CTCI 中鼎工程股份有限公司
CTCI Corporation

Responsible Artificial Intelligence Policy Statement

(This Statement shall be issued and implemented upon approval by the Information Security Promotion Committee)

Policy Purpose and Scope

CTCI Corporation (hereinafter referred to as the "Company") is committed to promoting the responsible application of artificial intelligence ("AI") in engineering services and corporate operations to enhance engineering quality, operational efficiency, innovation capabilities, and overall service value. The Company will continue to monitor developments in domestic and international AI governance trends, relevant laws and regulations, and industry practices. Where applicable, the Company will prudently adopt and reasonably apply AI technologies in accordance with the principles of corporate governance, regulatory compliance, and risk management, thereby supporting digital transformation and sustainable corporate development.

Governance Framework and Accountability System

The Company shall promote the allocation of responsibilities and management mechanisms for AI applications based on its existing frameworks for corporate governance, internal control, information security, and risk management. The Group Research and Innovation Center shall be responsible for the formulation, maintenance, and periodic review of this AI Policy document and may, as appropriate, propose revisions in light of developments in AI technologies, laws and regulations, and practical applications.

Relevant business units and personnel shall, within the scope of their respective duties, bear corresponding responsibility for the adoption, use, management, and outputs of AI tools and shall ensure that such applications comply with Company policies, laws and regulations, contractual requirements, and corporate ethics. Where AI applications result in errors, material harm, or legal liability, the matter shall be investigated and accountability shall be determined in accordance with the Company's existing allocation of authority and responsibility and rules governing rewards and disciplinary actions.

AI application cases involving significant risks, cross-unit applications, or uncertainty regarding the attribution of responsibility shall be submitted to the Information Security Promotion Committee. The Committee shall, based on the circumstances of each case, conduct deliberations, make determinations, and set forth any necessary management requirements.

The Company shall also continuously review the appropriateness of relevant governance measures in light of developments in AI technologies and practical applications.

Implementation Scope and Boundary Management

The Company shall prudently define the scope of use and operational boundaries of AI applications based on their purposes, contexts of use, data types, and levels of risk. Relevant units shall, based on business needs, project characteristics, and management requirements, clearly define the authorized scope of use, permitted functions, restrictions on data use, applicable contexts for outputs, and circumstances in which AI shall not be used. Based on these definitions, allowed use policies, guardrails, functional and capability restrictions, and control points requiring human intervention or escalation shall be established to distinguish among circumstances in which AI may be used to assist in performing tasks, circumstances requiring human confirmation, and circumstances in which AI should not be used.

The scope of use and operational boundaries of each AI application shall be proposed by the unit introducing or using the application based on actual needs and shall, in accordance with the Company's rules on authority and responsibility, be submitted to the relevant units with authority and responsibility for deliberation, confirmation, or filing for record, as applicable. The scope of AI applications shall be reviewed as appropriate in light of technological developments, legal and regulatory requirements, and the Company's management needs. Where the scope of use is expanded, the scope of data is changed, functions are adjusted, or the level of risk increases, the application shall be reassessed and the necessary review procedures shall be completed to ensure that its use is within the authorized scope and complies with governance principles and compliance requirements.

Compliance Standards and Prohibited AI Practices

The Company prohibits the use of AI for activities that violate laws and regulations, Company policies, contractual obligations, or ethical principles. The adoption and application of AI technologies shall comply with Taiwan's Artificial Intelligence Basic Act, the European Union's General Data Protection Regulation (GDPR) and Artificial Intelligence Act (EU AI Act), as well as other applicable laws and regulations and the Company's internal policies.

AI technologies shall not be used to infringe upon individual rights and interests, compromise information security, circumvent internal controls, manipulate or mislead others, exploiting vulnerabilities, engage in improper surveillance, perform unauthorized biometric surveillance, conduct social scoring, or for other purposes that may harm the public interest, the Company's reputation, or the rights and interests of stakeholders.

Relevant personnel shall use AI technologies prudently in accordance with Company policies and within the authorized scope, ensuring that such use adheres to the principles of responsible, compliant, and trustworthy AI use.

Principles of Data Privacy Protection and Data Governance

The Company places great importance on safeguarding personal data, trade secrets, confidential information, and intellectual property rights. The use of AI technologies shall comply with applicable laws and regulations, contractual obligations, the Company' s information security requirements, and data governance principles. For example, where the collection, processing, or use of personal data is involved, such activities shall comply with the applicable provisions of Taiwan's Personal Data Protection Act.

Where the Company's business information, customer data, project information, confidential data, or content involving intellectual property is involved, authorized systems that meet the Company's management requirements or tools approved by the Company shall be used. Throughout the lifecycle of AI development, deployment, application, and data processing, including the stages of data collection, input, processing, storage, use, output, sharing, retention, and deletion, relevant personnel shall carefully assess the use scenarios, data sensitivity, access controls, and data processing methods to mitigate the risks of data leakage, unauthorized use, improper use of models, or infringement of rights.

Information Security and System Protection Mechanisms

The adoption and application of AI technologies shall be aligned with the Company's "Information Security Policy Statement" and relevant information security management requirements, with due consideration given to system stability, data security, and operational reliability. In accordance with such statement, the Company has established an information security management system based on the requirements of the ISO 27001 information security management standard, with safeguarding information security, enhancing employees' information security awareness, continuously improving the information security management system, and complying with relevant laws and regulations, Company policies and requirements, and contractual requirements as essential management priorities.

Based on the actual use scenarios of AI applications, data sensitivity, and the potential impact of associated risks, the Company shall implement appropriate management, review, and security measures, including but not limited to access controls, identity authentication, retention of usage logs, system monitoring, data protection, encryption, incident response, vulnerability assessments, and penetration testing where necessary, in order to mitigate the risks of unauthorized access, data leakage, system abuse, model misuse, or other potential information security risks.

Access controls for AI systems and related information assets shall be clearly defined based on work-related needs. Relevant access control requirements shall be communicated to system service providers to facilitate the implementation of effective access control mechanisms and, in conjunction with audit mechanisms, reduce the risk of unauthorized access to systems.

In the event of an AI-related information security incident, the incident shall be promptly reported, necessary

incident response measures shall be taken, and mechanisms for learning from incidents shall be established to mitigate the damage caused by such incidents.

AI systems involving critical business operations shall have appropriate backup plans established and implemented to enable operations to be restored within an acceptable timeframe in the event of a system interruption or failure, thereby ensuring the timely resumption of critical business operations.

Through the foregoing measures, the Company shall ensure that AI applications comply with its overall security management requirements.

Fairness Principles and Bias Management

The Company supports the principles of fairness, inclusion, and respect for diversity. The adoption and application of AI technologies shall avoid inappropriate bias, differential treatment, or discriminatory impacts and shall, to the extent reasonably practicable, take into consideration their potential impacts on employees, customers, business partners, and other stakeholders.

When developing, training, or fine-tuning AI models, or introducing or using AI applications, each business unit shall, based on the purpose, degree of impact, and level of risk, identify, to the extent reasonably practicable, whether the input data, model outputs, or application results may give rise to unfair, biased, or discriminatory impacts. The Company may, taking into account the purpose, degree of impact, level of risk, actual needs, or other relevant factors, conduct necessary audits. Such audits may include assessing whether data sources and use scenarios are appropriate, whether outputs may cause unreasonable adverse impacts on specific individuals or groups, and whether the application process retains necessary mechanisms for human judgment, review, or correction.

Where concerns relating to fairness, non-discrimination, inclusion, or stakeholder rights and interests arise in connection with AI applications or related data, relevant responsible departments may be consulted as necessary to assist in the assessment. Based on the assessment results and practical needs, each business unit may make appropriate adjustments, restrict use, add human review, implement improvement measures, or retain relevant records to mitigate potential risks of unfairness and discrimination and to maintain fairness and trust in AI applications.

System Transparency and Explainability Principles

The Company values transparency and understandability in AI applications. The adoption and use of AI technologies shall, to the extent reasonably practicable, enable relevant personnel to understand their purposes, applicable use scenarios, authorized scope of use, primary functions, capabilities and limitations, and potential risks, so as to avoid inappropriate expectations regarding or over-reliance on AI-generated outputs or AI-assisted judgments, as well as use beyond the originally intended purposes.

For AI applications that have an impact on employees, customers, business partners, or other stakeholders, appropriate transparency measures shall be implemented based on their purposes and degree of impact. Such measures may include, where appropriate, clearly informing users that they are interacting with AI rather than a human, and indicating that content has been generated by or with the assistance of AI. Depending on the purpose, degree of impact, and technical feasibility of the AI application, the Company may, to the extent reasonably practicable, provide appropriate and readily understandable explanations. Depending on the actual circumstances and the needs of each case, such explanations may, as appropriate, include the rationale on which the outcome is based, material assumptions, key influencing factors, applicable conditions, limitations or uncertainties of the outcome, matters requiring further human judgment, verification, or supplementation, and other relevant information that helps users understand the outcome.

Human Autonomy and Decision-Making Oversight Mechanisms

AI technologies shall serve as tools to support decision-making, enhance efficiency, and assist professional judgment, and shall not replace the responsibilities of relevant personnel to perform the reviews, confirmations, approvals, or professional judgments required under their respective duties.

For AI applications involving engineering design, project execution, risk assessment, contractual obligations,

or other important business decisions, a Human in the Loop (human oversight) mechanism shall be adopted. Depending on the level of risk, different levels of human oversight, including human-in-the-loop, human-on-the-loop, or human-in-command, shall be incorporated to ensure effective, documented human oversight, while retaining professional review and final confirmation procedures.

Relevant responsible personnel shall, in accordance with the Company's authority and responsibility framework and practical needs, perform necessary reviews and exercise professional judgment with respect to AI-assisted outputs, and shall remain accountable for the final decisions. Where necessary, records relating to the use of AI-assisted decision-making, human oversight, review processes, and confirmation results shall be retained to ensure operational quality, safety, and reliability.

Environmental Sustainability and Ecological Footprint Management

The application of AI technologies shall contribute to enhancing engineering quality, operational efficiency, resource utilization efficiency, and overall service value, thereby supporting sustainable corporate development.

In the development, adoption, procurement, or use of AI technologies, the Company will, to the extent reasonably practicable, consider energy efficiency, environmental impacts, and suppliers' sustainability practices.

When evaluating third-party AI services or related technology solutions, the Company shall, to the extent reasonably practicable, consider factors such as energy efficiency, computing resource utilization, reduction of ecological footprint, and supplier sustainability performance as part of an overall assessment, in support of the principles of green engineering and environmental sustainability.

T.C. Li	J.S. Chung	Anthony Hsu	William Pung	Yu-Hung Su
EMO	HBO	IEPBO	ATFBO	EPCO
President	President	President	President	President

M.S. Lee
President
(CISO iterim)

Issue Date:2026/08/27