

Artificial Intelligence (AI) Governance Policy

2026/9/22

Article 1: Purpose

This Policy is established by Flytech Technology Co., Ltd. (the "Company") to ensure that the Company's use of artificial intelligence (AI) across product development, manufacturing, operations, and services balances innovation with effective risk management, and complies with applicable laws, regulations, and ethical standards.

This Policy sets out a structured AI governance framework that promotes transparency, controllability, and accountability in the use of AI, and helps prevent operational, regulatory, cybersecurity, and reputational risks arising from the misuse or failure of AI technologies. The framework is informed by the principles of the AI guidelines issued by Taiwan's Financial Supervisory Commission (FSC), as well as international standards, including ISO/IEC 42001 and ISO/IEC 27001.

Through the responsible adoption of AI, the Company aims to enhance operational efficiency, strengthen product competitiveness, and advance its digital transformation in support of its long-term business strategy.

Article 2: Scope

This Policy applies to all departments and employees of the Company and its subsidiaries, as well as to third parties that do business with the Company, including but not limited to contractors, consultants, system integrators, and suppliers.

The use of any AI technology in business operations, including systems developed in-house or sourced externally (such as machine learning models, generative AI tools, image recognition systems, or API-based services), shall comply with this Policy.

Article 3: Organization and Governance Structure

3.1 Final Approval Authority

The Chairman serves as the final approval authority for AI governance. The Chairman makes final decisions on AI-related strategies and policies, ensures the overall effectiveness of AI risk management, and aligns AI-related resource allocation with the Company's sustainability goals.

3.2 Chief Oversight Authority

The President serves as the chief oversight authority for AI governance. The President reviews and endorses AI-related strategies and policies, oversees the overall effectiveness of AI risk management, and ensures that AI-related resource allocation aligns with the Company's sustainability goals.

3.3 AI Governance Task Force

The Company has established the AI Governance Task Force as a dedicated review body.

- (a) Convener: The President or a project lead designated by the President.
- (b) Core Members: The Director of Information Technology (responsible for technology and cybersecurity), the Director of Legal Affairs (responsible for legal and regulatory compliance), and the Head of Internal Audit (responsible for risk assessment).
- (c) Responsibilities: The Task Force is responsible for:

- developing and revising AI governance policies and management procedures;
 - establishing AI risk classification and assessment methodologies;
 - reviewing high-risk AI use cases; and
 - overseeing AI model lifecycle management and the implementation of governance procedures.
- (d) Reporting: The Task Force shall report on the effectiveness of AI governance to the President, or a person designated by the President, on a quarterly basis. Any material AI-related incident shall be reported immediately.

3.4 AI Technical Support and Security Team

The AI Technical Support and Security Team is an operational unit established within the Information Technology Division. The Team is primarily responsible for evaluating the security of AI tools, building a secure internal AI platform, and submitting matters that require review, together with supporting evidence, to the AI Governance Task Force.

- (a) Responsibilities: The Team is responsible for:
1. implementing AI technologies and building the AI platform;
 2. managing AI models and establishing technical standards;
 3. promoting AI use cases and driving cross-departmental integration;
 4. establishing mechanisms to embed the AI platform into day-to-day operations;
 5. supporting risk assessment and monitoring; and
 6. managing the AI platform, which shall comply with information security (ISO/IEC 27001) and AI governance requirements and serve as the Company's sole official platform for AI applications. As a centralized control mechanism, the platform provides the following functions:
 - AI model deployment and version control
 - API management and access control
 - Usage logging and audit trails
 - Data security and access permission management
 - Generative AI security controls
- (b) AI Competency and Training: The Information Technology Division shall work with the Human Resources Division to establish a tiered AI competency development program, and to plan and deliver company-wide AI training for management, technical staff, and general employees, in order to strengthen AI skills and risk awareness. The two divisions shall also establish an AI talent development framework and an AI competency assessment and certification program to ensure that employees use AI appropriately and safely.
- (c) Reporting: The Team shall report to the AI Governance Task Force through quarterly working meetings and shall report any material incident immediately.

Article 4: AI Governance Operating Model

The Company's AI governance operating model establishes a consistent approach and control process for the adoption, development, and management of AI applications, ensuring that they remain under effective control and can be sustained over the long term.

Under this model, the Company shall implement a phased management mechanism that guides AI applications from innovation and experimentation through to full deployment. AI applications progress through three stages: Proof of Concept (PoC), Pilot, and Production. Each stage has its own review and control requirements, which the Company shall clearly define, including:

- Objectives and validation criteria
- Risk assessment and control measures
- Review and approval authority
- Go-live and monitoring requirements

This operating model ensures consistency, traceability, and effective risk management throughout the AI lifecycle, from development to deployment.

Article 5: AI Governance Principles

When adopting, developing, deploying, and using AI systems, the Company shall act prudently and responsibly and adhere to the following principles to ensure that its use of AI meets corporate governance, risk management, and regulatory requirements:

5.1 Legal Compliance

The use of AI shall comply with applicable laws and regulations, including those governing personal data protection, intellectual property, and data use. The Company shall ensure that all data is collected and used on a lawful basis, and shall not use data obtained from illegal sources or without proper authorization.

5.2 Human Oversight

AI systems shall be used to support, not replace, human decision-making. Decisions that have a significant impact on the Company's operations, product quality, customer interests, or regulatory compliance shall not be made by AI systems without appropriate authorization or human review. For high-risk AI applications, final review and decision-making authority shall remain with designated personnel to ensure that decisions are sound and accountability is clearly assigned.

5.3 Fairness and Bias Mitigation

AI models shall be designed to avoid biased or discriminatory outcomes arising from training data or algorithm design, including algorithmic bias that could infringe on human rights in employee recruitment, performance evaluation, or supply chain management. The relevant departments shall regularly review AI outputs for fairness and consistency, and make adjustments or corrections as necessary.

5.4 Data Minimization

AI systems shall collect, process, and use only the data necessary to perform specific tasks. Controls shall be established over the use and transmission of confidential company information, personal data, and customer data to prevent data leakage or misuse through unauthorized external AI tools.

5.5 Transparency, Explainability, and Accountability

In business processes involving AI, the scope of use, functional limitations, and decision-making role of AI shall be clearly identifiable. Significant decisions and high-risk applications shall be supported by an appropriate level of explainability, so that relevant personnel can understand the basis for AI-generated outputs. Accountability for AI systems and their outcomes shall be clearly assigned to designated personnel, so that any errors or disputes can be traced, addressed, and remediated.

5.6 Traceability

The Company shall maintain comprehensive records and management mechanisms for AI operations to ensure that AI-supported decision processes are traceable and auditable.

5.7 Risk-Based Management

AI systems shall be classified by risk level according to their intended use and scope of impact, with management and control measures applied accordingly. Higher-risk systems shall be subject to more rigorous review, monitoring, and

oversight to ensure that their operation remains within the Company's risk tolerance.

5.8 Security and Reliability

AI systems shall undergo appropriate testing, validation, and monitoring to ensure secure and reliable operation, and to prevent system errors, malfunctions, or external attacks from disrupting the Company's operations.

5.9 Responsible AI

The Company's use of AI shall follow the principles of Responsible AI, ensuring that AI technologies are developed and used in line with business ethics, regulatory requirements, and social responsibility. All AI-related activities shall balance technological innovation with risk management, and avoid causing undue harm to individuals, customers, or society.

Article 6: AI Governance Development Roadmap

The Company shall advance AI governance in phases, based on operational needs, technological developments, information security considerations, and the AI governance principles set out in this Policy, in order to progressively enhance governance maturity and AI adoption.

The development roadmap consists of three phases: short term (adoption and inventory), medium term (institutionalization), and long term (continuous improvement). The Information Technology Division shall lead and coordinate the implementation of the roadmap.

The risk level of each AI application shall be determined according to its potential impact on operations, regulatory compliance, customer interests, and information security.

Article 7: Risk Classification, Assessment, and Model Lifecycle Management

7.1 Risk Classification

The Company shall establish a consistent AI risk classification system. AI applications shall be classified as high, medium, or low risk based on their potential impact on operations, regulatory compliance, information security, and corporate reputation, with differentiated management measures applied to each level. High-risk AI applications shall also be subject to rigorous review and monitoring, including mandatory pre-deployment risk assessment, review by the AI Governance Task Force, human review, and periodic revalidation.

(a) High Risk

- Definition: An AI application is classified as high risk if errors, bias, failures, tampering, or misuse related to the application could directly or significantly affect personal safety, product quality, critical operations, the material interests of customers or employees, regulatory obligations, confidential data, or the Company's reputation; or if it directly triggers actions that are significant, irreversible, or difficult to remedy.
- Examples: Product release or nonconformance decisions, production equipment safety interlocks, automated control of R&D or manufacturing process parameters, decisions that deny customer eligibility or revoke customer rights, automated generation and submission of statutory filings, and direct execution of high-privilege cybersecurity responses.

(b) Medium Risk

- Definition: An AI application is classified as medium risk if it primarily provides recommendations, forecasts, classifications,

summaries, or process support, and its outputs may affect departmental operations, customer service, financial decisions, or management judgment, while effective human review and override mechanisms remain in place before any significant or irreversible action is taken.

- Examples: Sales forecasting, predictive maintenance alerts, quality anomaly detection, suggested customer service responses, internal staff scheduling recommendations, supplier risk ranking, internal document analysis, and first drafts of legal or procurement documents.

(c) Low Risk

- Definition: An AI application is classified as low risk if it is used only for general productivity tasks, content organization, or low-impact assistance, where errors would not materially affect safety, product quality, the material interests of customers or employees, regulatory obligations, critical operations, or the Company's reputation, and where outputs can be easily reviewed, corrected, or discarded.
- Examples: Meeting note summarization, summaries of public information, general translation and copyediting, first drafts of presentations, informal brainstorming, drafts of public marketing materials, and code formatting or test data generation.

7.2 Model Lifecycle Management

All AI systems shall be subject to comprehensive AI model lifecycle management. The lifecycle shall cover all stages from requirements planning to model retirement, including data collection and processing, model design and development, testing and validation, production deployment, and operational monitoring.

7.3 Three Lines of Defense

The Company adopts the Three Lines of Defense model for internal control to manage AI-related risks.

- (a) The first line of defense consists of the business units that use AI. These units shall ensure that AI is used in compliance with applicable requirements and shall be responsible in the first instance for the appropriateness of input data and the reasonableness of outputs.
- (b) The second line of defense consists of Legal Affairs, Information Technology management, and Risk Management. It is responsible for establishing AI governance procedures, conducting risk assessments, designing control measures, and reviewing high-risk AI applications. It also provides independent compliance and information security oversight of the first line, including the AI platform and applications developed by the Information Technology Division.
- (c) The third line of defense is the Internal Audit function, which shall periodically review the implementation and effectiveness of the AI governance framework and recommend improvements.

Article 8: Acceptable Use of AI

8.1 General Requirements

The use of AI shall comply with the following requirements, and users shall be accountable for their use of AI and its outcomes:

- (a) Confidential information, customer data, and non-public information shall not be entered into unapproved platforms.
- (b) AI outputs shall be evaluated for accuracy, reasonableness, and risk of bias, and shall undergo appropriate human review.
- (c) Appropriate controls shall be applied to AI-generated content to prevent misuse or the spread of misleading information.
- (d) The use of generative AI systems shall be subject to information security monitoring and logging.

8.2 Data Protection and Anonymization

Where the development or operation of AI models involves personal data or confidential company information, appropriate anonymization, de-identification, or masking measures shall be applied so that the data cannot be traced to specific individuals or directly reveal confidential information. Sensitive data that has not been processed in this way shall not be used for model training or entered into external AI services.

8.3 AI Content Transparency

The Company shall ensure that content generated by AI, or created with the assistance of AI, is identifiable as such where appropriate.

8.4 AI Content Labeling

AI-generated content that is provided externally or may influence decision-making shall be disclosed or labeled in a manner appropriate to its nature, including but not limited to annotations, system labels, or other technical measures (such as watermarks or identification tags), so that recipients do not mistake it for content produced entirely by humans.

8.5 Protection of Confidential Information

When using AI systems, employees and partners shall comply with the Company's AI usage policies and information security requirements, and shall act prudently and in good faith. Employees and partners shall not enter confidential company information, customer data, technical documents, or trade secrets into unapproved external AI systems, particularly public generative AI platforms, in order to prevent information leakage.

8.6 Use of Generative AI Outputs

Outputs from generative AI shall be used for reference only and shall not be incorporated directly into official external documents, customer communications, or significant decisions without human review. Users shall verify and correct AI-generated content as necessary to ensure its accuracy and legal compliance.

8.7 Outsourcing and Procurement of AI Services

When outsourcing or procuring AI services, the responsible department shall clearly specify in the contract the scope of services, data usage rights, information security responsibilities, confidentiality obligations, and liability for breach. The department shall also assess the supplier's risk management capabilities, and require the supplier to warrant that its training data and model outputs do not infringe third-party intellectual property rights and to indemnify the Company against any related claims, in order to reduce the Company's exposure to infringement claims arising from the use of such services. If the supplier cannot provide such warranties, the department shall implement appropriate risk mitigation measures or restrict the scope of use.

In addition, the responsible department shall encourage suppliers to prioritize cloud service providers that use renewable energy or operate energy-efficient infrastructure, in line with Green AI practices, to support the Company's Scope 3 emissions reduction and net-zero pathway.

Article 9: AI Incident Management

When an AI system experiences an anomaly during operation, such as erroneous predictions, significant bias, abnormal decision outcomes, or a suspected data breach, the relevant department shall immediately report the incident through the Company's internal reporting channels to department management and to the relevant functions, including Information Technology, Information Security, and Risk Management.

The Company shall establish emergency shutdown (kill switch) and manual takeover procedures for high-risk AI systems. Where necessary, the affected AI system shall be shut down immediately to contain the impact.

A root cause analysis shall then be conducted to determine whether the issue resulted from poor data quality, model design flaws, system malfunctions, or human error. Based on the findings, corrective actions, such as model retraining, data cleansing, strengthened controls, or process adjustments, shall be developed and their effectiveness monitored.

If the incident has had a significant impact on the Company's operations, product quality, or customer interests, or involves regulatory risk, it shall be reported to the AI Governance Task Force and, where appropriate, escalated to the Board of Directors.

Article 10: AI Management System

The Company shall establish a formal AI management system (AIMS) and progressively align it with ISO/IEC 42001 to ensure that AI governance is consistent, traceable, and capable of continual improvement.

The AIMS shall cover policy management, procedure development, risk assessment, control measures, performance monitoring, and continual improvement, and shall be refined on an ongoing basis through the Plan-Do-Check-Act (PDCA) cycle.

The Company shall retain AI-related documentation and records, including model design documents, test reports, change logs, and decision rationale, to support internal management and external audit requirements.

Article 11: Information Security Integration

The Company's AI systems shall be fully incorporated into the scope of its information security management system (ISMS) to ensure compliance with the information security controls required under ISO/IEC 27001. AI-related assets, including datasets, models, system platforms, and APIs, shall be included in asset inventories and risk assessments, and protected through access control, encryption, and privilege management measures appropriate to their criticality.

For AI models that are externally sourced or open source, the Company shall require suppliers to provide a software bill of materials (SBOM) or conduct regular scans for open-source vulnerabilities to mitigate the risk of supply chain attacks. Preventive and detective controls shall also be established to address AI-specific risks, such as training data leakage, model tampering, API abuse, and prompt injection attacks.

The Company shall implement a tiered monitoring framework:

- Routine monitoring shall be conducted in real time or daily, focusing on AI outputs and system behavior.
- Periodic reviews shall be conducted at least quarterly to evaluate model performance and security.
- Internal audits shall be conducted at least annually to verify the completeness and effectiveness of AI governance and security controls.

In the event of an AI-related information security incident, the Company shall immediately activate its information security incident response procedures, including reporting, containment, and recovery, and shall notify the AI Governance Task Force as appropriate.

Article 12: Monitoring, Recordkeeping, and Audit

12.1 AI Governance Maturity Management

The Company shall establish a mechanism for assessing AI governance maturity and periodically review the maturity of its AI applications, controls, and management systems. The assessment results shall inform policy and process improvements, resource allocation, and strategic adjustments, with the aim of continually strengthening the Company's AI governance capabilities.

12.2 AI Monitoring and Recordkeeping

The Company shall establish a comprehensive monitoring mechanism to continuously track the operation of each AI system, including its accuracy, error rates, abnormal outputs, and changes in how it is used. Monitoring intensity shall be proportionate to risk level. High-risk AI systems shall be subject to real-time monitoring and human review; medium-risk systems shall be evaluated periodically; and low-risk systems may be monitored through sample-based checks.

All records related to AI operations, including model versions, input and output logs, decision processes, and anomalies, shall be retained to ensure traceability and support future audits.

12.3 Internal Audit

The Internal Audit function shall periodically review the implementation of these mechanisms and recommend improvements to address any deficiencies.

Article 13: Oversight and Reporting

To strengthen oversight of AI risks, the AI Governance Task Force shall report on AI governance matters to the President, or a person designated by the President, at least quarterly. In the event of a material incident, such as an AI system failure, a regulatory violation, or an event with a significant impact on operations, the Task Force shall report it immediately and activate the appropriate response procedures.

Article 14: Implementation and Amendment

This Policy shall take effect upon approval by the Chairman. It shall be reviewed at least annually, and amended as necessary, to ensure that it remains appropriate in light of regulatory changes, technological developments, and the Company's evolving operational needs.

Detailed implementation rules shall be established separately following the approval of this Policy. Any matters not addressed in this Policy shall be governed by applicable laws and regulations and the Company's other internal policies.