in high-risk and sensitive scenarios without control. Company employees are not allowed to connect AI to production systems, sensitive data sources, or tools that can perform high-impact operations without authorization. AI outputs that have not been manually verified shall not be directly used for external commitments.

9. Low Ecological Footprint and Green AI

The Company reduces the energy use, water use, carbon emissions, and hardware resource footprint of self-owned or third-party AI capabilities, model training, and inference while meeting safety, quality, compliance, and business requirements. When purchasing or selecting models, platforms, and data centers, the Company takes economic inputs, energy efficiency, carbon emissions and water resource information, equipment utilization rate, and other factors into evaluation. The Company prioritizes using smaller or more efficient models that match the task, reuse existing models, optimize call and cache, set training frequency and save strategies reasonably to avoid unnecessary repeated training and excessive computational power consumption.

10. Third Party and Procurement Management

Before introducing third-party AI models, platforms, agents, or development services, the Company should fully evaluate the compliance of AI systems to ensure that the AI system meets requirements during development and application, including data usage and retraining, data location and cross-border transfer, retention and deletion, network and data security, model capabilities and limitations, fairness, transparency, and other aspects.

The Company should specify data rights and usage restrictions, prohibition on unauthorized training, confidentiality and security measures, event notifications, service continuity, model or clause change notifications, etc. in third-party procurement contracts.

11. Continuous Monitoring and Improvement

The Company establishes appropriate performance, accuracy, robustness, fairness, security, availability, and resource efficiency indicators, and continuously monitors indicators covering performance degradation, abnormal output, and control failure capabilities. Significant changes in models, data, usage, interfaces, suppliers, or infrastructure should trigger reassessment, testing, and approval. Important or high-risk systems should be reviewed at least annually or in accordance with risk requirements.

Any person who discovers that AI has caused or may cause privacy breaches, security incidents, discrimination, false information, significant errors, out-of-control behavior, or other harm should immediately report through internal company event reports, compliance reports, or other reporting channels.

12. Prohibited AI Practices

The Company prohibits the development, procurement, use, or deployment of the following unacceptable AI systems or practices:

A. Using subconscious, manipulative, inducing, or deceptive techniques to substantially distort personal behavior and cause or potentially cause significant harm.

B. Exploiting, misleading, or improperly influencing individuals or specific groups by exploitation of vulnerabilities due to age, disability, or specific socio-economic conditions, thereby substantially distorting their behavior and causing or potentially causing significant harm.

C. Implementing social scoring and social ranking based on individual or group social behavior, personality traits, personal characteristics or inferential characteristics, resulting in unfavorable treatment or unreasonable

and disproportionate differential treatment in scenarios unrelated to the purpose of data collection.

D. Indiscriminately capturing Internet or CCTV images to establish or expand facial recognition databases.

E. Conducting real-time remote biometric recognition, facial recognition monitoring, or other biometric monitoring without legal authorization.

F. Other AI systems and practices that violate laws, regulations, fundamental rights, business ethics, or company policies.

13. Training and Awareness

The Company regularly conducts multi-dimensional training on AI literacy, AI risk, acceptable use, data privacy, cybersecurity, intellectual property, and event reporting based on roles and risks. Developers, approvers, supervisors, and high-risk scenario users receive specialized training that matches their responsibilities and is regularly updated.

14. Supplementary Provisions

This policy is interpreted and implemented by the Company's IT department.

This policy shall be reviewed at least once a year and revised in a timely manner when there are changes in legal regulation, company strategy, technical capabilities, risk environment, or major events.

Yihai Kerry Arawana Holdings Co., Ltd

September 16, 2026