PHISON

Phison Electronics Corp.
Artificial Intelligence Governance Policy

Preamble

Phison Electronics Corp. (hereinafter referred to as "the Company") is committed to promoting responsible and trustworthy artificial intelligence. The Company complies with relevant regulations and international governance principles throughout the artificial intelligence lifecycle to ensure its compliance and reliability.

Boundaries of Application

This policy applies to all internal units of the Company. At this stage, it does not extend to suppliers and business partners. If future business needs arise (such as outsourced development or cloud AI service procurement), relevant regulations and supplier commitment clauses will be incorporated in a future revision of this policy.

I. Commitments

1. Ensure that artificial intelligence development complies with regulations and corporate policy requirements.
2. Ensure that artificial intelligence development aligns with the Company's sustainability goals and information security policies.
3. Enhance employees' artificial intelligence literacy and sense of responsibility.
4. Ensure that artificial intelligence applications respect data privacy.
5. Ensure that the artificial intelligence system development lifecycle complies with cybersecurity standards.
6. Prevent potential biases within artificial intelligence applications.
7. Retain human-in-the-loop mechanisms within artificial intelligence applications.
8. Ensure the transparency and explainability of artificial intelligence applications, and clearly label AI-generated content and AI-driven decisions.
9. Establish and implement artificial intelligence governance and clear accountability mechanisms.
10. Clearly define the boundaries of what artificial intelligence can and cannot perform, and restrict access permissions to sensitive artificial intelligence functions (e.g., biometric recognition, internal surveillance).
11. Balance low-carbon and sustainable development by actively evaluating and promoting energy efficiency and ecological footprint management for artificial intelligence applications.
12. Prohibit the use or deployment of artificial intelligence applications that involve manipulative behaviors, exploitation of vulnerable groups, social scoring, or unauthorized biometric surveillance.

PHISON

II. Governance Structure

1. Phison establishes an Artificial Intelligence Governance Committee (hereinafter referred to as the "AI Governance Committee"), which operates independently of the existing Information Security Committee. It shall be led by senior executives, with members comprising cross-departmental representatives from legal, cybersecurity, human resources, and business operations.
2. The responsibilities of the AI Governance Committee include: reviewing and deliberating on this policy and its amendments; overseeing the implementation of the artificial intelligence governance framework; reviewing human-in-the-loop mechanism designs for high-risk artificial intelligence application scenarios; periodically reviewing the performance of AI ethics and fairness management; and regularly reporting governance outcomes to senior management (or the Board of Directors).
3. The operations of the AI Governance Committee shall be integrated with the Company's sustainability, data governance, and cybersecurity policies to avoid organizational redundancy, and shall be periodically reviewed for continuous improvement.

III. Actions

(1) Regulatory Compliance

Artificial intelligence development continuously aligns with government regulations, laws, and relevant guidelines, with regular reviews of its compliance and implementation status.

(2) Education and Training

Plan and promote artificial intelligence education, training, and awareness mechanisms. All employees receive basic training in artificial intelligence ethics and risk awareness. Departments directly using or operating artificial intelligence tools (such as human resources recruitment teams, cybersecurity/compliance teams, R&D, and sales) receive advanced training to strengthen their risk awareness, ethical understanding, and legal compliance capabilities.

(3) Data Governance and Privacy Protection

Introduce and implement artificial intelligence data governance and privacy protection mechanisms. In accordance with personal data protection regulations and the Company's privacy policy, the principles of personal data protection, purpose limitation, data minimization, storage and deletion, and the lawful use of third-party data are followed throughout all stages of artificial intelligence data collection, training, development, deployment, and maintenance.

(4) Cybersecurity

Implement mechanisms such as secure design, access control, encryption, vulnerability management, penetration testing, prompt injection attack protection, and incident response throughout the artificial intelligence system development lifecycle to ensure the security, integrity, and availability of systems and data.

(5) Ethics and Fairness

Establish and execute ethical and fairness management mechanisms for artificial intelligence applications. Referencing international artificial intelligence governance principles (such as the OECD AI Principles), adopt bias identification, fairness testing, representative data verification, and continuous monitoring mechanisms to prevent artificial intelligence from causing unfair, discriminatory, or biased results for specific groups. Artificial intelligence applications used for recruitment or performance evaluation screening are prioritized for fairness audits and reviewed at least once a year.

(6) Human-in-the-Loop

Ensure that artificial intelligence applications incorporate human-in-the-loop mechanisms. For artificial intelligence decisions involving significant rights, high risks, or irreversible impacts, mechanisms for human review, intervention, secondary review, termination, or overwriting are retained, and full automation is prohibited. At this stage, the Company explicitly mandates that the following scenarios require human review and retention of the final decision-making power, and final outcomes must not be executed automatically by AI:

- Human resources recruitment, interview scoring, or performance evaluation screening.
- Access control involving gates/biometric recognition and internal surveillance applications.
- Automated response decisions for cybersecurity or legal compliance incidents.

(7) Transparency and Explainability

When planning, introducing, and utilizing artificial intelligence systems, disclose the purpose, capabilities, limitations, risks, and decision-making basis of the artificial intelligence in an understandable manner. Clearly inform users in appropriate contexts that they are interacting with an artificial intelligence system rather than a real person. AI-generated content provided externally or internally, as well as decision-making outcomes assisted or driven by AI (such as recruitment screening results), must be clearly labeled as AI-generated or AI-assisted decisions.

(8) Management and Accountability Mechanisms

Explicitly establish management and accountability mechanisms for artificial intelligence:

- **AI Business Owner:** Assumed by the head or designated representative of each business unit introducing/using the artificial intelligence application, responsible for the business justification and impact assessment of the application.
- **Model Owner:** Assumed by the Technical System Integration Division, responsible for model technical security reviews, performance, and vulnerability management.
- **Data Owner:** Assumed by the data-owning department, responsible for data source legality, quality, and privacy compliance.
- **Risk Review Unit:** Assumed by the Legal Affairs Department (or risk management unit), responsible for regulatory compliance and risk reviews.
- **Cybersecurity Review Unit:** Assumed by the Safety & Resource Integration Department, responsible for cybersecurity risk reviews.

In addition, establish mechanisms for artificial intelligence incident notification, investigation, remediation, and traceability of responsibility. Establish appeal/review channels (which may be integrated with existing employee grievance or whistleblowing mechanisms) for colleagues or third parties (such as job applicants) affected by artificial intelligence decisions, in order to identify, assess, and mitigate related risks.

PHISON

(9) Usage Regulations and Safeguard Mechanisms

Formulate artificial intelligence usage regulations and safeguard mechanisms, and implement management across all stages of the artificial intelligence system development lifecycle. Explicitly regulate authorized uses, capability boundaries, prohibited uses, and exception escalation review mechanisms. Restrict access permissions for sensitive artificial intelligence functions (such as biometric recognition and behavior monitoring) to authorized personnel only. Introduce risk control and documentation management to ensure traceability, compliance, and to prevent function abuse, creep, or unintended uses.

(10) Low-Carbon and Sustainability

When adopting internal or third-party artificial intelligence models, computing resources, and data centers, evaluate their energy efficiency, carbon intensity, water consumption, computational optimization, and renewable energy usage, prioritizing solutions with a lower ecological footprint. Reference the carbon emissions and energy consumption data from the Company's existing ESG/Sustainability Report as a baseline, and integrate the quantified impact of artificial intelligence-related initiatives on sustainability outcomes (such as energy-saving benefits and computing efficiency improvements) into existing sustainability KPI disclosures.

(11) Prohibition of Improper Applications

Establish verification mechanisms to prohibit the use or deployment of artificial intelligence applications that involve manipulative behaviors, exploitation of vulnerable groups, social scoring, or unauthorized biometric surveillance. Authorized biometric uses, such as for access control or attendance tracking, may continue to be used in accordance with current regulations (and employees must be informed of the purpose and scope of use); however, any unauthorized or covert employee behavior monitoring, emotion/behavior scoring, or social scoring applications are strictly prohibited.

(12) Maintenance and Monitoring

Establish and execute artificial intelligence system maintenance and monitoring mechanisms to continuously monitor model performance, data drift, bias, and security incidents. If the scope of this policy extends to suppliers in the future, supplier risk assessments and compliance reviews will be strengthened.

IV. Policy Effectiveness and Review

The appropriateness of this policy is reviewed annually or upon the occurrence of major changes, and necessary revisions are made. Following review and deliberation by the AI Governance Committee, this policy is submitted for approval prior to implementation; the same procedure applies to its amendments.

Chairman
Wee Kuan Gan

July 2026