Artificial Intelligence (AI) Management Policy

I. Purpose of the Policy

To regulate the use of Artificial Intelligence (AI) tools within EVE Energy Co., Ltd. (hereinafter collectively referred to as "EVE Energy", "EVE", the "Company", or "We"), enhance the safety and compliance of Artificial Intelligence (AI) applications, and effectively safeguard the data security and intellectual property rights of the Company, its clients, and business partners, this Policy is hereby formulated. As an integral component of the Company's AI governance framework, this Policy aims to provide support for responsible innovation and sustainable business operations.

II. Scope of Application

This Policy applies to all employees, interns, and outsourced personnel of the Company, as well as third-party partners who access AI tools using the Company's IT resources.

III. AI Governance Responsibilities

The Company strictly complies with applicable data protection laws and regulations in the countries or regions where it operates, including but not limited to the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, and the *General Data Protection Regulation (GDPR)* of the European Union. The Company has established an internal AI management mechanism approved by senior management, and designated a dedicated department to coordinate the promotion and daily management of AI applications. Each department is responsible for implementing AI usage risk management within its respective domain, ensuring that responsibilities are clearly assigned to specific roles and that effective measures are fully implemented.

The Company has comprehensively deployed and continuously advanced the following governance initiatives focusing on AI compliance and secure applications:

(1) **Enhancing Technical Control and Audit Mechanisms**

Establishing and improving the technical control and audit framework for AI usage. Regarding AI tool access, the Company formulates and dynamically updates a corporate-level AI tool access whitelist, and conducts regular security risk assessments for third-party AI tools. For deployed AI models, the Company implements periodic evaluations and audits to avoid potential bias in the use of AI models.

(2) **Improving AI System Transparency and Reliability**

Proactively disclosing the use cases, capability scope, and functional limitations of AI tools to enhance usage transparency. Conducting continuous validation and monitoring of deployed AI models, strictly regulating training data sources, promptly detecting and correcting model drift or performance degradation over time, and regularly implementing system maintenance and updates to ensure the stable and reliable operation of AI systems.

(3) **Deepening AI Application Assessment and Risk Prevention**

Establishing a normalized AI application assessment mechanism to regularly track AI usage and performance scores across departments, while concurrently conducting specialized assessments on information leakage risks, to ensure the safe and compliant deployment of AI technologies in various business scenarios.

(4) **Strengthening AI Security Training and Awareness for All Employees**

Organizing specialized raining on AI security and promoting the signing of the *AI Usage Commitment Letter* by all employees. Integrating data security and AI compliance requirements into the onboarding education system for new employees, thereby reinforcing employees' awareness and prevention capabilities regarding AI risks from the very beginning.

(5) **Clarifying Accountability Mechanisms**

Establishing a clear accountability framework for outcomes produced by AI. The head of each department serves as the primary person responsible for AI data security within their

respective department, overseeing execution and conducting regular self-inspections. In cases where improper AI usage leads to errors or causes damage, the Company will initiate investigation procedures in accordance with applicable laws and regulations, implement tiered accountability, and take timely and effective remediation measures to effectively prevent the escalation of risks.

IV. AI Usage and Tool Access Management

To clearly define the authorized scope and capability boundaries of AI tools, the Company has established a tiered management mechanism based on three levels of data classification. Differentiated AI usage rules are formulated accordingly to ensure that all AI applications operate securely within controllable parameters. The specific classifications and requirements are as follows:

Data Category	Definition	Usage Requirements
Red Line	Involves core technologies, unpublished patents, sensitive business data, etc	Strictly prohibited from being inputted into public AI tools in any form
Low-Risk Data	Does not contain specific trade secrets but requires desensitization before use	Must be desensitized; only Company-approved AI tools may be used
General Data	General knowledge unrelated to the Company's specific business	AI may be used, provided that no internal Company information is involved

Note: Examples of Red Line Data include core formulas, process parameters, unpublished R&D information, lists of core customers/suppliers, and pricing, etc.

(1) **Labeling and Usage Principles for AI-Generated Content**

The Company implements categorized management for AI-generated content and sets differentiated labeling requirements based on content formats and application scenarios

to enhance the transparency of AI-generated content and AI interactions. Any AI-generated content (including text, images, audio, and video) released externally or delivered for use must be distinctly and clearly labeled to ensure that stakeholders can clearly identify the source of the content, thereby safeguarding their right to know and the effectiveness of their decision-making.

AI outputs shall serve solely as supplementary references in the Company's critical business decision-making. Final decisions must be made by personnel with the appropriate authority to ensure the effective implementation of accountability.

(2) **Access Control for Sensitive AI Functions**

Access to sensitive AI functions, such as facial recognition and biometric analysis, is subject to strict permission controls. These functions are restricted to specific approved scenarios and shall not be deployed without authorization.

(3) **AI Tool Access and Risk Management**

The Company implements an access whitelist management system for AI tools and applies differentiated controls based on security assessment results. AI tools or agents deemed to pose significant security risks during evaluation (including but not limited to prompt injection, data leakage, and system vulnerabilities) are, in principle, prohibited from being deployed on the Company's intranet and office devices.

Where the use of such tools is genuinely required for special business scenarios such as technical research, use is permitted only upon authorization and under the precondition that no sensitive data is involved, risks are controllable, and network isolation and access control measures are fully in place.

V. Commitments on AI Applications

Adhering to the concept of Responsible AI, the Company makes the following commitments:

(1) Respect data privacy and safeguard cybersecurity. Do not use AI for any activities that may infringe upon data privacy, cybersecurity, intellectual property rights, trade secrets, or user privacy.

(2) Refrain from using or deploying AI systems that engage in manipulative behavior, exploitation of the vulnerabilities, social scoring, or unauthorized biometric surveillance.

(3) Establish an AI usage logging and regular audit mechanism to support internal governance and external oversight.

(4) Dynamically update the AI tool access whitelist and usage guidelines in response to technological advancements and evolving risk landscapes.

(5) Prioritize the use of the Company's unified private AI platform to ensure data security and controllability.

(6) Advance energy-saving renovations for proprietary data centers and optimize infrastructure energy consumption management to have a low AI ecological footprint, including but not limited to carbon and water footprints.

(7) Establish grievance mechanisms for users and third parties to provide appeals process for stakeholders affected by AI decisions or outcomes, thereby safeguarding their legitimate rights and interests.

VI. Policy Interpretation and Effectiveness

This Policy has been reviewed and approved by the Strategy and Sustainable Development Committee of the Company (a board-level committee). It is officially released to the public through official channels, such as the Company's website, and shall come into effect on the date of issuance. The Company reserves the right of final interpretation of this Policy.

EVE Energy Co., Ltd.

August 2026