

ENNOCONN CORPORATION

ARTIFICIAL INTELLIGENCE POLICY

Article 1 Purpose

Ennoconn Corporation (the “Company”) is committed to advancing industrial transformation, operational efficiency, and sustainable value creation through innovative technologies. In response to the rapid development and widespread application of artificial intelligence (“AI”), the Company establishes a responsible AI governance framework founded on the principles of human-centeredness, ethical business conduct, risk governance, information security, privacy protection, transparency, accountability, and sustainable development. This framework is intended to ensure that the research and development, introduction, deployment, use, operation, maintenance, and management of AI comply with applicable laws and regulations, social ethics, corporate governance standards, and stakeholder expectations.

This Policy serves as the Company’s highest-level governance principle for responsible AI. It is intended to enhance the trustworthiness of technology, protect stakeholder rights and interests, mitigate risk, and support corporate innovation, operational resilience, and sustainable development objectives.

Article 2 Scope of Application

This Policy applies to Ennoconn Corporation and its subsidiaries and sub-subsidiaries in which the Company directly or indirectly holds more than 50% of the equity interests. It covers the following circumstances:

1. AI systems, models, and applications independently or jointly developed, trained, fine-tuned, deployed, operated, or maintained by the Company.
2. The procurement, introduction, integration, or use of third-party AI tools, platforms, models, cloud services, and data-processing services.
3. Employees’ use of AI tools in operational management, product research and development, data analytics, knowledge management, process automation, customer service, internal collaboration, and decision support.
4. Activities involving AI technologies in products, services, or solutions provided to customers, or in the Company’s internal processes.

Article 3 International Frameworks and Legal Compliance

This Policy has been formulated with reference to the principles and spirit of the following international frameworks and legislation:

1. **OECD AI Principles:** The Company follows the internationally recognized core principles for trustworthy AI, including inclusive growth, sustainable development and well-being; human-centered values and fairness; transparency and explainability; robustness, security and safety; and accountability.

2. **UNESCO Recommendation on the Ethics of Artificial Intelligence:** The Company follows UNESCO's first global normative instrument on AI ethics, which protects human rights, fundamental freedoms, and human dignity, and promotes environmental and ecosystem sustainability.
3. **European Union Artificial Intelligence Act (EU AI Act):** The Company refers to the principles embodied in the world's first comprehensive AI regulatory framework, including risk-based governance, transparency disclosures, human oversight, AI literacy, and prohibited practices.
4. **Taiwan Artificial Intelligence Basic Act:** The Company follows the governance principles set forth therein, including sustainable development and well-being; human autonomy; privacy protection and data governance; cybersecurity and safety; transparency and explainability; fairness and non-discrimination; and accountability. The Company also takes into consideration its legislative direction concerning high-risk applications, risk classification, warning labels, allocation of responsibility, and remedies.

In addition to this Policy, the Company shall comply throughout the research and development, introduction, deployment, use, and management of AI with the laws and regulations of Taiwan and the jurisdictions in which it operates. These include, without limitation, the Artificial Intelligence Basic Act, the Personal Data Protection Act, and other laws, regulations, and competent-authority requirements governing intellectual property, trade secrets, labor rights and interests, consumer protection, information disclosure, industry supervision, and AI applications in regulated sectors.

Article 4 Governance Principles

1. Sustainable Development and Human-Centeredness

In promoting AI applications, the Company shall balance operational benefits with the public interest, environmental sustainability, digital inclusion, and the protection of human rights. AI shall support human autonomy, protect personality rights, and respect democracy, the rule of law, and cultural values. It shall not replace necessary human judgment, accountability, or safeguards for rights and interests.

2. Risk-Based Classification and Controls for High-Risk AI

The Company adopts a risk-based approach to AI applications. Risks shall be identified, classified, reviewed, and controlled according to the intended purpose, data type, data sensitivity, affected persons, degree of impact, reversibility, legal and regulatory requirements, and potential harm.

For purposes of this Policy, a "high-risk AI application" means the research and development, introduction, deployment, or use of AI whose purpose, data type, application context, or output may materially affect an individual's life, physical integrity, health, safety, privacy, fundamental rights, employment opportunities, or property interests, or may materially affect the Company's operations, legal and regulatory compliance, information security, or stakeholder rights and interests.

High-risk AI applications shall be subject to enhanced prior assessment, approval by accountable authorities, human oversight, warning labels, ongoing monitoring, incident reporting, exception escalation, and, where necessary, restriction or suspension.

3. Data Privacy and Data Governance

During the research and development, training, testing, deployment, and use of AI systems, the Company shall appropriately protect personal data, customer data, employee data, supplier data, trade secrets, and other sensitive information. The principles of lawfulness, fairness, necessity, purpose specification, and data minimization shall be observed.

Confidential, sensitive, restricted, or legally non-disclosable information shall not, without authorization, be entered into inappropriate external AI tools, platforms, or services. AI applications involving personal data shall be governed by controls for the collection, processing, use, retention, deletion, and cross-border transfer of such data in accordance with applicable laws and regulations.

4. Information Security and System Safety

Based on its existing information security management system, the Company shall implement appropriate security controls for AI systems and their related data, models, interfaces, operating environments, and third-party services. Such controls include, without limitation, identity authentication, tiered access authorization, data protection, log retention, vulnerability management, incident reporting, backup, recovery, and supply-chain security requirements, in order to reduce risks including unauthorized access, data leakage, model misuse, adversarial attacks, prompt injection, and other cybersecurity threats.

5. Prevention of Bias and Unfair Use

Throughout the design, data collection, training, testing, validation, deployment, and use of AI systems, the Company requires careful review of data sources, data quality, model logic, and application contexts to prevent data bias, design defects, or improper use from producing unfair, inconsistent, or discriminatory outcomes for particular individuals or groups.

For AI applications affecting the rights and interests of employees, customers, suppliers, or other stakeholders, the Company shall strengthen the identification and review of bias risks and, where necessary, implement human review, adjustment, usage restrictions, or discontinuation.

6. Human Judgment and Intervention in Significant Decisions

The Company does not permit AI, in the absence of appropriate human oversight, to make decisions independently where such decisions are irreversible, material, high-risk, or may affect individual rights and interests.

AI applications involving legal and regulatory compliance, personal data and privacy, information security, labor rights and interests, customer rights and interests, material operational risks, or other high-impact matters shall include clear mechanisms for human review, approval, intervention, reconsideration, rejection, escalation, or termination.

7. Transparency, Explainability, and Appropriate Labeling

Where appropriate, the Company shall disclose the fact that AI is being used, its purposes, principal capabilities, limitations, risks, and allocation of responsibilities. Where users interact with an AI system, or where content is generated or assisted by AI, appropriate disclosure, explanation, or labeling shall be provided according to the context.

For high-impact uses, the Company shall make reasonable efforts to provide an explanatory basis sufficient to support understanding, verification, and review. AI output shall not be treated as a final conclusion without verification.

8. Accountability and Traceability

Each AI application shall have a clearly designated accountable unit and allocation of responsibilities, including a business or product owner, data steward, system administrator, and personnel responsible for risk, legal and regulatory compliance, or information security review.

As necessary, the Company shall retain relevant documentation, decision records, review records, model versions, and anomaly-handling records to support accountability, internal management, compliance verification, investigations, and improvement. If an AI application results in error, bias, dispute, complaint, information security incident, or other adverse impact, the matter shall be reported, investigated, corrected, and improved in accordance with internal procedures.

9. Clear Boundaries for Permitted and Prohibited AI Activities

The Company shall establish clear authorization scopes, purpose limitations, usage rules, capability constraints, and prohibited activities for AI use. Without appropriate review and approval, AI shall not be used beyond its original intended purpose or authorized scope, or for a purpose lacking a legal basis or proportionate controls.

Employees shall not use AI to engage in forgery, deception, infringement, unauthorized disclosure, manipulation, circumvention of internal controls, violation of law, or other misconduct.

10. Low Ecological Footprint and Environmental Sustainability

The Company recognizes the potential impacts of AI on energy consumption, computing resources, water resources, and carbon emissions. It encourages consideration of energy efficiency, computing optimization, equipment and resource efficiency, infrastructure sustainability, and supplier sustainability performance throughout the research and development, deployment, procurement, and use of AI.

Where feasible, the Company shall give priority to models, platforms, data centers, or supplier solutions offering better energy efficiency, lower resource waste, and stronger sustainability performance.

11. Prohibition of Improper or High-Risk Misuse

The Company shall not develop, deploy, or support AI for any of the following purposes:

- (1)** AI systems that materially influence individual behavior through manipulation, deception, misleading practices, or intentional distortion.

- (2) AI systems that exploit age, disability, or socioeconomic vulnerability to exert improper influence, exploitation, or differential treatment.
- (3) AI systems that use social scoring to improperly classify or rank individuals or subject them to unreasonable differential treatment.
- (4) Real-time remote biometric identification or surveillance, or other privacy-infringing AI applications, without lawful authorization.
- (5) Other AI applications that violate laws or regulations, infringe human rights or privacy, endanger safety, disseminate misleading information, fabricate content, or are manifestly unfair.

12. AI Literacy, Education, Training, and Capacity Building

According to different roles, risk contexts, and application scopes, the Company shall continuously promote education, training, and awareness concerning AI ethics, data governance, privacy protection, information security, human-AI collaboration, identification and evaluation of AI outputs, and legal and regulatory compliance, in order to enhance the AI knowledge, risk awareness, and responsible-use capabilities of employees and relevant personnel.

Article 5 Governance Structure, Accountable Units, and Cross-Functional Responsibilities

The Company establishes an AI governance structure with clearly allocated responsibilities. The following roles and accountable units shall perform their respective duties to implement cross-functional collaboration and this Policy:

Governance Role	Level / Designated Accountable Unit	Specific Management Responsibilities
I. Highest Oversight Level	Board of Directors	1. Approve this Policy and subsequent amendments. 2. Receive management reports on AI governance and material risk-management progress. 3. Oversee and provide guidance on the Company's direction for the use of material AI technologies.
II. Management Oversight Level	Office of the President / Sustainability Development and Nomination Committee (ESG)	1. Promote implementation of this Policy and supervise related systems, resource allocation, and cross-functional collaboration. 2. Periodically review AI risk and compliance-audit progress, and report material developments and incidents to the Board of Directors.
III. Functional Review and Support Units	Information Management Department (IT) /	1. Conduct technical reviews of AI-system infrastructure and deployment environments.

Governance Role	Level /	Designated Accountable Unit	Specific Management Responsibilities
		Information Security Department (Sec)	2. Establish AI cybersecurity defenses and manage vulnerabilities, system backup, and log retention.
		Legal & Compliance Office	1. Review compliance for the introduction and application of AI. 2. Assist in drafting supplier contracts and data-licensing terms.
		Data Protection Office (DPO)	1. Review AI processes involving personal-data processing. 2. Ensure that data governance complies with the data-minimization principle and cross-border transfer requirements.
		Human Resources (HR)	1. Provide employee education and training on AI ethics and literacy. 2. Ensure fairness and human oversight in the use of AI for human-resources purposes.
IV. Implementing and User Units		Business, Product R&D, Project, and Operations Units	1. Manage, monitor, and document day-to-day risks arising from AI tools. 2. Immediately intervene and report when an anomaly occurs.

Article 6 Complaints, Incident Reporting, and Improvement

The Company shall establish appropriate mechanisms for reporting, investigating, handling, correcting, and improving concerns, complaints, accidents, deviations, information security incidents, privacy incidents, or other adverse impacts arising from AI use. Where necessary, corresponding measures shall be taken, including suspension, restriction, withdrawal, modification, stakeholder notification, or other appropriate action.

A stakeholder who believes that the Company's AI application or related data-processing activities have affected their rights or interests may submit a complaint or feedback through the complaint and contact channels publicly disclosed on the Company's website. The Company will accept, investigate, respond to, correct, and follow up on the matter according to its nature.

Website complaint channel: <https://www.ennconn.com/tw/consumer-protection-and-privacy/>

Article 7 Policy Review and Amendment

The Company will periodically review the appropriateness of this Policy in light of technological developments, legal and regulatory updates, international standards, stakeholder expectations, operational needs, and the evolving risk landscape, and will amend it as necessary to continuously improve its responsible AI governance mechanisms.

Article 8 Implementation

This Policy shall take effect upon approval by the Board of Directors. The same shall apply to any amendments.