Qisda

Artificial Intelligence Governance Policy

1. Purpose :

This Policy aims to provide foundational principles for the responsible development and use of artificial intelligence (AI) tools and services. By establishing a governance framework, Qisda Corporation (hereinafter referred to as the "Company") seeks to pursue the operational benefits and innovations brought about by AI, while mitigating potential threats to the trustworthiness, confidentiality, integrity, ethical use, and availability of digital assets

2. Scope :

This Policy shall apply to all employees, contractors, suppliers, outsourced vendors, partners, and authorized personnel participating in the Company's AI systems. It shall also apply to the development, testing, deployment, operations, change, and decommissioning of AI systems, as well as the use of third-party AI tools.

3. Responsibility :

Board of Directors Level: Responsible for approving the strategic direction of AI, overseeing significant AI-related risks across the Company, and ensuring the allocation of adequate human, technological, and financial resources.

AI Governance Committee : As a standing executive body, it is composed of the General Manager as Convener, the Chief Information Officer as Chair, the Chief Legal Officer, the Chief Risk Officer, and representatives from business units. Responsible for establishing and implementing the Company's AI governance framework, executing AI strategy, managing AI-related risks, reviewing significant AI initiatives, and overseeing compliance, information security, and data governance related to AI.

Authorized Users: Shall comply with this Policy and related codes of conduct, take responsibility for the AI-generated outputs they use, and proactively report any violations of the principles herein.

4. Glossary of term :

Artificial Intelligence (AI) System: A machine-based system that, for a given set of explicit or implicit objectives, infers from the inputs it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence real or virtual environments.

Generative AI: AI models designed to create new content (such as text, images, audio, video, or code) that resembles human-generated material.

Data Minimization: The collection of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

5. Flow Chart：

AI operations shall follow the lifecycle process below:

1. System Planning and Development： Define clear objectives and requirements; conduct secure development and deployment in accordance with SSDLC principles.
2. Access Control and Operation: Strictly regulate and manage access permissions based on the principle of least privilege.
3. Data Collection and Input: Process and input data with proper authorization, legitimate sources, and compliance with data quality requirements.
4. System Operations and Monitoring: Deploy in real-world environments with continuous monitoring of model validity drift and potential impacts.

6. Activities Description：

6.1 Legal and Regulatory Compliance：

The Company is committed to complying with the Artificial Intelligence Basic Act, the EU AI Act, the EU General Data Protection Regulation [GDPR]) and relevant industry regulatory guidelines.

6.2 Risk Management and Classification Mechanism：

The Company classifies AI applications into four risk levels for management purposes, in reference to international regulations:

6.2.1 Unacceptable Risk: The following practices are explicitly prohibited pursuant to the EU AI Act: (1) behavioral manipulation exploiting cognitive vulnerabilities or subliminal techniques; (2) social credit scoring; (3) unauthorized real-time biometric identification

(e.g., facial recognition); (4) malicious exploitation of system vulnerabilities.

6.2.2 High Risk: Applications such as recruitment screening and credit assessment require independent validation and continuous monitoring.

6.2.3 Limited Risk: Applications such as chatbots must fulfill transparency disclosure obligations.

6.2.4 Minimal Risk: Applications such as spam filtering may be used freely.

6.3 Core Governance Principles

6.3.1 Human-Centricity and Autonomy: AI shall augment human capabilities rather than replace them. Significant decisions must retain effective and fully documented human control (Human-in-command), monitor (Human-on-the-loop), intervene, or escalate mechanisms, ensuring personnel retain the authority to approve or shut down systems (Human-in-the-Loop).

6.3.2 Transparency and Explainability: AI decision-making processes shall provide stakeholders with understandable explanations. In terms of transparency, when using generative AI to assist in business activities, the fact that the interacting party is an AI system, along with its capabilities, limitations, reference data sources, and potential risks, shall be appropriately disclosed. Where user rights are affected, channels for inquiry, appeal, correction, or assistance shall be provided.

6.3.3 Security and Robustness: Measures shall be established to defend against adversarial attacks and ensure that AI systems continue to function correctly when encountering erroneous inputs. Additionally, cybersecurity measures shall be implemented, including penetration testing, incident response, and encryption technologies, to protect AI systems from unauthorized access, data theft, and malicious attacks.

6.3.4 Fairness and Non-Discrimination: Biases in training data shall be monitored and corrected, bias audits shall be conducted, and data diversity shall be ensured. Upon detection of bias, corrective measures shall be initiated, with manual review, appeal, or correction procedures provided as necessary. Where sensitive attributes are involved, principles for use and control shall be established to prevent unreasonable differential treatment.

6.3.5 Privacy Protection: In accordance with the guidelines of Artificial Intelligence Basic Act, the EU AI Act, the EU General Data Protection Regulation [GDPR]) and relevant industry regulatory guidelines, privacy protection shall be strictly enforced. The lifecycle of AI systems shall adhere to the principles of data minimization, purpose limitation, lawful use, and necessity. Where personal data is involved, data protection shall be implemented throughout the processes of collection, processing, use, storage, transmission, and deletion. Confidential data shall not be entered into external AI tools or third-party platforms without authorization.

6.3.6 Clear Boundaries and Accountability: AI applications shall define clear boundaries regarding authorized scope, data use, and user responsibilities. AI systems shall be traceable, enabling the tracking of data sources, key configurations, inputs and outputs, and manual review records , and specific roles shall be designated to assume responsibility. In the event of a security incident or significant anomaly, the process for reporting, investigation, and corrective prevention shall be followed.

6.3.7 Environmental Sustainability: The Company requires its own and third-party AI data centers and model service providers to strive to reduce energy consumption and carbon emissions associated with AI computing.

6.3.8 Common Good and Well-Being: The Company shall strive to achieve a balance of interests and shared well-being among humanity, society, and the environment, and shall be committed to cultural diversity, social inclusion, and environmental sustainability, with the aim of fostering an AI-enabled society that safeguards human physical and mental well-being, promotes the interests of all people, and enhances the overall environment.

6.4 AI System Lifecycle Management

AI systems shall be subject to controlled management throughout their entire lifecycle, from requirements definition to decommissioning, in compliance with policies, regulations, Responsible AI principles, and risk management requirements.

6.5 Annual Review

This Policy shall be reviewed at least annually, and updated as necessary to reflect changes in legal requirements, business operations, and the threat landscape.

6.6 Penalties

Violations of this Policy shall be subject to disciplinary actions in accordance with

Qisda

Company regulations.

Non-compliance by third parties shall be addressed in accordance with contractual agreements.

7. Authority of Document Revised：

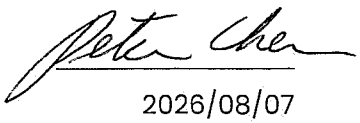
The scope of governance under this Policy covers Qisda and its subsidiaries, suppliers, contractors, and business partners. Upon being signed by the Chairman on behalf of the Company, this Policy shall be implemented by the AI Governance Committee, with the Board of Directors serving as the highest-level decision-making and governance body.

This Policy shall take effect upon approval by the Board of Directors. The same procedure shall apply to any amendments thereto.

This Policy was established on August 7, 2026.

Chairman

Peter Chen



2026/08/07