Chunghwa Telecom Co., Ltd. Artificial Intelligence Governance Policy

Chunghwa Telecom Co., Ltd. (hereinafter referred to as "the Company") is committed to promoting responsible and trustworthy artificial intelligence. Throughout the artificial intelligence lifecycle, the Company adheres to applicable laws and regulations and international governance principles to ensure compliance and trustworthiness. This Artificial Intelligence Governance Policy applies to all units of the Company and, where necessary, extends to suppliers and partners to define governance boundaries and enhance the comprehensiveness of the policy.

Commitment

I. Ensure that the development of artificial intelligence complies with regulatory requirements and Company policies.
II. Ensure that the development of artificial intelligence is aligned with the Company's sustainability objectives and cybersecurity policies.
III. Strengthen employees' artificial intelligence literacy and sense of responsibility.
IV. Ensure that artificial intelligence applications respect data privacy.
V. Ensure that the development lifecycle of artificial intelligence systems complies with cybersecurity requirements.
VI. Avoid potential bias in artificial intelligence applications.
VII. Retain human intervention mechanisms in artificial intelligence applications.
VIII. Ensure the transparency and explainability of artificial intelligence applications.
IX. Establish and implement artificial intelligence governance and accountability mechanisms.
X. Clearly define the permitted and prohibited boundaries for the use of artificial intelligence.
XI. Actively promote the application of artificial intelligence while balancing low-carbon and sustainable development.
XII. Prohibit the use or deployment of artificial intelligence applications that undermine digital equality.

Action

I. Continue to align the development of artificial intelligence with government regulations, laws, and relevant guidelines, and regularly review compliance and implementation status.
II. Establish an artificial intelligence governance framework, supervised by the Board of Directors or an authorized governance unit, with clearly defined roles and

responsibilities. Integrate sustainable development, data governance, and cybersecurity policies, and conduct regular reviews and continuous improvement.

III. Plan and promote artificial intelligence education, training, and awareness programs to strengthen employees' risk awareness, ethical understanding, and regulatory compliance capabilities in relation to artificial intelligence applications.

IV. Implement and enforce artificial intelligence data governance and privacy protection mechanisms. In accordance with personal data protection regulations and the Company's "Privacy Policy," the collection, training, development, deployment, and operation of artificial intelligence must comply with the principles of personal data protection, purpose limitation, data minimization, retention and deletion, and lawful use of third-party data.

V. Throughout the development lifecycle of artificial intelligence systems, implement security-by-design, access control, encryption, vulnerability management, penetration testing, prompt attack protection, and incident response mechanisms to ensure the security, integrity, and availability of systems and data.

VI. Establish and implement ethics and fairness management mechanisms for artificial intelligence applications. Refer to international artificial intelligence governance principles, such as the OECD AI Principles, and adopt bias identification, fairness testing, representative data review and audit, and continuous monitoring mechanisms to prevent artificial intelligence from producing unfair, discriminatory, or biased outcomes against specific groups.

VII. Ensure that artificial intelligence applications are equipped with human-in-the-loop mechanisms. For decisions involving material rights and interests, high-risk scenarios, or irreversible outcomes, retain mechanisms for human review, intervention, verification, suspension, or override, and prohibit fully automated execution. The purpose, capabilities, limitations, and operational logic shall also be appropriately disclosed.

VIII. When planning, implementing, and using artificial intelligence systems, disclose the purpose, capabilities, limitations, risks, and decision-making basis of artificial intelligence in a comprehensible manner. In appropriate contexts, clearly inform users when they are interacting with an artificial intelligence system.

IX. Clearly establish artificial intelligence management and accountability mechanisms by designating responsible parties for artificial intelligence business ownership, model ownership, and data ownership, as well as risk, regulatory compliance, and cybersecurity review units. Establish mechanisms for incident reporting, investigation, corrective action, accountability tracing, and external complaint handling in order to identify, assess, and mitigate related risks.

X. Establish artificial intelligence usage guidelines and protection mechanisms, and

implement management across all stages of the artificial intelligence system development lifecycle. Clearly define authorized uses, capability boundaries, prohibited uses, and exception escalation and review mechanisms, and introduce risk control and documentation management to ensure traceability, compliance, and the prevention of misuse, capability expansion, or unintended use.

XI. When adopting proprietary or third-party artificial intelligence models, computing resources, and data centers, evaluate their energy efficiency, carbon intensity, water resource usage, computing optimization, and renewable energy consumption. Priority shall be given to solutions with a lower ecological footprint.

XII. Establish review mechanisms to prohibit the use or deployment of artificial intelligence applications that involve manipulative behavior, exploitation of vulnerabilities, social scoring, or unauthorized biometric surveillance in order to promote a diverse and equitable digital environment.

XIII. Establish and implement operational monitoring mechanisms for artificial intelligence systems, continuously monitor model performance, data drift, bias, and safety incidents, and strengthen supplier risk assessments and compliance reviews.

Chairman Chih-Cheng Chien Date: 06/22/2026

This Policy shall be reviewed annually or whenever significant changes occur to assess its appropriateness and to make necessary revisions. This Policy shall be implemented upon approval by the Chairman of the Board, and the same applies to all subsequent amendments.