东方日升负责任人工智能使用政策

Risen Energy Responsible Artificial Intelligence Use Policy

目的与适用范围 | Purpose and Scope

东方日升将人工智能视为支持运营效率、质量管理、数据分析、风险识别及数字化管理的辅助工具。同时，公司认识到，人工智能使用可能带来数据隐私、网络安全、偏差、透明度、责任归属及合规性等方面的风险。

Risen Energy recognizes artificial intelligence as a supporting tool for operational efficiency, quality management, data analysis, risk identification and digital management. The Company also recognizes that AI use may involve risks relating to data privacy, cybersecurity, bias, transparency, accountability and compliance.

本政策明确公司负责任使用人工智能的基本要求，适用于东方日升及下属子公司、员工及相关第三方服务商在业务活动中使用人工智能工具、模型、系统及相关应用的行为。

This Policy sets out the Company' s basic requirements for the responsible use of AI. It applies to Risen Energy, its subsidiaries, employees and relevant third-party service providers when using AI tools, models, systems or AI-enabled applications in business activities.

基本原则 | Basic Principles

公司对人工智能采取基于风险、保留人工监督的使用方式。人工智能可用于辅助分析、草拟、监测、预测、分类及流程改进，但不得替代专业判断、管理责任和个人的最终责任。

The Company adopts a risk-based and human-supervised approach to AI use. AI may

be used to support analysis, drafting, monitoring, prediction, classification and process improvement, but it shall not replace professional judgment, management responsibility or human accountability.

公司在人工智能使用过程中遵循合法合规、安全可控、公平审慎、透明可解释、责任明确和人工监督的原则。

In the use of AI, the Company follows the principles of legality, security, fairness, transparency, explainability, accountability and human oversight.

人工智能适用场景 | Appropriate Use of AI

公司可在适当业务场景中使用人工智能，包括生产工艺改进、质量检测辅助、预测性维护、研发分析、能源与碳数据管理、供应链风险筛查、市场研究、客户服务支持、翻译、文件起草、培训及内部知识管理等工作。

The Company may use AI in appropriate business scenarios, including manufacturing process improvement, quality inspection support, predictive maintenance, R&D analysis, energy and carbon data management, supply chain risk screening, market research, customer service support, translation, document drafting, training and internal knowledge management.

用于对外披露、客户沟通、监管提交、法律文件、财务事项或重大经营决策的 AI 生成内容，应在使用前经责任人员审核并批准。

AI-generated content used for external disclosure, customer communication, regulatory submission, legal documents, financial matters or major business decisions must be reviewed and approved by responsible personnel before use.

数据隐私与保密 | Data Privacy and Confidentiality

公司在人工智能使用过程中尊重数据隐私。个人信息、商业秘密、客户和供应商数据、未公开财务数据及敏感技术信息，应按照适用法律法规、公司数据分级管理要求及信息安全制度予以保护。

The Company respects data privacy in the use of AI. Personal information, confidential business information, customer and supplier data, unpublished financial data, trade secrets and sensitive technical information shall be protected in accordance with applicable laws, internal data classification rules and information security requirements.

未经授权，员工不得将保密或敏感信息输入公共人工智能工具。

Without authorization, employees shall not enter confidential or sensitive information into public AI tools.

网络安全 | Cybersecurity

公司保护人工智能使用过程中涉及系统的网络安全。相关部门应根据适用场景落实访问控制、数据保护、系统安全审查、漏洞管理和事件响应等措施。

The Company protects the cybersecurity of systems involved in the use of AI. Relevant departments shall, where applicable, apply access control, data protection, system security review, vulnerability management and incident response measures.

不得使用人工智能绕过安全控制、生成恶意代码、开展未经授权的系统测试，或以违反公司制度的方式处理数据。

AI shall not be used to bypass security controls, generate malicious code, conduct unauthorized system testing or process data in violation of Company policies.

公平性、偏差与人工监督 | Fairness, Bias and Human Oversight

公司努力避免 AI 辅助输出中可能存在的潜在偏差。不得以可能导致歧视、不公平对待或误导性结论的方式使用人工智能。

The Company seeks to avoid potential bias in AI-assisted outputs. AI shall not be used in a way that may result in discrimination, unfair treatment or misleading conclusions.

对于关键决策和高影响事项，公司保留人工参与并允许人工干预。责任人员应有权审查、质疑、纠正、否决或升级处理 AI 辅助结果。

For critical decisions and high-impact matters, the Company keeps humans in the loop and allows human intervention. Responsible personnel must be able to review, challenge, correct, override or escalate AI-assisted results.

涉及员工、供应商、客户、安全、合规、财务或法律事项的不可逆或高风险决策，不得仅以人工智能结果作为唯一依据。

AI shall not be used as the sole basis for irreversible or high-stakes decisions involving employees, suppliers, customers, safety, compliance, finance or legal matters.

透明度、可解释性与责任归属 | Transparency, Explainability and Accountability

公司在适当情况下推动人工智能系统透明度及 AI 生成结果的可解释性。使用人员在使用前应了解相关 AI 工具的目的、能力、局限和风险。

The Company promotes transparency of AI systems and explainability of AI-generated results where appropriate. Users should understand the purpose, capabilities, limitations and risks of AI tools before using them.

各使用部门应对本部门工作中采用的 AI 辅助输出的准确性、合法性、保密性和适当性负责。发

生错误输出、不当内容、数据泄露、安全事件或其他 AI 相关风险时，应及时报告并处理。

Each department using AI remains responsible for the accuracy, legality, confidentiality and appropriateness of AI-assisted outputs used in its work. Errors, inappropriate outputs, data leakage, security incidents or other AI-related risks shall be reported and addressed in a timely manner.

使用边界与禁止事项 | Boundaries and Prohibited Practices

公司明确人工智能可以做什么和不可以做什么。人工智能可辅助业务工作，但不得独立作出招聘、晋升、解聘、薪酬、纪律处分、供应商准入、客户信用、财务审批、法律承诺、对外披露或重大商业合同等最终决定。

The Company defines clear boundaries for what AI can and cannot do. AI may support business work, but it shall not independently make final decisions on recruitment, promotion, dismissal, remuneration, disciplinary action, supplier admission, customer credit, financial approval, legal commitments, external disclosure or major business contracts.

公司不得使用或部署涉及操纵性行为、利用个人脆弱性、社会评分、未经授权的生物识别监控，或适用法律法规禁止的其他人工智能系统，包括在适用情况下欧盟《人工智能法案》所禁止的人工智能实践。

The Company does not use or deploy AI systems involving manipulative behavior, exploitation of vulnerabilities, social scoring, unauthorized biometric surveillance or other prohibited practices under applicable laws and regulations, including prohibited AI practices under the EU AI Act where applicable.

第三方人工智能工具 | Third-Party AI Tools

在采用第三方人工智能工具或服务用于业务活动前，责任部门应关注其数据安全、隐私保护、知识产权风险、网络安全控制、服务可靠性及是否符合公司要求。

Before adopting third-party AI tools or services for business use, the responsible department should consider data security, privacy protection, intellectual property risk, cybersecurity controls, service reliability and compliance with Company requirements.

涉及公司数据处理、系统接入或业务流程嵌入的第三方人工智能工具，应根据公司采购、信息安全、合规及数据管理要求进行必要评估。

Third-party AI tools involving Company data processing, system access or integration into business processes shall be subject to necessary assessment in accordance with the Company' s procurement, information security, compliance and data management requirements.

政策批准、执行与持续改进 | Policy Approval, Implementation and Continuous Improvement

本政策由公司管理层批准。流程与信息中心总监负责统筹本政策的实施、监督、定期审查和更新，并协同相关业务及职能部门推进落实。

This Policy is endorsed by the Company' s Executive Management. The Director of the Process and Information Security Center is responsible for coordinating the implementation, monitoring, periodic review and update of this Policy, in collaboration with relevant business and functional departments.

随着人工智能技术和监管要求持续发展，公司将根据法律法规、业务需求、技术发展及风险管理

要求，适时审查并更新本政策。

As AI technology and regulatory expectations continue to evolve, the Company will review and update this Policy where necessary based on laws and regulations, business needs, technology development and risk management requirements.

总裁/签名（**President** Signature）：

日期（Date）： July 2026