

Taiwan Mobile Responsible Artificial Intelligence Governance Principles

Established by the Board of Directors on August 5, 2026

Article 1 Purpose

To ensure that the development, procurement, deployment and use of artificial intelligence (AI) technologies comply with the requirements of corporate governance, cybersecurity, privacy protection, human rights, ethics and sustainable development, Taiwan Mobile Co., Ltd. (the “Company”) hereby establishes these Principles.

While advancing AI innovation and digital transformation, the Company shall identify, assess and manage the risks that AI may pose to individuals, customers, employees, business partners, society and the environment, and shall establish a trustworthy, responsible and human-centered AI governance mechanism.

Article 2 Scope of Application

These Principles apply to the Company and its affiliates that are subject to the Company's governance and management.

The entities and persons covered by the preceding paragraph include all employees of the Company and its affiliates. Where suppliers, contractors, commissioned entities, successful bidders, legal entities, organizations or individuals cooperating with the Company use AI in performing work commissioned by the Company, the responsible project unit shall require them to comply with the relevant requirements of these Principles through contractual provisions or other written arrangements.

The AI systems covered by these Principles include AI models, systems, platforms, tools, applications and related services that are independently developed, jointly developed, outsourced for development, procured, introduced, integrated or used by the Company or by a commissioned third party.

The management scope described in the preceding paragraph shall cover the entire lifecycle of an AI system, including:

1. Requirements planning and assessment of intended use.
2. Data collection, acquisition, processing and governance.
3. Model design, development and training.
4. Testing, validation and pre-deployment review.
5. Deployment, use and access management.
6. Ongoing monitoring, maintenance and improvement.
7. Deactivation, retirement and data disposition.

Article 3 Governance Principles

The development, procurement, introduction, deployment and use of AI by the Company shall comply with the following principles.

1. Sustainable Transformation and Co-prosperity

The Company shall proactively monitor AI trends and technological developments, introduce appropriate AI applications based on business needs, and promote process redesign, operational optimization,

service innovation , and the enhancement of organizational capabilities to create long-term value for the Company and its stakeholders.

When using AI, the Company shall balance environmental, social and governance (ESG) objectives, and assess impacts on labor rights, digital equity, information accessibility, social inclusion and other public interests, so as to prevent AI adoption from exacerbating existing inequalities or causing unreasonable exclusion through the introduction of AI.

The Company shall also assess the energy consumption, water usage, carbon emissions and other environmental impacts of AI models, computing resources and related data centers, reduce the ecological footprint generated by AI systems and models throughout their lifecycle, continuously improve model and computing efficiency, and prioritize energy-efficient equipment, low-carbon infrastructure and renewable energy in implementation of the low ecological footprint principle.

When procuring or using third-party AI systems or related services, the Company shall, depending on the associated risks and materiality, require third-party providers to maintain low ecological footprint management mechanisms, and shall incorporate suppliers' environmental impacts, resource efficiency, low ecological footprint management capabilities and sustainability management capabilities into its assessments.

2. Accountability and Human Autonomy

AI systems shall serve as tools to support, assist or improve the quality of decision-making, and shall not replace the ultimate responsibility borne by personnel pursuant to applicable laws and regulations, corporate governance requirements or assigned business authorities.

For critical decisions involving material operations, finance, personnel, customer rights and interests, credit, privacy, safety or other high-risk matters, the Company shall keep humans in the loop by retaining appropriate and effective human oversight, human review and final decision-making authority shall be retained. AI shall not independently make irreversible final decisions or final decisions with material impacts.

Based on the intended use and risks of an AI system, the Company shall clearly define business responsibilities, technical responsibilities, data responsibilities, risk management responsibilities, and approval authorities.

Authorized personnel shall have the capability and authority to review, intervene in, verify, modify, override, suspend, terminate or escalate an AI system or its outputs.

The Company shall establish mechanisms for reporting, investigating, improving, remedying and tracking accountability for errors, inappropriate outcomes, harm or other negative impacts caused by AI systems.

3. Security and Robustness

Throughout the entire lifecycle of an AI system, including the use and development of AI, the Company shall implement information security, cybersecurity and business continuity management measures commensurate with the level of risk.

Such measures may include identity authentication, access management, access control, data encryption, vulnerability management, security testing, model safeguards, anomaly detection, redundancy mechanisms, incident reporting and emergency response.

The Company shall protect against data poisoning, prompt injection, malicious commands, unauthorized access, model tampering, leakage of confidential information, system misuse and other threats that may affect the security and trustworthiness of AI systems.

Before deployment, an AI system shall undergo necessary security, stability, accuracy and performance testing. After deployment, the Company shall continuously monitor its operating status, output quality, anomalous behavior, model drift and performance degradation.

Where an AI system experiences a material anomaly, failure or attack, exceeds the acceptable risk threshold, or may cause material impacts, the Company shall promptly take necessary measures such as restriction, isolation, correction, suspension or retirement.

When procuring, introducing or using third-party AI systems or related services, the Company shall assess their cybersecurity and adopt appropriate controls, including blacklist management and restrictions on the use of AI systems or tools presenting high risks or cybersecurity concerns, in order to mitigate data leakage, unauthorized access, cross-border transfers and other circumstances that may affect system security. The Company shall periodically review the security of such systems or services and, where necessary, restrict, suspend or otherwise appropriately manage their use.

4. Privacy and Data Governance

In the collection, acquisition, training, testing, deployment, application, retention and deletion of data for AI models and systems, the Company shall comply with requirements relating to personal data protection, trade secrets, intellectual property rights and other applicable laws, regulations and contracts to ensure data privacy in the use and development of AI.

Data used by AI shall come from lawful sources, serve legitimate purposes and be subject to appropriate authorization. The Company shall confirm that the manner of use is consistent with the original purpose of collection, the reasonable expectations of data subjects and applicable contractual terms.

The Company shall follow the principles of data minimization, purpose limitation, accuracy, storage limitation and access control, and shall collect, process and use only the data necessary to achieve a specified purpose.

For personal data, confidential information or sensitive data, the Company shall implement risk-based safeguards such as de-identification, pseudonymization, masking, encryption, data classification, access control and other appropriate protective measures.

Without appropriate authorization, personal data, trade secrets, customer information, internal confidential information or protected intellectual property shall not be entered into, provided to or disclosed to an AI system.

The Company shall also assess, based on risk, the data use, retention, cross-border transfer, retraining and deletion mechanisms of third-party AI services.

5. Transparency and Explainability

Based on the intended use, risk, technical characteristics and level of impact of an AI system, the Company shall disclose, in an appropriate and understandable manner, its use, primary purpose, capabilities, limitations, potential risks and conditions of application.

When users interact with an AI system, they shall, where appropriate, be clearly informed that they are interacting with an AI system rather than a human.

Where the Company provides externally any text, images, audiovisual materials, audio or other content generated by AI, it shall adopt appropriate labeling, disclosure or identification measures based on the level of risk and the context of use to ensure transparency of AI systems.

When AI participates in or influences a decision that has a material impact on an individual's rights or interests, the Company shall provide an explanation proportionate to stakeholders' needs, including the principal influencing factors, basis for the decision, applicable limitations and the means of human review.

High-risk AI systems shall maintain a reasonable degree of traceability and explainability, and the Company shall retain necessary records of data sources, model versions, test results, decisions and human intervention.

6. Fairness and Non-discrimination

In the use and/or development of AI involving human resources management, supplier management, customer service, marketing recommendations, credit assessment or other matters that may affect the

rights and interests of individuals or groups, the Company shall identify, assess and mitigate risks of potential bias and discrimination arising from data, models, algorithms and application processes.

Training, testing and validation data used by AI systems shall, in view of the intended application, have appropriate quality, representativeness and completeness.

The Company shall not cause unreasonable differential treatment, exclusion or discriminatory outcomes based on gender, age, ethnicity, nationality, religion, physical or mental condition, socioeconomic status or any other characteristic protected by law.

High-risk AI systems shall undergo periodic assessments of fairness, bias and disparate impact before deployment and during operation.

Where unreasonable bias, discrimination or adverse impacts are identified in an AI system, the Company shall take measures such as data correction, model adjustment, restricted use, human review or discontinuation of the application.

Article 4 Appropriate Use and Risk Boundaries

The Company shall identify and classify risks based on the intended use of an AI system, affected persons, data sensitivity, importance of the decision, technical complexity and potential severity of harm, and shall implement management measures proportionate to the risks.

Each AI system shall clearly define its approved purpose, scope of application, authorized users, data scope, permissions, conditions and limitations, and prohibited uses. Users shall use the system in accordance with data confidentiality classifications and operational authorizations, and shall avoid use beyond the originally approved purpose, functional scope or context. Users shall not provide Company-sensitive information or personal data to generative AI tools, nor shall they submit queries that may involve confidential business information or personal data. AI products specifically identified by competent authorities as presenting concerns shall be subject to use restrictions in accordance with applicable requirements.

Without assessment, review and appropriate approval, an AI system shall not be repurposed, nor shall human oversight, security controls or access restrictions be circumvented.

The Company shall not develop, procure, deploy or use any of the following AI systems or applications:

1. Systems that use subliminal, deceptive, manipulative or misleading techniques to materially distort an individual's behavior and may cause harm.
2. Systems that exploit vulnerabilities arising from age, physical or mental condition, economic circumstances or other disadvantaged situations to influence or manipulate individual decision-making and may cause harm.
3. Systems that engage in social scoring based on an individual's social behavior, personality traits or information unrelated to the original purpose, resulting in unreasonable, disproportionate or detrimental treatment.
4. Biometric identification, remote identification, tracking or surveillance conducted without lawful authorization, legitimate purpose and necessary procedures.
5. Other AI systems that violate laws or regulations, human rights, public order or Company ethical standards, or that may cause material adverse impacts.

Article 5 Risk Classification and Review

The Company shall establish a tiered management system based on the risk level of AI systems.

An AI risk assessment shall consider at least the following matters:

1. Whether the system affects individual rights and interests, eligibility, opportunities or material benefits.

2. Whether the system uses personal data, sensitive data or confidential information.
3. Whether the system involves automated or semi-automated decision-making.
4. Whether the system may cause bias, discrimination, misleading outcomes or other societal impacts.
5. Whether the system may affect information security, business continuity or critical infrastructure.
6. Whether the system is highly scalable, used on a large scale or difficult to reverse.
7. Whether the system is provided by a third party whose model, data or operating mechanisms lack transparency.
8. Whether the system may have material environmental or resource-use impacts.

High-risk AI systems shall complete cross-functional review and obtain all necessary approvals before development, procurement or deployment. Material AI initiatives may be submitted to the appropriate level for review in accordance with the Company's corporate governance procedures.

Article 6 Third-party and Supplier Management

When procuring, outsourcing the development of, or using third-party AI systems, models, data or services, the Company shall conduct appropriate due diligence and risk assessments based on the level of risk.

Assessment matters may include:

1. Data sources and lawfulness of use.
2. Protection of personal data and confidential information.
3. Information security and incident response capabilities.
4. Model accuracy, stability and bias management.
5. Transparency, explainability and human intervention mechanisms.
6. Data retention, reuse, model training and deletion mechanisms.
7. Environmental footprint and resource efficiency.
8. Regulatory compliance and external verification.
9. Cybersecurity-risk products, services or suppliers subject to restrictions announced by competent authorities.

As necessary, the Company shall use contracts, terms of service, audits, periodic reviews or improvement requirements to ensure that third parties comply with these Principles and applicable management requirements.

Article 7 Stakeholder Rights, Complaints and Remedies

Based on the risk and level of impact of an AI system, the Company shall provide appropriate channels for inquiries, feedback, human review, objection, complaint or remedy.

For individuals or stakeholders materially affected by an AI decision or output, the Company shall provide a reasonable explanation and an opportunity for human intervention.

The Company shall properly handle AI-related complaints, errors, negative impacts and incidents involving impairment of rights and interests, and shall take corrective action, withdrawal, remediation, improvement or other necessary measures according to the nature of each case.

Article 8 Education, Training and Capacity Building

Based on employees' duties and the risks associated with their use of AI, the Company shall provide appropriate education and training on AI governance, ethics, data protection, information security and compliance.

Personnel involved in AI development, procurement, data management, regulatory compliance, information security, risk management and high-risk applications shall receive professional training appropriate to their responsibilities.

The Company shall continuously enhance employees' awareness of AI capabilities, limitations, risks and appropriate use, and shall establish necessary operating guidelines and consultation channels.

Article 9 Monitoring, Recordkeeping and Continuous Improvement

The Company shall establish appropriate monitoring, audit and recordkeeping mechanisms based on the risk level of AI systems.

Monitoring may include:

1. Accuracy and performance.
2. Model drift and data drift.
3. Fairness and bias.
4. Information security and anomalous incidents.
5. Human intervention and review.
6. Customer complaints and negative impacts.
7. Energy use, carbon emissions and other environmental impacts.
8. Compliance with laws, regulations and internal requirements.

The Company shall periodically review the necessity, effectiveness and risks of AI systems, and shall take measures such as correction, retraining, restriction, suspension or retirement based on monitoring results.

Article 10 Governance Structure and Responsibilities

These Principles shall be approved by the Board of Directors.

The Board of Directors, or a governance mechanism authorized by it, shall oversee the Company's AI governance policies, material risks and implementation.

Executive management shall be responsible for establishing the AI governance system, allocating necessary resources, supervising implementation and conducting periodic reviews.

Each business and functional unit shall, in accordance with its responsibilities, implement needs assessment, risk management, review, use, monitoring and improvement of AI.

Information technology, information security, legal affairs, regulatory compliance, personal data protection, risk management, human resources, procurement, sustainability and other relevant units shall jointly participate in AI governance according to the nature of each case.

Article 11 Information Disclosure

The Company shall appropriately disclose its AI governance principles, governance structure, management measures and implementation results in accordance with applicable laws and regulations, governance needs and stakeholder expectations.

Public information shall be accurate, clear and understandable, and shall be consistent with actual implementation.

Article 12 Periodic Review

The Company shall periodically review these Principles and related management systems in response to changes in laws and regulations, technological developments, business models, the risk environment and stakeholder expectations, and shall amend them as appropriate.

Article 13 Implementation

These Principles shall take effect upon approval by the Board of Directors. The same shall apply to any amendments.