Responsible Artificial Intelligence Systems Program

Wistron is committed to establishing a “Responsible Artificial Intelligence System” as a core objective. Wistron has developed a Responsible AI (RAI) system policy as its principal guiding framework, actively driving intelligent transformation by implementing RAI management mechanisms and building governance and accountability across four dimensions: organization, processes, technology, and talent.

Wistron is dedicated to embedding key elements throughout the AI lifecycle, including data and privacy protection, fairness audits, transparency and explainability, continuous monitoring, and incident response. By regularly conducting RAI incident drills, internal and external audits, and training programs, Wistron establishes rapid feedback mechanisms to address emerging threats and changing compliance requirements.

1. ISO 42001 Artificial Intelligence Management System

Wistron obtained ISO/IEC 42001:2023 Artificial Intelligence Management System (AIMS) certification in July 2026 and in accordance with that standard, implemented the Plan-Do-Check-Act (PDCA) cycle management model. Wistron conducts at least one internal audit and one external third-party audit each year and undertakes recertification every three years to ensure comprehensive implementation of information security management mechanisms and the continued validity of the certification, demonstrating a long-term commitment to the management of responsible artificial intelligence systems. In 2026 the certification was granted by SGS, with the certificate valid through July 20, 2029. The scope of certification is as follows:

1.1 Deployment, integration, and operation of the internal “Columbus AI Platform”, supported by an internal knowledge base, enabling employees to use virtual expert functionalities, where the organization acts as an AI Provider.

1.2 Design, development, testing, validation, deployment, and maintenance of the “Machine

Learning-based Part Number Master Analysis and Definition System", used to generate predictive outputs for part number master data analysis, definition, and reporting, where the organization acts as AI Producer.

1.3 Use of the AI-powered "Recruitment and Hiring Knowledge Base" on the "Columbus AI Platform" for internal access to recruitment, hiring, and related human resources policies and procedures, where the organization acts as an AI User.

2. Responsible Artificial Intelligence System Policy and Organization

To promote and implement AI governance and to ensure the confidentiality, integrity, and availability of Wistron's critical AI system assets, these systems shall operate within compliant, secure, and reliable parameters. This approach aims to meet legal and regulatory requirements and the objectives of Responsible AI, thereby earning customer trust, fulfilling commitments to shareholders, and ensuring the continuity of critical business operations and sustainable long-term management.

To strengthen Wistron's long-term competitiveness and enhance information security governance, Wistron's Board of Directors approved the renaming of the "ESG Committee" to the "ESG and Information Security Committee" on April 2, 2025. An Information Security Committee was established under this committee, with the President & CEO and Chief Digital & Information Security Officer, serving as the top guiding officers. This structure represents Wistron's commitment to advancing information security and Responsible AI (RAI), and it oversees the implementation of information security and RAI management systems, technical standards, operations and maintenance.

The Chief Information Officer was appointed as the Management Representative, and the Head of the Information Security Governance Office as the Executive Secretary to coordinate information security and RAI matters. On October 1, 2025, the Information Security Committee created an RAI working group within the committee to focus on the planning, execution, and oversight of RAI governance initiatives.

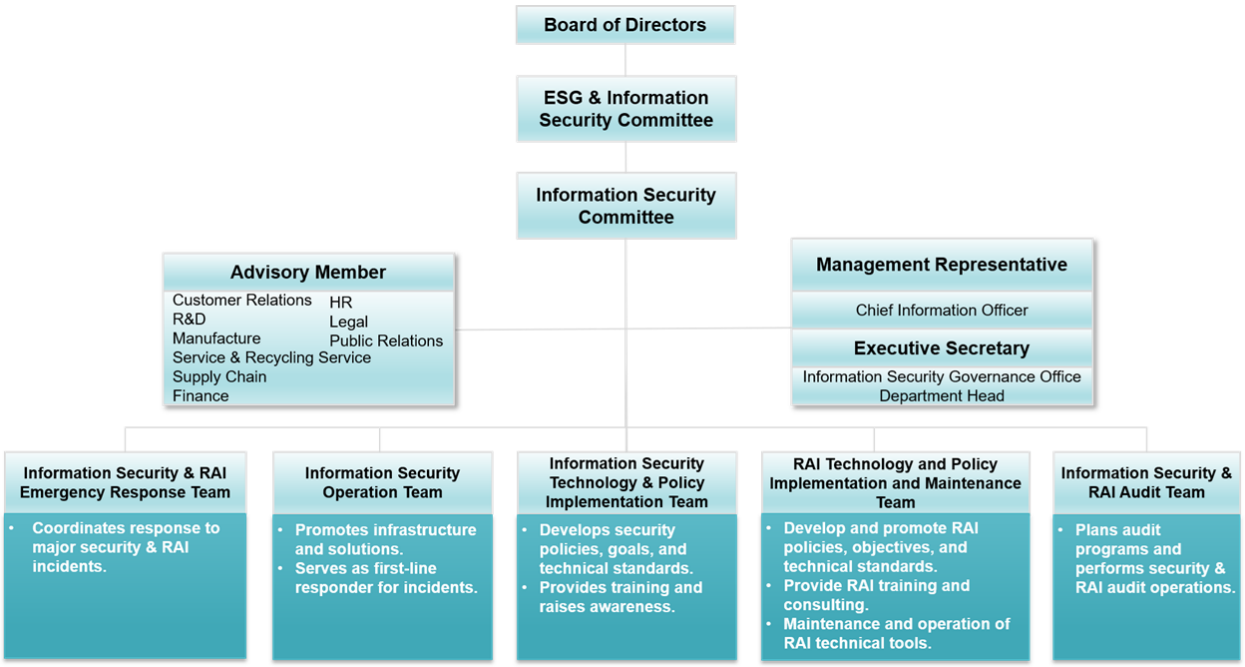
By defining clear responsibilities and adopting a functionally organized structure, Wistron has increased the execution efficiency and transparency of its AI governance system, further strengthening the organization’s governance foundation for AI risk management. Using the “Information Security Policy” and the “Responsible Artificial Intelligence System Policy” as management frameworks, Wistron protects information assets related to employees, customers, suppliers, and operations, thereby ensuring sustainable business continuity.

2.1 Responsible Artificial Intelligence System Policy

To ensure Wistron Information Technology Co., Ltd.’s AI products and services and to address the opportunities and challenges they entail, Wistron has established the "Responsible Artificial Intelligence System Policy" to govern core RAI principles—including safety, fairness, robustness, validity, and reliability—throughout the AI lifecycle, covering planning, design, development, testing, and deployment. This policy ensures compliance with applicable laws and regulations, builds customer trust, fulfills commitments to shareholders, supports Wistron’s sustainability objectives, and safeguards the continuity of critical business operations.

2.2 Information Security Committee — Organizational Structure

The Information Security Committee meets once each quarter and may convene ad hoc meetings when necessary; members of each subgroup are required to attend. Meeting agendas include reports on information security and RAI incident handling, progress reports from each subgroup on the advancement of their internal matters, items requiring cooperation from relevant units, and other related recommendations or miscellaneous motions. The Information Security Committee held four meetings in 2025, and the Management Representative reported on the status of information security and RAI implementation to the Board in December.



3. Responsible Artificial Intelligence System Management Strategy

To respond to the rapid changes in internal and external environments, Wistron has added an RAI function group within its existing information security organization, responsible for planning, promoting, and managing RAI-related risks and policies. Wistron focuses on building governance and accountability across four main areas: a clear responsibility and role-allocation structure; formulation of RAI policies and management plans; promotion of automated deployment, detection, and monitoring mechanisms; and talent education and hands-on training.

Wistron's RAI governance mechanisms are developed with reference to ISO/IEC 42001:2023 Artificial Intelligence Management System (AIMS), the U.S. National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), and the EU AI Act. By integrating information security governance frameworks and protective measures, Wistron promotes a comprehensive governance system that covers accountability structures, policy standards, and automated monitoring. At the same time, through training and technical practice, Wistron enhances organizational expertise to ensure that, under a vision of innovation and sustainability, intelligent transformation is realized and a resilient, secure, and responsible corporate environment is established.

4. Formulation of RAI Policies and Management Plans

To manage the AI lifecycle and operational mechanisms, Wistron has issued implementation policies and standards. These policies and standards provide a concrete and robust foundation for deepening AI governance in the future, ensure consistent management mechanisms across the organization, and establish a systematic PDCA (Plan-Do-Check-Act) iterative improvement cycle.

4.1 Responsible AI Lifecycle Management Standard

The RAI lifecycle management standard specifies Wistron's standard operating procedures and the execution and monitoring records to be retained for each stage of the AI system lifecycle, covering seven major phases: planning, design, data management, data engineering, system development/model training, testing/deployment, and operations/monitoring.

4.2 Establishing Data Access Permission Mechanisms

During the design phase, developers must plan for the system to include data access permission features, and for sensitive AI systems that may raise ethical or privacy concerns, implement strict access controls at this stage. Restricting access ensures that only authorized personnel can use such functions, thereby reducing the risk of misuse or abuse. Implementation is achieved during system design and development by adopting an authorization mechanism based on multi-dimensional tags. Each function or data item can be labeled with a set of authorization tags (example dimensions: site/country, job level, department, etc.). User accounts also store attribute tags in the same dimensions; when a user attempts to access a function or data item, the system compares the user’s tags with the resource’s authorization tags and allows display or operation only if the authorization conditions (tag matches) are met. Otherwise, the system blocks the content from being shown. Example: a particular AI system is enabled only for specified country/site/job levels;

users whose tags do not match will not see the content.

4.3 RAI Incident Reporting, Event Management, and Incident Drills

To ensure the effectiveness of RAI system management and to rapidly address RAI incidents, vulnerabilities, or suspicious activities, Wistron has established a comprehensive escalation process that enables employees to promptly report issues and trigger the incident response mechanism. Employees may report or appeal suspicious behavior, vulnerabilities, or RAI incidents/complaints through multiple channels such as internal platforms, the local IT Helpdesk (ext. 11119), the reporting system, or by contacting the RAI team directly. If internal or external personnel have any questions about the use of AI systems or ethical issues, they may visit the ESG website's "Contact" page and submit feedback or file a complaint via the RAI issues contact email (RAI@wistron.com). This process ensures that every RAI incident receives appropriate attention and response immediately.

To strengthen rapid response and sustained protection for RAI incidents, Wistron integrates RAI incident handling with the Security Operations Center (SOC) and monitor RAI alerts comprehensively through the AI Service Portal (ASP), enabling timely detection and mitigation of potential threats to prevent escalation.

Whether incidents are reported by employees or detected by system monitoring, Wistron handles them in accordance with the Information Security Incident Management Standard and the Responsible AI Incident Operating Procedures. RAI incidents are classified into three severity levels. Depending on the severity, three different levels of response organizations are mobilized. Wistron has also defined the required timeliness for handling incidents and the frequency of reporting updates. Each incident response follows nine steps: initial notification and assessment / classification, escalation, initial containment, analysis, post-analysis containment, eradication, recovery, reporting, and post-incident lessons learned. This process institutionalizes the reporting, classification, handling, statistics, and tracking of RAI incidents so that incidents can be reported and responded to quickly and services restored in the shortest possible time, ensuring normal business

operations.

To ensure continuity of operations and to minimize the impact of major RAI disasters on critical AI systems, Wistron continually refine detection and protection mechanisms as threats evolve through continuous learning. This includes regularly conducting RAI incident drills to improve our AI security response capabilities and protective measures.

5. Promotion of Automated Deployment, Detection, and Monitoring Mechanisms

5.1 Automated Testing and Deployment for Secure AI System Development

During the system development/model training and testing/deployment phases, MLSecOps (Machine Learning Security Operations) automated testing and deployment are executed. MLSecOps integrates security principles and practices into the entire lifecycle and operational processes of ML/AI systems, ensuring that data, models, and inference services have controllable, auditable, and recoverable security during development, deployment, and operation.

5.2 AI System Security Protection and Monitoring Mechanisms

Wistron extends existing cybersecurity protections (e.g., Identity and Access Control, DevSecOps, penetration testing, SOC monitoring) to AI system applications and introduce dedicated AI protection technologies and tools to defend against cyberattacks and to prevent the generation of harmful or inappropriate content. Specific measures include deploying AI guardrails at the input side to guard against prompt injection and malicious inputs, applying content filtering and risk assessments at the output side, and combining automated anomaly detection, content classification, and related mechanisms to reduce risks of abuse and attacks.

Throughout development, deployment, and operational lifecycle, Wistron strictly comply with privacy and data protection regulations and establish comprehensive data governance and AI lifecycle controls to ensure RAI measures are implemented. AI guardrails should also integrate privacy protection capabilities to proactively detect and block input/output

behaviors that could lead to personal-data leakage or regulatory violations, and forward related logs and indicators into centralized audit and incident-response systems (e.g., SIEM/SOC) to enable tracking, auditing, and rapid response.

5.3 RAI Metrics Monitoring Mechanism

During the system development/model training, testing/deployment, and operations/monitoring stages, an RAI metrics monitoring mechanism is implemented to ensure that requirements such as transparency, validity/reliability, explainability, and fairness are implemented.

5.3.1 Transparency

To ensure transparency in the development and use of AI systems, content generated by the AI (such as text, images, or decisions) will be labeled as AI-generated on the system interface or in output files. Users should exercise caution when consulting or relying on this information.

5.3.2 Validity/Reliability

During the development and use of AI systems, establish mechanisms to test validity and reliability. Validity can measure the degree of difference between outputs and the true targets; implementations include metrics such as Accuracy, Precision, and F1-score. These metrics mainly indicate the proportion of correct model predictions and are used to evaluate overall performance on classification tasks. After an AI system is deployed, continuously monitor related operational validation metrics and system logs, and perform an initial review when metric anomalies are found or user feedback is received, then escalate issues to maintenance personnel for troubleshooting and repair. Through a regular evaluation and monitoring mechanism, determine whether the AI model experiences drift or performance degradation over time or as external conditions change. When model accuracy declines, detect it early and take corrective actions—such as retraining the model with new data or adjusting its parameters—to ensure the AI system’s reliability and compliance with requirements.

5.3.3 Explainability

When a user makes a request, an RAI metrics monitoring mechanism can be used to explain how the AI system reaches its decisions. Specific methods include using SHAP (SHapley Additive exPlanations) to measure each feature's contribution to the output, which helps evaluate and clarify the system's decision-making.

5.3.4 Fairness and Bias Mitigation

During the development and use of AI systems, establish algorithmic bias detection mechanisms, fairness assessment metrics, and AI-generated content identification. Based on risk level (low / medium / high), set post-deployment monitoring frequencies of 12 / 9 / 6 months, respectively, to periodically evaluate, detect, and reduce bias in training data and generated outputs. Specific methods include using metrics such as Disparate Impact and R-squared Parity, which are statistical measures that assess whether a model or decision disproportionately disadvantages protected groups (e.g., gender, race, age). If the proportion for a protected group is significantly lower, disparate impact may be present.

Additionally, AI guardrails should incorporate detection and filtering of improper terms (e.g., violent content, pornography, discriminatory or hateful speech) at both input and output stages. Because these issues can relate to fairness, detection logs should be consolidated into a centralized audit and incident-response system (for example, SIEM/SOC) to facilitate tracking, auditing, and rapid response.

6. Strengthening Employee RAI Education and Practical Training

To ensure employees have a deep understanding of RAI objectives and can apply them effectively, Wistron will hold regular RAI education, training, and awareness activities. Training topics will be tailored to different departments, job functions, and roles—for example, Product Owner, Tech Lead, and Data Scientist—so they meet actual business needs. Content will range

from foundational risk knowledge to lifecycle development, testing, deployment, and advanced operational practices.

Examples include courses such as “OWASP Top 10 for LLM Applications – 2025 Edition,” which help users understand the risks and vulnerabilities of generative AI. Beyond conveying the importance of Wistron’s governance mechanisms, these courses encourage users to pay attention to the risks of using AI systems and strengthen the organization’s cybersecurity and privacy governance goals.

The “RAI Metrics Workshop” will develop practical skills for AI system Data Scientists, covering preparation and installation of RAI metrics tooling and hands-on implementations for ML / LLM / Agent systems. The workshop will translate abstract RAI governance objectives—such as fairness, robustness, and validity/reliability—into quantifiable, monitorable, and actionable metrics and operational processes. Through these training programs, employees will be equipped to apply RAI concepts within their respective roles and implement them in accordance with actual business needs.

7. Sustainability Initiatives

In April 2024, Wistron received approval from the Science Based Targets initiative (SBTi) for its science-based emissions reduction target (SBT), in support of the Paris Agreement’s goal to limit global warming to no more than 1.5°C above pre-industrial levels. Wistron is committed to achieving carbon neutrality for Wistron’s operational activities by 2030 and net-zero value-chain emissions by 2050.

Throughout the AI system lifecycle, Wistron selects third-party AI data centers that prioritize waste reduction, emissions reduction, and efficiency—such as Microsoft’s cloud services. Microsoft has committed to net-zero carbon by 2030, and its AI data centers reached 100% renewable energy for annual electricity consumption in 2025, efforts that help reduce energy use, water consumption, and carbon intensity.

For our own data centers, Wistron focuses on energy-saving optimization, monitoring

and reducing energy use, and encouraging the use of renewable energy. Our data center is located in the Hsinchu AI Smart Park; the building meets LEED Gold standards as an intelligent green building, and roughly 60% of its electricity supply comes from green power. These measures are pursued to make concrete contributions to sustainable development.

8. Sustainability Practices

Wistron has deployed an "AI air-conditioning and compressed-air group control system" across its global factories to address the increased electricity consumption and carbon emissions associated with higher production capacity. This solution replaces traditional manual on/off operations and parameter adjustments by collecting environmental factors, schedules, and equipment parameters via the Internet of Things (IoT) and micro-weather stations, thereby reducing the risk of production-line downtime caused by electrical overload. The system was shared on the COP28 Climate Action Platform and specifically corresponds to the following two sustainability management practices and has received one award recognition:

8.1 Quantification of AI’s Impact on Sustainability

This project uses a data-driven approach to systematically measure the environmental impact of AI tools. The system employs machine-learning models to predict demand and combines a genetic algorithm to automatically recommend equipment start-up combinations, keeping operations energy-efficient. The quantified results are as follows:

8.1.1 Equipment level: AI dynamic control reduced electricity consumption of air-conditioning and compressed-air equipment by 16%.

8.1.2 Manufacturing level: Through demand forecasting and dynamic air-supply compensation, electricity consumption per finished good decreased by 41%.

8.1.3 Overall carbon reduction: Since implementation in 2021, the project has delivered concrete electricity savings and carbon reductions for Wistron, achieving a 36%

reduction in overall carbon emissions and enabling progress reporting to stakeholders with concrete data.

8.2 Lowering the Ecological Footprint (Scope 1 & 2)

For the ecological footprint of production operations (Scope 1 & 2), Wistron implements the following measures through an AI control system:

8.2.1 Algorithms and energy-efficiency control: The system features a biweekly rolling "self-learning and retraining" mechanism combined with anomaly detection, keeping one-hour-ahead electricity and air-pressure forecast error rates within 5%. It also uses fuzzy control linked to variable-frequency equipment to reduce idle energy consumption.

8.2.2 Data monitoring: Deploy smart meters for water, electricity, and gas; establish an electricity baseline and monitor consumption parameters in real time to precisely manage major equipment energy use within the plant.

8.2.3 Project benefits: Through AI demand forecasting and dynamic start-up combinations, electricity consumption for air-conditioning and compressed-air equipment was reduced by 16%, delivering actual electricity savings of 10.75 million kWh—approximately equivalent to a carbon reduction of 8,645 tons.

8.3 Scaled Deployment and 2023 Lighthouse Factory Benefits

The "AI air-conditioning and compressed-air group control system" has reached advanced maturity and has been standardized for deployment across Wistron’s global factories. At the Zhongshan Factory, the system—together with a decarbonization management platform—was used to implement plant energy management and data-driven carbon-reduction tracking. The quantified carbon-reduction benefits produced by this effort were one of the key evaluation items for Zhongshan Factory’s 2023 World Economic Forum (WEF) "Global Lighthouse" recognition. The specific benefits are as follows:

8.3.1 Energy cost savings: Through plant-wide energy management optimization, the factory achieved cumulative energy cost savings of approximately USD 8.02 million.

8.3.2 Project and Green Power Carbon-Reduction Contribution: In addition to the specific carbon reductions from the AI air-conditioning and air-compression optimization project, the plant’s self-built solar power station (annual generation: 5.5 million kWh) further reduces carbon emissions by 4,423 tons, concretely fulfilling the commitment to lower our ecological footprint.