

Ennoconn Responsible AI Governance and Management Framework

I. Purpose of the Framework

To implement the Company's "Responsible AI Policy," Ennoconn Corporation integrates Artificial Intelligence (AI) governance into its existing mechanisms for sustainability governance, information security, risk management, data protection, and operational management, establishing the Responsible AI Governance and Management Framework. This framework focuses on the use management, risk control, education and training, information disclosure, grievance handling, and performance tracking of AI tools, platforms, models, and related applications, in order to balance innovation benefits, information security, privacy protection, compliance requirements, and sustainable value.

II. Scope of Application

This framework applies to Ennoconn Corporation and its subsidiaries (and sub-subsidiaries) in which it holds a 50% or greater stake, and covers:

1. AI systems, models, and applications developed in-house, co-developed, deployed, tuned, or maintained by the Company.
2. Third-party AI tools, platforms, models, cloud services, and data processing services procured, introduced, integrated, or used by the Company.
3. Employees' AI usage behaviors in scenarios such as operational management, product research and development, data analysis, knowledge management, process automation, customer service, internal collaboration, and decision support.

III. Governance Structure

The Company promotes AI governance based on its existing governance structure, which is jointly executed by relevant responsible units.

1. Board of Directors: Oversees major AI governance directions, major risks, and important management progress.
2. Management Level: Supervises the promotion of the AI management framework, cross-departmental collaboration, and resource allocation.

3. ESG Promotion Office: Coordinates AI governance disclosure, cross-departmental coordination, and tracking.
4. Information Security Management Department: Responsible for AI-related information security controls, access management, monitoring and auditing, and incident response.
5. Legal Office / Management Department: Responsible for data protection, legal compliance, and reviewing usage guidelines.
6. Business and User Units: Handle AI introduction evaluation, daily management, document retention, and anomaly reporting according to their respective duties.

IV. Implemented Management Measures

(1) Hierarchical Authorization and Usage Restrictions for Sensitive AI Capabilities

The Company adopts hierarchical authorization and usage restrictions for AI capabilities involving sensitive data, high-risk uses, or potential impacts on personal rights. For AI applications involving image recognition, surveillance, mass processing of personal data, or significant impacts on the rights of individuals or third parties, the responsible unit must conduct risk identification, purpose review, authorization approval, and necessary supervisory measures according to internal procedures; without approval, unauthorized deployment, expansion of the usage scope, or external provision is prohibited.

(2) Appropriate Labeling of AI-Generated Content and AI-Influenced Outcomes

To enhance transparency and identifiability, the Company adopts appropriate disclosure, explanation, or manual review mechanisms for AI-generated or AI-assisted content according to the usage context. When users interact with AI systems, or when content is generated, organized, summarized, suggested, or outputted as decision support by AI, relevant units should adopt appropriate labeling or explanations based on the nature of the content and the level of risk, to avoid it being mistaken for purely human-generated content or an unreviewed final conclusion.

(3) Monitoring of Model Performance, Drift, and Anomalies

For AI models and applications developed in-house, continuously tuned, or requiring continuous maintenance by the Company, the responsible unit should establish continuous or regular performance monitoring, anomaly review, and necessary correction mechanisms based on the level of risk, and retain relevant review and

processing records. When there is a significant decline, deviation from expectations, or inconsistency with actual usage scenarios in model output quality, accuracy, applicability, or stability, or when there are other signs of model drift or performance degradation, analysis, adjustment, retraining, usage restriction, or suspension of use should be conducted according to internal procedures to maintain the reliability, appropriateness, and continuous effectiveness of the AI applications.

(4) Review of Fairness and Bias Risks

For AI applications involving the rights and interests of employees, customers, suppliers, or other stakeholders, the responsible unit of the Company shall conduct regular or as-needed bias risk identification, appropriateness review, and fairness assessment based on the level of risk, to prevent unfair, inconsistent, or discriminatory outcomes caused by data bias, design flaws, model logic, or improper use. For high-impact uses or deployed high-risk AI applications, measures such as manual review, parameter adjustment, usage restriction, supplementary data verification, reassessment, or suspension of use should be taken as appropriate to reduce bias risks and protect stakeholders' rights.

(5) Reducing Energy and Environmental Loads of AI Applications

During the introduction and use of AI tools, platforms, models, and related infrastructure, the Company incorporates considerations of energy efficiency, computing resource usage efficiency, data center sustainability, and supplier sustainability performance, and prioritizes the evaluation or selection of AI cloud, data center, model, or supplier solutions with better energy efficiency, lower resource consumption, or renewable energy commitments. The Company also helps improve energy management efficiency, optimize resource use, and support carbon reduction benefits through smart energy management systems, device monitoring and prediction systems, Edge AI, and related digital tools. Existing operations and sustainability management have also introduced relevant management foundations such as ISO 50001, ISO 14064-1, ISO 14001, and ISO 27001 to continuously strengthen energy management, resource efficiency, and information security resilience.

(6) AI-Related Grievance Mechanism

If stakeholders believe that the Company's AI applications, AI-generated content, AI-influenced outcomes, or related data processing behaviors affect their rights and interests, they may file a grievance or provide feedback through the grievance and contact channels publicly disclosed on the Company's official website. The Company

will accept, investigate, respond, correct, and track improvements based on the nature of the case. Official website grievance channel:
<https://www.ennconn.com/tw/consumer-protection-and-privacy/>

(7) Quantitative Tracking of AI Tools' Benefits to Sustainability and Operations

The Company continuously tracks the contribution of AI tools and related digital solutions to operational efficiency and sustainability outcomes, and gradually establishes quantitative indicators to support management decisions and information disclosure. Current tracking directions include but are not limited to:

- The benefits of AI/Edge AI applied to smart energy management, equipment monitoring and prediction, and process optimization.
- The contribution of AI tools to energy management, carbon reduction, resource efficiency, or productivity improvement.
- The outcomes of personnel training, tool usage, and digital transformation driven by AI empowerment.

2025–2026 Performance and Targets:

- Complete the promotion of basic AI empowerment in 2025.
- All 205 employees participating in the AI empowerment training program in 2025.
- Target to complete the cultivation of 31 AI seed members in 2026.
- The New Taipei City Government Administration Building saved a cumulative 1.8 million kWh of electricity from 2023 to 2025 through optimization using the AI software "Digital Twin system." Labor costs decreased by 21%, reducing the need for maintenance manpower by approximately 11 people.

(8) Employee Training on AI Ethics, Information Security, and Usage Capabilities

The Company has promoted the AI empowerment training program and introduced tools such as Gemini and NotebookLM to enhance employees' digital productivity and human-machine collaboration capabilities; simultaneously, combining information security and data protection requirements, it strengthens employees' awareness of AI usage risks, data processing, information security, and compliance requirements. Relevant training content covers AI ethics, data governance, privacy protection, information security, output identification, acceptable use policies, and precautions for high-risk applications. The Company will continue to promote education, training, and

advocacy on AI ethics, data governance, privacy protection, information security, output identification, and acceptable use policies based on different roles and application scenarios.

- Comprehensive introduction of AI technology in 2025.
- All 205 employees participating in the AI empowerment training program.
- Three-stage AI cultivation plan.
- Target to complete the cultivation of 31 AI seed members in 2026.
- Introduction of digital and information security tools such as Gemini, NotebookLM, Google Workspace, and SecOps.

V. External Verification

The Company continuously evaluates the feasibility of external verification for its AI management system, and will continuously refine it with reference to the ISO/IEC 42001 international management system standard based on actual implementation progress.

VI. Continuous Improvement

The Company will continuously review and improve the AI management framework in accordance with technological evolution, regulatory updates, stakeholder expectations, operational needs, and risk situations, and will disclose relevant indicators and progress based on actual implementation results.