TCL Zhonghuan Renewable Energy Technology Co., Ltd.

Responsible Artificial Intelligence Management Policy

1. Introduction

As a global leader in the new energy photovoltaic (PV) industry, TCL Zhonghuan Renewable Energy Technology Co., Ltd. and its subsidiaries (hereinafter referred to as “TCL Zhonghuan”, “we” or “the Company”) are committed to driving sustainable development through technological innovation. We continue to advance smart manufacturing and digital transformation, and actively explore the application of artificial intelligence (AI) technologies in areas such as crystal growth process control, intelligent quality inspection, production planning and scheduling, digital twin factories, supply chain collaboration, operations management and customer service.

We fully recognize that, while AI technologies improve production efficiency, product quality and resource efficiency, they may also give rise to risks relating to data security, privacy protection, algorithmic bias, lack of transparency, unclear accountability and environmental impacts. Guided by the principles of “safety and trustworthiness, human-centricity, fairness and transparency, clear accountability, and green development”, the Company has formulated this Responsible Artificial Intelligence Management Policy (hereinafter referred to as “this Policy”). This Policy sets out the Company’s management structure, principles, requirements and actions for AI governance, so as to ensure that the development, procurement, deployment and use of AI technologies comply with applicable laws and regulations, international guidelines and the Company’s sustainability goals, and to promote the safe, reliable, compliant and sustainable application of AI.

2. Scope

This Policy applies to TCL Zhonghuan’s headquarters and all of its wholly-owned and controlled subsidiaries. All directors, senior management and employees of the Company are required to comply strictly with this Policy. This Policy covers all AI systems, models, algorithms, tools and services that are independently developed, jointly developed, externally procured, deployed or used by the Company (hereinafter collectively referred to as “AI systems”), throughout their entire lifecycle, from planning and design, data preparation, development and training, testing and validation, and deployment, to operational monitoring and decommissioning.

At the same time, this Policy applies to suppliers, contractors, technology service providers and partners involved in the development, deployment or operation of the Company’s AI systems. We encourage

external strategic partners, upstream suppliers and downstream channel partners to comply with this Policy and to work together with us to build a responsible AI ecosystem.

3. Commitments

TCL Zhonghuan attaches great importance to the potential impacts of AI applications on its employees, customers, partners, suppliers, communities and the general public (hereinafter collectively referred to as “stakeholders”). We commit to developing and using AI in a responsible manner, ensuring that AI always serves and assists people, and firmly oppose any development or application of AI that infringes on personal privacy, endangers cybersecurity, results in unfair discrimination or harms the lawful rights and interests of stakeholders.

We are committed to complying with all applicable laws, regulations and regulatory requirements, 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, the Interim Measures for the Management of Generative Artificial Intelligence Services and the Measures for Labeling Artificial Intelligence-Generated and Synthetic Content. We actively draw on guidelines such as the Ethical Norms for New Generation Artificial Intelligence, the Organisation for Economic Co-operation and Development (OECD) AI Principles and the UNESCO Recommendation on the Ethics of Artificial Intelligence, and continuously monitor regulatory developments in China and abroad, including the EU Artificial Intelligence Act (EU AI Act), so as to update the Company’s management requirements in a timely manner.

The Company has incorporated AI governance into its overall risk and compliance management. Building on its ISO 27001-certified information security management system and its Privacy Protection Policy, the Company extends its data security, privacy protection and cybersecurity requirements across the entire AI lifecycle. The Company actively refers to the ISO/IEC 42001 AI management system standard to improve its governance framework, and is exploring external independent verification of its AI management system, so as to ensure the professionalism and international compliance of its governance system.

Using 2026 as the base year, the Company commits to achieving, by 2030, the core control targets of keeping the number of major AI security and ethics incidents at zero each year, achieving 100% risk assessment coverage of newly deployed AI applications, and achieving 100% coverage of responsible AI training for employees in AI-related positions, so as to continuously strengthen its AI risk prevention and control capabilities.

4. Strategies

4.1 Management Structure

The Board of Directors is the highest decision-making and supervisory body for the Company's responsible AI management. It is responsible for reviewing major matters related to the Company's AI governance and overseeing the implementation of this Policy.

The General Manager serves as the primary responsible person (the person in charge at the highest decision-making level) of the Company's Digital Transformation Committee (hereinafter referred to as the "DTC"), which is the highest management-level body responsible for the Company's AI strategy and responsible AI management. The DTC is responsible for approving this Policy, formulating the Company's AI development strategy and governance principles, approving high-risk AI applications, and regularly receiving reports on AI risk management.

The DTC has established a Responsible AI Working Group, which is led by the Information Security Technology Team and composed of the digital/IT, legal and compliance, audit, human resources, sustainability (ESG) and relevant business departments. The Working Group is responsible for implementing this Policy and related systems, and for organizing the registration and filing, risk assessment, compliance review, monitoring and auditing, and training and awareness of AI applications.

Each business department and subsidiary bears primary responsibility for the AI applications within its unit, and shall designate a model owner and a responsible business lead for each AI system, who are responsible for the system's day-to-day operation, performance monitoring, risk identification and issue rectification. The Company's Audit Department is responsible for independent oversight and auditing of the implementation of this Policy.

4.2 Respecting Data Privacy and Protecting Personal Information

The Company respects data privacy in the use and development of AI, and strictly protects personal information and data security throughout the development, training, deployment and operation of AI systems, in line with the Company's Privacy Protection Policy:

(1) Adhere to the principles of lawfulness, legitimacy, necessity and good faith. Data used for training and operation must come from lawful sources and be authorized for use. Data involving personal information shall be subject to minimal collection and authorization management, and shall not be used beyond its original purpose without the consent of the data subjects;

(2) Establish a data classification and grading management mechanism, and apply protective measures such as de-identification, anonymization, encryption and access control to sensitive personal information and trade secrets;

(3) Establish a data lifecycle management mechanism covering the entire process of data collection, storage, use, sharing, archiving and deletion; where cross-border data transfer is involved, strictly complete the security assessment, filing or certification procedures required by applicable laws and regulations;

(4) Prohibit employees from entering the Company's trade secrets, personal information or other protected data into external AI tools or services that have not been approved by the Company;

(5) Regularly conduct AI-related data privacy risk assessments and internal reviews.

4.3 Protecting the Cybersecurity of AI Systems

The Company incorporates AI systems into its overall information security and cybersecurity management system to protect the cybersecurity of systems in the use and development of AI, and to ensure that AI systems are stable, reliable and controllable:

(1) Establish secure design and secure development requirements for AI systems, embedding security requirements into system planning, development and go-live review processes;

(2) Implement tiered access control and operation log auditing for models, training data, algorithm code and operating environments;

(3) Conduct model security testing and vulnerability management to prevent risks such as data poisoning, model theft, adversarial attacks, prompt injection and unauthorized access;

(4) Implement network isolation and abnormal traffic monitoring for AI applications in industrial control scenarios to ensure the safe operation of production systems;

(5) Conduct cybersecurity due diligence on third-party AI products and services;

(6) Establish an incident response mechanism for AI security incidents, and include AI systems in the scope of the Company's regular vulnerability scans, cybersecurity attack and defense drills, and internal and external audits.

4.4 Keeping Humans "in the Loop" and Allowing Human Intervention

Adhering to a human-centric approach, the Company ensures that AI always assists rather than replaces human judgment, and keeps humans "in the loop" for critical decisions. Decisions involving

personal safety, employee rights and interests, customer interests, or major business, financial, legal and compliance matters shall not be made solely by AI systems:

(1) Establish human review, human intervention and final decision-making mechanisms according to the risk level of each application scenario, ensuring that critical decisions can be reviewed, adjusted or overridden by authorized personnel;

(2) In manufacturing scenarios, AI process control systems shall be monitored by authorized personnel during operation, who retain the authority to intervene, switch to manual control or perform an emergency stop at any time; abnormal results identified by systems such as AI-powered quality inspection shall be verified by humans in accordance with prescribed procedures;

(3) Define human intervention authority and escalation procedures, and establish mechanisms to identify, correct and roll back abnormal AI outputs;

(4) Prevent employees from developing undue reliance on AI outputs, and ensure that users are capable of understanding and evaluating AI-generated results.

4.5 Ensuring Transparency and Explainability

The Company is committed to ensuring the transparency of AI systems and the explainability of AI-generated results and decisions, and to enhancing their traceability and trustworthiness:

(1) Establish an AI application inventory to register and manage the scenarios, purposes, responsible persons, risk levels, model versions, deployment status and compliance assessment results of the Company's AI applications, and make necessary disclosures on major AI application scenarios and governance through channels such as the Company's sustainability report;

(2) Clearly inform users when they are interacting with an AI system (e.g., intelligent customer service); uploading the Company's trade secrets, customer information or sensitive business data to unapproved public AI services is prohibited;

(3) Adopt review, labeling or explanatory measures for AI-generated or synthetic content in accordance with applicable laws and regulations and the relevant use scenarios, and ensure that such content undergoes human review before external release;

(4) Establish record-keeping mechanisms for model development, training data, version changes and deployment, and retain traceable information on key decision-making processes;

(5) Where technically feasible, enhance model explainability by giving priority to interpretable features and methods, and provide the necessary rationale for decisions in important business scenarios.

4.6 Avoiding Potential Bias and Ensuring Fairness

The Company is committed to promoting fair, impartial and inclusive AI applications and avoiding potential bias in the use and development of AI. The Company's AI applications are currently concentrated in industrial manufacturing scenarios. For AI applications that may affect individual rights and interests, such as recruitment, performance evaluation and attendance management, the Company applies stricter fairness management:

(1) Identify potential bias during model design, training and validation, and improve the representativeness and quality of training data;

(2) Prohibit AI systems from subjecting individuals to unjustified differential treatment on the basis of gender, age, ethnicity, race, nationality, religious belief, marital or childbearing status, disability or other factors;

(3) Conduct algorithmic fairness testing for high-impact scenarios involving individual rights and interests, and establish mechanisms to identify, monitor and correct bias;

(4) Regularly assess deployed AI systems for the fairness and consistency of their outputs.

4.7 Establishing Clear Accountability for AI Outcomes

The Company adheres to the principles of "clearly defined responsibilities, aligned authority and accountability, and end-to-end traceability", and establishes clear accountability for outcomes produced by AI models and tools:

(1) Define the responsibilities of the Board of Directors, the DTC, the Responsible AI Working Group, business departments and functional departments in AI governance;

(2) Designate a model owner and a responsible business lead for each AI system, who bear management responsibility for the system's compliance, security and operational outcomes;

(3) Users of AI systems bear corresponding responsibility for the decisions they make based on AI outputs;

(4) Establish mechanisms for the reporting, investigation, rectification and continuous improvement of AI risk incidents, and conduct root cause analysis and accountability tracing for issues arising from AI applications;

(5) Provide employees, customers and other parties affected by AI-driven decisions with channels for explanation, appeals to contest AI decisions or outcomes, and human review.

4.8 Risk Assessment and Tiered Management

The Company implements tiered risk management for AI applications throughout their lifecycle:

(1) Before project initiation or procurement, the responsible business department shall register the AI system and conduct a preliminary risk identification, classifying it as high, medium or low risk according to the degree of its potential impact on personal safety, production safety, the rights and interests of employees and customers, personal information, business decisions and the environment;

(2) High-risk AI applications (including but not limited to applications involving biometric identification or the processing of sensitive personal information, applications affecting the material rights and interests of employees or customers, and applications that may have a significant impact on personal safety or production safety) shall undergo an AI impact assessment prior to deployment. The assessment shall cover data security and privacy protection, algorithmic fairness, safety and reliability, transparency, human rights and environmental impacts, and such applications may go live only upon approval by the DTC;

(3) Medium- and low-risk AI applications shall be included in the Company's information system go-live review process and undergo security assessment and compliance review;

(4) A new risk assessment shall be conducted when an AI system undergoes material changes or an expansion of its intended use, or when a major risk incident occurs.

4.9 Model Monitoring and Auditing

The Company has established continuous monitoring and auditing mechanisms for AI models to ensure that they remain reliable and effective throughout their lifecycle:

(1) Before go-live, AI models shall complete functional, performance, security and reliability testing and validation, and may be deployed only after meeting predefined metrics;

(2) After go-live, continuous monitoring mechanisms shall be established to detect and correct drift or degradation of AI models over time, tracking key indicators such as accuracy, false detection rate, missed detection rate and stability, with timely alerts, corrections or rollbacks when anomalies are identified;

(3) Establish a model version management mechanism under which model retraining and iterative updates are subject to testing, validation and approval, with complete version records retained;

(4) Regularly review model performance, suitability and risk levels, and optimize or decommission models that no longer meet requirements;

(5) Include AI management in the scope of the Company's internal audits and compliance inspections, with the Audit Department regularly auditing the implementation of this Policy.

4.10 Defining Clear Boundaries and Prohibited AI Practices

The Company ensures that AI systems operate within an authorized, controllable and appropriate scope. AI shall not act as an independent decision-making entity, nor replace human responsibilities prescribed by laws and regulations. The Company defines clear boundaries for each AI system, specifying its purpose, permissions and applicable scenarios, and prohibits any use beyond the authorized scope. Access to sensitive AI capabilities such as facial recognition and biometric identification is limited through approval, permission controls and log auditing. The Company prohibits the development, procurement, deployment or use of AI to engage in the following activities:

(1) Manipulative or deceptive behavior, or otherwise improperly influencing individuals' autonomous decision-making;

(2) Exploitation of the vulnerabilities of vulnerable groups, or exerting unfair influence on them;

(3) Social scoring of individuals leading to detrimental treatment;

(4) Biometric identification and surveillance that is unauthorized or exceeds lawful purposes, illegal facial recognition, and profiling of individuals;

(5) Illegal collection, use or sharing of personal data;

(6) Generating or disseminating false information, committing fraud or producing malicious content;

(7) Activities that infringe on human rights or violate internationally recognized ethical principles;

(8) Other AI applications prohibited by laws and regulations.

4.11 Green and Low-Carbon AI

As a new energy company, the Company integrates the philosophy of green development into the entire lifecycle management of AI:

(1) When procuring and deploying AI products and services, consider their energy efficiency and carbon emission performance, and give priority to more energy-efficient solutions and to data centers and cloud services powered by renewable energy;

(2) Continuously optimize the use of computing resources in model training and inference to reduce the ecological footprint of AI operations;

(3) Leverage AI to promote energy conservation and consumption reduction, yield improvement, green manufacturing and efficient resource utilization, and progressively quantify the contribution of AI applications to the Company's sustainability goals.

4.12 Third-Party and Supply Chain Management

The Company extends its responsible AI requirements to AI-related cooperation with third parties:

(1) Conduct due diligence on AI suppliers and technology service providers to assess their data protection, cybersecurity and model security capabilities, their compliance with relevant international regulations and their ethics management capabilities, and clearly define compliance responsibilities in contracts;

(2) Clearly set out requirements on data protection, security and confidentiality, intellectual property, allocation of responsibilities and this Policy in cooperation agreements;

(3) Regularly evaluate the risks and performance of third-party AI products and services, and promptly take measures such as rectification, suspension or termination of cooperation when major risks are identified.

4.13 Complaints and Penalties

We continuously improve our existing internal reporting and communication mechanisms and channels through which employees, customers, partners, suppliers and other relevant parties can report AI-related risk incidents or violations, or file objections and appeals to contest AI decisions or outcomes, and we regularly review and improve our responsible AI practices. Relevant parties may report directly to a supervisor or to the Company's Audit Department, or through the telephone number or email address below.

Tel: 022-23789766-8022

Email: jubao@tzeco.com

Address: No. 10 Haitai South Road, Huayuan Industrial Park, Xiqing District, Tianjin

The Company supports anonymous reporting and commits to keeping whistleblowers' personal information strictly confidential and effectively safeguarding their lawful rights. The Company strictly prohibits any direct or indirect discrimination, obstruction, suppression or retaliation against whistleblowers.

For any violation of this Policy or of AI-related laws and regulations, we adopt a zero-tolerance approach, promptly conducting investigations and taking corrective action against unlawful or non-compliant

conduct, and imposing corresponding disciplinary sanctions on the responsible departments and personnel according to the degree and scope of the impact caused by the incident.

4.14 Education and Training

The Company continuously enhances employees' awareness of and capabilities in the responsible use of AI:

(1) Incorporate AI-related data security, privacy protection and compliant use requirements into the annual information security training for all employees;

(2) Provide dedicated training on AI ethics, model security and the compliant use of generative AI for personnel involved in AI development, operation and maintenance, and use;

(3) Strengthen the AI governance capabilities of management and employees in key positions, and promote case studies of responsible AI practices.

5. Policy Review and Revision

The Board of Directors is the highest decision-making and supervisory body for the Company's responsible AI management. The release of this Policy and the related commitments has been endorsed by the Company's executive management. The Responsible AI Working Group is responsible for the version management of this Policy, which will be reviewed at least once a year and updated and revised as appropriate. The review covers changes in relevant laws and regulations, developments in international standards and technology, changes in customer and regulatory requirements, and the Company's internal AI applications and management. In the event of any material change, an updated version will be released promptly to ensure that the content of this Policy remains current and applicable.

This Policy is published on TCL Zhonghuan's official website for reference by all stakeholders, and is communicated to employees and key stakeholders through emails, meetings, internal learning platforms and other means. Its implementation and the related key performance indicators are disclosed annually in the Company's sustainability report.