Wistron Corporation

Responsible Artificial Intelligence System Policy

Article 1 Objective

To ensure that artificial intelligence (AI) products and services of Wistron Corporation's (hereinafter referred to as "the Company"), and to address the opportunities and challenges brought by artificial intelligence (AI), the Company has established the "Responsible AI System Policy" to regulate the core principles of Responsible AI (RAI) throughout the AI lifecycle, including planning, design, development, testing, and deployment, with emphasis on security, fairness, robustness, reliability, and validity. This ensures compliance with relevant laws and regulations, thereby gaining customer trust, fulfilling commitments to shareholders, supporting the Company's sustainable development goals, and ensuring the operation of critical business functions.

Article 2 Scope

This policy applies to the Company’s global employees, suppliers, and customers who enter the Company’s premises.

Article 3 Organization and Authority

3.1 The Board of Directors serves as the highest decision-making body for promoting information security and policy-making and is responsible for approving information security and RAI governance policies, objectives, and programs, as well as providing the resources necessary for management operations. Under the Board, the Sustainability and Information Security Committee is established to determine the enterprise’s information security development direction, strategy, and objectives. Under that committee, an Information Security Committee is formed. The Information Security Committee oversees the Company’s information security management system, RAI management system, technical standards, operational maintenance, and the implementation and governance of RAI-related principles, and holds ultimate responsibility for AI system outputs, risk-related decisions, regulatory compliance, incident investigation, and attribution.

3.2 The Information Security Committee convenes quarterly and may hold ad hoc meetings as necessary; members of the subordinate groups are required to attend. Meeting agendas include:

(i) Reports from each subgroup on the progress of their internal initiatives;
(ii) Handling and investigating information security and RAI incidents;
(iii) Matters requiring cooperation from Company units;
(iv) Other relevant proposals or ad hoc motions.

3.3 An RAI incident response organization shall be established, and an incident reporting mechanism put in place to integrate internal information security and RAI personnel with external expert resources. The Company will monitor RAI risks, including emerging AI-related threats within the monitoring scope, and respond rapidly to incidents while implementing mitigation strategies.

3.4 When violations or threats occur, RAI incidents shall be managed through an escalated, tiered reporting process and response mechanism. The Company will maintain transparency of incident information with affected stakeholders, complete incident investigation, handling, and remediation reports, and provide detailed descriptions of the actions taken to address risks and prevent future occurrences.

Article 4 RAI Must Be Maintained by All Company Personnel

4.1 All employees of the Company should pay attention to any potential RAI risks and report them to the relevant RAI unit in accordance with the RAI incident reporting procedures.

4.2 The RAI Technology and Policy Implementation and Maintenance Team is responsible for establishing RAI management mechanisms and assisting in the resolution of RAI incidents to ensure the Company’s RAI objectives are met.

4.3 The Company shall periodically provide RAI education, training, and awareness activities for employees. Provide appropriate training based on different employee roles to establish RAI knowledge and awareness among all personnel, strengthen all employees' responsibility for the Company's RAI objectives, and ensure compliance with relevant requirements.

Article 5 Integrity and Protection of the AI System Life Cycle

5.1 Privacy and Data Protection

5.1.1 During the development, deployment, and use of AI systems, privacy and personal data protection laws and regulations must be respected. Reference

should be made to applicable regulations in the place of operation (e.g., the European Union's General Data Protection Regulation (GDPR) and Taiwan's Personal Data Protection Act), recognizing the critical role these laws play in protecting fundamental rights.

5.1.2 Establish data governance and AI system development lifecycle control mechanisms to ensure RAI controls are maintained throughout the data and AI development lifecycle. For data used by AI models — for example, functional data and user accounts collected during system design — label attributes across the same dimensions (e.g., site, country, job grade, department). On access, the system should automatically compare labels and permit access only when they match, to prevent data leakage and ensure that only authorized users can modify or access sensitive information.

5.2 Information Security Protections

5.2.1 Extending existing information security protection mechanisms to AI system applications, including practices such as DevSecOps, penetration testing, and SOC monitoring.

5.2.2 Implement information security measures to defend against cyberattacks and prevent the generation of harmful or inappropriate content. For example, deploying AI guardrail tools to control the safety of AI inputs and outputs, reduce risks from prompt-injection and similar attacks, and prevent generation of harmful or inappropriate content. AI guardrail should also integrate privacy protection functions to proactively detect and block inputs/outputs that could lead to personal data leakage, information security or RAI violations, or other noncompliant behavior. Relevant logs and indicators should be fed into centralized audit and incident response systems (e.g., SIEM/SOC) to facilitate tracking, auditing, and rapid response.

5.2.3 Continuously learn from and test actual deployment conditions and evolve detection and protection mechanisms as threats change. This includes regular penetration testing, RAI incident drills, and other exercises to strengthen AI system incident response capabilities and protections.

5.3 Fairness and Absence of Bias

During development and use, AI systems should strive to avoid producing discriminatory or biased outcomes. This includes establishing algorithmic bias detection mechanisms, fairness evaluation metrics, and AI-generated content identification, identifying and mitigating biases in training data and generated outputs, and conducting bias testing to prevent potential prejudices.

5.4 Transparency and Explainability

5.4.1 Ensure transparency during development and use of AI systems, including informing users when they are interacting with an AI system and fully disclosing the system's intended purposes, authorized scope, and capabilities so that users understand the system's risks and limitations. AI systems are limited to internal or otherwise approved uses; unauthorized external sharing, commercial resale, or outsourcing is strictly prohibited. Any illegal, noncompliant, or rights-damaging uses affecting the Company or third parties are forbidden. Use AI guardrail tools to control output content; AI outputs should be reviewed and verified before adoption or transmission, and final judgments should rely on independent assessment. System users are responsible for the final application and its impact to prevent misuse, abuse, mission scope creep, or other unintended applications.

5.4.2 During operations, AI systems should be continuously monitored. Determine which RAI metrics to monitor based on task characteristics. If metric anomalies are detected or user feedback is received, perform issue investigation, escalated, tiered diagnosis, and remediation to ensure the AI system continues to operate within its originally intended design scope.

5.4.3 Upon user request, provide testing mechanisms and easy-to-understand explanations that clarify how the AI system makes decisions.

5.5 Human Oversight and Decision-Making

AI systems should be subject to appropriate and documented human oversight. Human oversight should be implemented through suitable governance mechanisms, including but not limited to human-in-the-loop, human-on-the-loop, or human-in-command approaches, and must grant humans the authority and capability to intervene, override, or escalate actions.

5.6 Sustainability

During AI development, deployment, and use, environmental management commitments should be followed. Consider carbon reduction and efficiency across the AI system lifecycle, including for the Company’s own or third-party AI data centers. Operational optimizations should be pursued, such as monitoring and reducing energy consumption, promoting efficiency-enhancing techniques, encouraging use of renewable energy, or employing AI systems to assist with energy-monitoring and optimization, in order to achieve improved control and energy savings.

Article 6 Continuously optimize the RAI Management System

6.1 Conduct RAI risk assessment operations. Include AI system-related risks in the assessment scope and invest necessary resources (including equipment, tools, personnel, services, etc.) to protect and create value.

6.2 Regularly conduct internal and external audit operations to review the Company's AI systems and ensure that control measures operate effectively and are continuously improved.

Article 7 Strengthening Third-Party RAI Requirements

7.1 The Company's third parties (e.g., suppliers) shall comply with the Company's RAI policy and related procedures.

7.2 Third parties involved in AI systems should be required, based on the risk assessment results, to cooperate in implementing these RAI management requirements.

Article 8 Management Commitment

8.1 The Company's commitment to RAI management is to ensure the provision of necessary resources for the operation of the RAI management system, including continuous investment in RAI governance and security, minimizing losses by preventing and reducing the impact of RAI incidents.

8.2 Under the RAI management commitment, the Company shall not develop, deploy, or use AI systems that do not comply with applicable laws and regulations, particularly those involving manipulative behavior, exploitation of vulnerabilities, implementation of social scoring, or conducting unauthorized biometric

surveillance. For example, the Company shall not develop, deploy, or use AI systems that employ biometric identification (including facial recognition) or other identifiable characteristics to target specific individuals or groups for continuous surveillance in a manner that disregards or infringes upon human rights.

Article 9 Implementation and Review

This policy should be regularly reviewed and adjusted according to the latest RAI developments to comply with relevant laws and regulations.

Article 10 Take effect

This policy shall be implemented after being approved by the Board of Directors, and the same shall apply when amended.

This policy was established on August 4, 2026.