



Trina Solar Co., Ltd

Responsible AI Management Policy

Responsible Department	Process Digitalization Department		
Supporting Department	Risk Control Management Department		
Approved By	ESG Management Committee		
Document No.	TSL-ESG-001	Effective Date	2026-09-01

1. Purpose

Trina Solar Co., Ltd., together with its branches and wholly owned or controlled subsidiaries (collectively, "Trinasolar" or "the Company"), uses technological innovation to advance sustainable development and actively explores applications of artificial intelligence (AI) in research and development, intelligent manufacturing, operations management, supply chain collaboration, customer service, risk management, and other areas. The Company recognizes that, while AI can create value, it may also pose risks involving data security, privacy, algorithmic bias, lack of transparency, accountability, and environmental impact. This Policy establishes requirements for the development, procurement, deployment, use, and management of AI systems. Its purpose is to support the safe, lawful, fair, transparent, and sustainable use of AI in the Company's operations and to manage related risks. The Company adopts the principles of legality and compliance, safety and control, fairness and transparency, human oversight, accountability, and sustainable development. This Policy is based on the laws and regulations applicable where the Company operates and takes into account relevant national and international AI standards.

2. Scope

This Policy applies to AI-related activities conducted worldwide by Trina Solar Co., Ltd., its branches, and its wholly owned or controlled companies. It covers all employees and management personnel, as well as AI systems, products, models, and services that the Company develops independently, helps develop, procures, deploys, or uses. These include, without limitation: (a) large-scale models developed or deployed locally within the Company; (b) external third-party large-scale models and AI services procured, deployed, or used by the Company; and (c) AI systems independently developed or co-developed by the Company.

Through contracts, agreements, procurement terms, or other appropriate means, the Company shall require suppliers, contractors, consultants, and partners that participate in the development, deployment, or operation of AI systems, or provide related services on behalf of the Company, to comply with the applicable requirements of this Policy. The Company also encourages its supply chain partners to improve responsible AI management practices.

3. Definition

Description	Definition
Artificial Intelligence System (AI System)	<i>It refers to an engineered system that, for a given set of human-defined objectives, generates outputs such as content, predictions, recommendations, or decisions.</i>
Large-scale Model	<i>It refers to a deep learning model trained on large volumes of data, with a complex computational architecture, capable of handling complex tasks and demonstrating a degree of generalization.</i>
Fairness	<i>It refers to the property of an AI system whereby its treatment, conduct, or outcomes respect established facts, social norms, and beliefs and are not affected by favoritism or unjust discrimination.</i>
Transparency	<i>It refers to the property of an AI system that enables it to communicate appropriate information about the system to stakeholders.</i>
Explainability	<i>It refers to the ability of an AI system to express, in a way people can understand, the material factors that influence its outputs or actions.</i>
Human-in-Command	<i>It refers to a form of oversight in which a human retains ultimate control over, and the right to override, an AI system.</i>
Human-on-the-Loop	<i>It refers to a form of oversight in which a human monitors an AI system in real time or near real time.</i>
Human-in-the-Loop	<i>It refers to a form of oversight in which an AI output may be acted upon only after human review and approval.</i>
Applicable Law	<i>It refers to any law, regulation, policy, rule, order, decision, judicial interpretation, treaty, judgment, ruling, international, local, industry or association standard, or other legal requirement applicable to the Company in relation to AI management.</i>

4. Content

4.1 Core Principles

4.1.1 Compliance with laws and regulations. The Company shall comply with Applicable Law and ensure that AI systems remain lawful throughout their life cycle.

4.1.2 Safety and control. The Company shall establish a security management framework covering the entire AI life cycle. The framework shall protect both the AI system itself and the external environment and guard against cyberattacks, data breaches, model misuse, and other risks.

4.1.3 Fairness and transparency. The Company shall ensure that AI decision-making is fair and impartial and does not discriminate based on race, sex, age, religion, disability, or other protected characteristics. The Company shall provide appropriate transparency regarding the use of AI and AI-generated content, and protect stakeholders' right to know when AI is used in decision-making.

4.1.4 Human oversight. The Company shall maintain meaningful human oversight and intervention for critical decisions. Irreversible or high-impact decisions shall not be executed entirely by an AI

system.

4.1.5 Accountability. The Company shall establish accountability for AI management and hold organizations at every level responsible for carrying out their assigned duties and obligations.

4.1.6 Sustainable development. The Company shall consider the environmental impact of AI systems and take measures to reduce the energy consumption and carbon emissions associated with AI computing resources, supporting green and low-carbon development.

4.2 Requirements for the Use of AI Systems

4.2.1 When developing or deploying an AI system, the Company shall define its authorized use cases, capability boundaries, and limitations in the relevant technical documentation. The AI system shall not be used outside the authorized scope.

4.2.2 In any of the following circumstances, the department requesting the AI system shall submit a risk assessment to the Company's Data Compliance and Security Assessment Team in accordance with the Company's Data Security Risk Assessment Policy. The risk assessment shall describe the intended use case, purpose, types of data involved, and expected impact:

- (a) the development of a new AI system, or the introduction or deployment of a new AI system developed by an external third party;
- (b) the processing of Company data classified as Level C or above; or
- (c) a material change or update to the AI system.

4.2.3 If an AI system behaves unexpectedly or departs from its intended use, the issue shall be reported immediately to the head of the AI development team or the AI deployment team, as applicable.

4.2.4 Prohibited AI Practices

- (a) **Illegal activities are prohibited.** AI systems shall not be used, deployed, or applied for any activity that violates Applicable Law, including inciting the subversion of state power; endangering national security or interests; damaging the national image; inciting separatism; undermining national unity or social stability; promoting terrorism, extremism, ethnic hatred, or ethnic discrimination; or disseminating violent, obscene, or pornographic content.
- (b) **Infringement is prohibited.** AI systems shall not be used, deployed, or applied to infringe or improperly use a third party's intellectual property, including copyrights, trademarks, patents, and trade secrets. They shall not be used to infringe the lawful rights and interests of others, including

rights of portrait, reputation, honor, privacy, and personal information, or to endanger another person's physical or mental health.

- (c) **High-risk activities are prohibited.** AI systems shall not be used or deployed for high-risk activities, including:
- (i) systems that use subliminal, purposefully manipulative, or deceptive techniques in a manner that causes or is likely to cause significant harm or distorted behavior;
 - (ii) harmful manipulation of a person's behavior or exploitation of a person's vulnerabilities, including vulnerabilities related to age, disability, or a specific socioeconomic situation;
 - (iii) evaluations or classification of individuals in a manner that may result in discrimination or harm, including judgments based on social behavior or personal characteristics;
 - (iv) creation of facial or emotion-recognition databases through untargeted scraping of facial images;
 - (v) emotion recognition in the workplace, except for medical or safety purposes;
 - (vi) biometric categorization systems that infer sensitive characteristics from biometric data, including race, religion, age, sexual orientation, and political opinions; or
 - (vii) real-time remote biometric identification (RBI) systems in public places.
- (d) **Malware is prohibited.** AI systems shall not be used to create or distribute malware or any content intended to facilitate unauthorized access to or use of computer systems or data.
- (e) **Misrepresentation is prohibited.** An application that uses an AI system shall not mislead end users about, or fail to disclose, the presence of AI. AI shall not be used where known risks or hazards are not addressed through appropriate safeguards, oversight, and human control.
- (f) **Unverified reliance is prohibited.** Information generated by an AI system shall not be relied upon until its accuracy, potential harm, and other risks specific to the intended use have been assessed.

4.3 Data Compliance and Personal Information Protection

4.3.1 When designing, developing, deploying, or using an AI system, data shall be collected and processed lawfully, for a legitimate purpose, only to the extent necessary, and with appropriate security. To ensure lawful and compliant data collection:

- (a) when automated tools are used to collect data, their impact on third-party network services shall be assessed. Such tools shall not unlawfully intrude into another party's network or interfere with

the normal operation of its network services;

- (b) the collection and use of open-source datasets shall comply with the applicable open-source license or otherwise be authorized;
- (c) the collection or use of personal data shall comply with Section 4.3.3 of this Policy; and
- (d) when data is obtained from an external third party through procurement, collaboration, or another arrangement, the data, representations, and supporting compliance documentation provided by the counterparty or partner shall be reviewed.

4.3.2 Intellectual property protection shall be incorporated into the design, development, deployment, and use of AI systems. Infringement shall be prevented when training data are selected and when outputs are generated.

4.3.3 Where personal information is processed at any stage in the design, development, deployment, or use of an AI system, the processing shall comply with Applicable Law, the Company's Personal Information Protection Management Policy, and other relevant internal requirements, including the following:

- (a) personal data may be processed only with the data subject's consent or on another lawful basis;
- (b) only the minimum personal data necessary to provide the relevant function may be collected, and excessive collection, use, or storage of personal information shall be avoided; and
- (c) sensitive personal information may be processed only with the separate consent of the individual concerned or on another lawful basis.

4.3.4 Cross-border transfers of data shall comply with Applicable Law governing such transfers and with the Company's Cross-border Data Compliance Management Policy and other relevant internal requirements.

4.4 Cybersecurity

4.4.1 AI systems shall be developed and deployed in accordance with the Company's Secure Development Management Standard. Software shall be developed in accordance with the Secure Coding Standard and shall meet applicable security requirements. Before an AI system goes live, it shall undergo penetration testing and may be launched only if the test results meet security requirements.

- 4.4.2** Company data classified as Level B or above shall be encrypted when stored or transmitted within an AI system. The encryption algorithms used shall comply with national, international, and industry standards.
- 4.4.3** Each type of training data, including text, images, audio, and video, shall be filtered in full before it is used for training. Filtering methods may include keyword filters, classification models, and manual sampling. Unlawful and harmful information shall be removed.
- 4.4.4** Inputs to AI systems shall be continuously monitored. Protective measures, such as prompt shields, shall be used to guard against malicious input attacks, including injection attacks, data theft, and adversarial attacks.
- 4.4.5** The Company shall establish capabilities for monitoring AI system operations and maintain security incident response plans. It shall conduct regular response exercises and promptly refine its response strategies in light of industry security incidents, significant public concerns, and regulatory changes so that evolving security risks are addressed.

4.5 Fairness

- 4.5.1** Before training data are used, the size and balance of the dataset shall be explored and the data shall be preprocessed to ensure diversity and representativeness. Based on the analysis, necessary measures such as data cleaning, screening, supplementation, or rebalancing shall be taken to identify and reduce potential bias caused by inappropriate data distributions.
- 4.5.2** Throughout algorithm design, model training and optimization, and service delivery, fairness risks shall be identified in light of the specific use case. Measures such as training-data screening and output validation shall be used to reduce the risk of discrimination based on ethnicity, belief, nationality, region, sex, age, occupation, health, or similar characteristics.
- 4.5.3** Each AI system shall undergo a bias audit regularly, and at least once a year, to identify potential fairness risks and support appropriate corrective measures.

4.6 Human Involvement and Intervention

- 4.6.1** The Company applies a three-tier human oversight framework:

Tier	Applicable systems	Oversight required
Tier 1 Human-in-	All AI systems	Ability to stop, veto, or override AI

Tier	Applicable systems	Oversight required
Command		outputs at any time
Tier 2 Human-on-the-Loop	AI systems used in automated decision-making	Real-time intervention and suspension of AI system operations
Tier 3 Human-in-the-Loop	AI systems used in irreversible or high-stakes decisions	Review, approval, or rejection of recommendations produced by the AI system

4.6.2 Where a decision is irreversible or high-stakes, an AI system may provide recommendations only.

The final decision shall be made by a human manager. Such decisions include, without limitation:

- (a) decisions that may have an irreversible or high-stakes impact on an individual's employment, credit, health, safety, liberty, or other fundamental rights, including hiring, termination, promotion, and demotion;
- (b) material business decisions, including significant financial decisions, critical production safety decisions, and legal or compliance determinations; and
- (c) other activities that may have an irreversible or high-stakes impact on the Company's business or on an individual.

4.6.3 Any person who identifies an obvious error in an AI system's output or a risk of harm shall immediately suspend the relevant operation and report the matter to the head of the AI development team or the AI deployment team, as applicable.

4.6.4 If an affected individual objects to an AI-assisted decision, the Company shall promptly arrange for the relevant business department to conduct a human review. The review shall be completed within a reasonable period, and the individual shall be notified of the outcome in writing.

4.7 Transparency and Explainability

4.7.1 Users shall be clearly informed when they are interacting with, or receiving services from, an AI system rather than a natural person. They shall also be informed of material risks and limitations associated with the system's outputs.

4.7.2 AI-generated content released externally, including text, images, audio, and video, shall carry a label where required by Applicable Law.

4.7.3 Explanations shall be understandable and tailored in detail to different stakeholders. For example,

users should receive information about the system's purpose and decision results, while product providers should receive information about the algorithmic model and operating environment.

4.8 Environmental Sustainability

4.8.1 The Company is committed to taking effective measures, including drawing on its strengths in new energy, to reduce the life-cycle ecological footprint of AI data centers and large-scale models, including energy consumption, water use, and carbon emissions. Sustainable AI development will form part of the Company's ESG strategy.

4.8.2 Environmental sustainability shall be included in the criteria used to evaluate external third-party AI system and large-scale model suppliers. The Company will give preference to suppliers with a smaller environmental footprint.

4.9 Accountability and Liability

4.9.1 An AI system shall not be treated as an independent legal person. Legal responsibility for an AI-assisted decision rests with the relevant human accountable party:

- (a) **AI system developer.** For an AI system developed internally, the head of the development team is responsible for the system's technical design, the compliance of its training data, and its baseline security performance;
- (b) **AI system deployer.** When the Company deploys an AI system developed by an external third party, the head of the deployment team is responsible for the system's suitability, compliance of the use case, and the final deployment decision; and
- (c) **AI system user.** The person who actually uses an AI system is directly responsible for the specific operations performed, the manner in which the system is used, and the resulting outcomes.

4.9.2 Any violation of Applicable Law or this Policy that subjects the Company to an administrative penalty, dispute, financial loss, harm to brand or reputation, or another adverse effect (collectively, an "Adverse Effect") shall be investigated in accordance with the Trinasolar Employee Handbook and the Company's Business Misconduct and Accountability Management Policy. Disciplinary action shall be imposed in accordance with the applicable classification of the violation, the seriousness of the circumstances, and the prescribed disciplinary levels and procedures. If the conduct

constitutes a criminal offense, the Company may refer the matter to the competent authority for investigation of legal liability.

4.10 Training and Capability Building

4.10.1 The Company shall continue to strengthen employees' awareness of and ability to use AI responsibly. Training shall be tailored to job responsibilities and risk levels and cover AI ethics and compliance, data security and privacy protection, cybersecurity, model security, and related topics. The Company shall promote examples of responsible AI practices and strengthen the AI governance capabilities of management and personnel in key roles.

4.10.2 Based on business needs, the Company may provide specialized training or capability assessments for personnel involved in the development, procurement, deployment, operation, or use of AI systems. The objective is to ensure that they understand each system's authorized scope, capability boundaries, risk requirements, and human oversight responsibilities.

4.11 Monitoring, Appeals and Continuous Improvement

4.11.1 The Company shall establish mechanisms for AI risk monitoring and continuous improvement. It shall regularly conduct internal reviews, compliance checks, and risk assessments of its AI management framework; develop corrective measures for identified issues; and track their implementation. AI management requirements shall be updated as appropriate to reflect Applicable Law, regulatory requirements, technological developments, industry practices, and stakeholder feedback.

4.11.2 The Company shall provide channels for reporting AI risk incidents and appealing disputed outcomes, and shall accept feedback and oversight from employees, customers, suppliers, and other stakeholders. Objections to an AI-assisted decision shall be reviewed and handled by a human in accordance with the human involvement and intervention requirements of this Policy.

5. Supplementary Instruction

5.1 References

NO.	Document Name	Document NO.
-----	---------------	--------------

1	Interim Measures for the Management of Generative AI Services	
2	EU AI Act (Regulation (EU) 2024/1689)	
3	Artificial Intelligence - General Principles for Trustworthiness (GB/T 47507-2026)	

5.2 Revision Record

Document No.	Version	Responsible person for drafting/revising	Effective Date	Revision Details and Reason
TSL-ESG-001	V01	Process Digitalization Department	2026-09-01	New Version Releases

5.3 Special Instructions

The Board of Directors serves as the highest decision-making and oversight body for this Policy. The publication of the relevant policy and commitments has been endorsed by the Board of Directors and senior management. The Process Digitalization Department leads responsible AI management and is responsible for version control, interpretation, annual review, and updates to this Policy. The Risk Control Management Department supports responsible AI management and organizes relevant departments to identify and assess AI risks and conduct oversight and continuous improvement. Each business and functional department is responsible, within its remit, for managing the AI systems it develops, procures, deploys, or uses.

This Policy remains effective for two years and shall, in principle, be reviewed at least annually. It shall be revised promptly if there is a material change in Applicable Law, regulatory requirements, technology, or the Company's business. When a new policy is issued, the previous policy is automatically repealed. If another Company policy governing AI conflicts with this Policy, this Policy prevails.