晶科能源
www.jinkosolar.com
中国上海市闵行区申长路1466弄1号
201106
No. 1, Lane 1466,
Shenchang Road, Minhang District,
Shanghai, China
电话:(86)21-5180 8777
传真:(86)21-5180 8600
Tel:(86)21-5180 8777
Fax:(86)21-5180 8600

# Jinko Solar Information Security and Privacy Protection Policy

Version: 2026V1.1

## 1. Overview

Jinko Solar Co., Ltd. (hereinafter referred to as "Jinko Solar" or "the Company") strictly complies with 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 Administrative Measures for the Multi-Level Protection of Information Security, and other applicable laws, regulations and requirements. With reference to ISO/IEC 27001, the Company has established an information security management system to strengthen information risk controls and implement information security safeguards. The Company also attaches great importance to privacy protection and, with reference to ISO/IEC 27701, Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management- Requirements and Guidelines (hereinafter referred to as the "Privacy Information Management System"), advances compliant privacy data management throughout the data lifecycle. The Jinko Solar Information Security and Privacy Protection Policy (hereinafter referred to as this "Policy") is intended to regulate the Company's data processing activities, ensure effective governance of information security and privacy protection, and safeguard the legitimate rights and interests of the Company and its stakeholders.

## 2. Scope of Application

This Policy applies to all business and operational activities of the Company and its branches and subsidiaries. The Company encourages all directors, members of senior management and employees, as well as value chain partners (including service providers, suppliers and business partners), to follow this Policy and jointly protect information security and privacy. This Policy also applies to the Company's mergers, acquisitions and other business transactions, as well as due diligence activities, worldwide. The Company is also committed to exercising its influence over non-controlled joint ventures and encouraging them to act in accordance with this Policy.

## 3. Publication Statement

The Risk Compliance and ESG Management Committee is responsible for version control of this Policy and the commitments herein. The Information Security and Confidentiality Management Department, the Infrastructure & Information Security Department and other relevant departments track annual management progress and review and update the relevant policies and procedures, subject to review and confirmation by the Board of Directors and senior management. As a general rule, this Policy is reviewed annually to ensure that it remains current and applicable. This Policy is prepared in both Chinese and English. In the event of any inconsistency between the two versions, the Chinese version shall prevail. This Policy is publicly available in the ESG section of Jinko Solar's website, and key stakeholders are informed through emails, meetings, online notifications and other means.

**4. Commitments and Targets**

In accordance with the requirements of the ISO 27001 Information Security Management System and the ISO 27701 Privacy Information Management System, the Company continues to improve and upgrade its information security management system and integrates its information security policies and related practices into Company-wide risk and compliance management. The Company treats the private information of key stakeholders (including customers, employees and suppliers) as strictly confidential, adheres to the principles of lawfulness, fairness and necessity, and closely monitors information security and privacy protection matters affecting all stakeholders. The Company commits to obtaining authorization through relevant contracts or agreements, separate privacy agreements or other written notices, thereby ensuring that authorization or consent is obtained from 100% of relevant stakeholders, and to respecting their rights to be informed, to make decisions and to request deletion, among other rights relating to their information.

By the end of 2030, the Company commits to maintaining 100% coverage of cybersecurity risk assessments and core data leakage risk assessments, and achieving 100% coverage of its core systems by third-party ISO 27001/ISO 27701 certification.

**5. Actions and Practices**

**5.1 Governance Structure and Dedicated Functions**

The Board of Directors is the highest oversight body for information security and confidentiality management and is responsible for determining the relevant strategies and policies. The Company has established the Information Security and Confidentiality Committee as the highest decision-making body for information security and privacy protection matters. It comprises members of senior management (including the CIO and CEO) and the Data Protection Officer (DPO). The management support layer is the Information Security and Privacy Protection Working Group, consisting of the Information Security and Confidentiality Management Department and the Information Security Department. The execution and implementation layer is composed of the heads of the various systems and departments, together with information security and privacy protection liaisons. All employees form the supervision and participation layer. In addition, the Company has formulated supporting policies, including the Confidentiality Management Policy and the Data Security Management Policy, to strengthen security management throughout the data lifecycle, ensure data confidentiality and integrity, and effectively protect the privacy of internal and external stakeholders.

**5.2 Compliance Management and System Development**

The Company strictly complies with 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 Administrative Measures for the Multi-Level Protection of Information Security, and other applicable laws, regulations and requirements. In accordance with the ISO 27001 Information Security Management System and the ISO 27701 Privacy Information Management System, the Company regularly conducts internal information security audits covering all business operations, builds end-to-end safeguards encompassing data collection, storage and transmission, adopts advanced technologies, and continuously improves its information security risk warning and emergency response capabilities. Each year, the Company engages third-party organizations to review the security of IT-related systems and infrastructure and professional assessment organizations to conduct specialized multi-level protection assessments of information systems. All systems are subject to penetration testing and vulnerability scanning, including simulated hacker attacks, before going live, to ensure that no medium- or high-risk vulnerabilities remain. Server vulnerability scans are performed every six months, with remediation completed within prescribed time limits. Systems undergoing material changes are subject to penetration testing once or twice a year on average, depending on their importance, and identified deficiencies and areas for improvement are remediated.

**5.3 Information Security and Privacy Protection for Stakeholders**

The Company treats the private information of key stakeholders (including customers, employees and suppliers) as strictly confidential and adheres to the principles of openness, lawfulness and fairness. Before collecting information, the Company obtains authorization through cooperation agreements, separate privacy agreements or other written notices, thereby ensuring that authorization or consent is obtained from 100% of relevant stakeholders, and provides an opt-out option to stakeholders who do not consent to information collection. During collection, the Company follows the principle of data minimization and does not receive or collect additional irrelevant information. The types of personal information collected, together with the source, purpose, method of collection and intended use of each item, are presented in an easy-to-understand manner (such as in tables). Text notices, pop-ups, links and other means are used to explain the purposes of collection and related matters, ensuring that processing occurs only after the data subject has been informed and has provided explicit consent. When sharing data with third parties (such as business partners and service providers), the Company obtains the data subject's explicit consent, informs the data subject of the type of recipient and the purpose of sharing, signs confidentiality agreements, and conducts regular security reviews. The Jinko Solar Code of Conduct for Supply Chain Partners also sets out the respective confidentiality responsibilities and obligations of the Company and its supply chain partners. The Company regularly conducts stakeholder due diligence to verify the effectiveness of partners' information security measures.

The Company fully respects stakeholders' control over their information and ensures that they may access data they have shared, transfer such data to other processors, and correct or delete the information as appropriate. Information already obtained is managed in compliance with applicable requirements through encrypted storage, strict controls over extraction procedures, activity audits and other measures. The Company also commits not to use the information of key stakeholders (including customers, employees and suppliers) for secondary purposes and to promptly delete information that is no longer necessary.[1]

The Company retains relevant data (including personal data) in accordance with business needs and legal obligations, generally for no longer than is necessary to achieve the intended purpose, namely the minimum period required for business purposes. The Company's Data (Including Personal Information) Retention Period Requirements specify retention periods for various types of records. For example, routine operational data (such as meeting minutes) are generally retained for three years, while market research reports are generally retained for five years.

**5.4 Information Security and Privacy Risk Management**

The Company manages confidential information responsibly. It continuously establishes and improves its vulnerability analysis mechanism and systematically identifies potential security weaknesses in information systems through processes including identification and collection, prioritization, remediation and verification, and closed-loop management. This creates a continuous improvement cycle of "identification-assessment-remediation-verification" and builds a proactive security defense for the organization.

Led by the Information Security and Confidentiality Management Department, the Company carries out information security and privacy protection work by reviewing whether collection channels are lawful and compliant and whether the scope of collection follows the principle of data minimization. During data storage, it evaluates the security of storage systems, including the risks of equipment failure, cyberattacks and access-control vulnerabilities. During data transmission, it reviews whether encryption technologies are properly applied to prevent data from being stolen or tampered with in transit. The Company then performs quantitative risk assessments based on the likelihood and impact of each risk. Based on the assessment results, corresponding response strategies are developed according to risk level. For material risks, the Company also formulates specific response strategies, including emergency response, recovery, remediation and prevention measures.

**5.5 Internal Controls and Data Leakage Prevention**

The Company standardizes operating procedures across all operations, classifies and grades data by information sensitivity, applies different levels of restriction, and improves lifecycle management across data creation, collection, modification, use, transfer, storage and destruction. Internal data access permissions are established so that employees may access, edit or upload

[1] In recent years, through systematic monitoring, the Company has not identified any information of key stakeholders (including customers, employees and suppliers) being used for secondary purposes. In 2025, the proportion of information of key stakeholders (including customers, employees and suppliers) used for secondary purposes was 0%.

data only within the scope of their authorization. Systems record activity logs in real time to ensure traceability. The Company has also established a global zero-trust network and an Enterprise Mobility Management (EMM) secure mobile workspace. By using security technologies such as zero-trust remote access, it separates employees' workspaces from their personal environments and reduces the risks arising from remote access to internal systems by untrusted endpoints. The Company also requires partners (including suppliers) to comply with its privacy security protection requirements. Suppliers involved in processing private data must sign dedicated data governance compliance agreements to maintain high standards of compliance in their data processing activities.

**5.6 Business Continuity**

The Company proactively identifies core business scenarios and the information systems, data and resources on which they depend. It assesses potential security risks in each system, analyzes the specific financial, compliance and reputational impacts of system disruption, prioritizes systems for management according to the severity of impact, and uses the results to establish business recovery time objectives and strengthen its incident response planning (IRP) capabilities.

**Pre-incident prevention:** The Company continuously advances improvements to technology projects and business management and promptly updates and upgrades supporting security protection equipment, data encryption systems and access-control software. These measures improve the security and confidentiality of information systems and safeguard business continuity at source. In addition, the Information Security and Confidentiality Committee leads an annual assessment of potential security incidents and organizes one cybersecurity emergency drill for critical systems each year. Centered on scenarios involving system anomalies and privacy information leakage caused by cyberattacks, the drills simulate the full process of responding to cybersecurity emergencies and enhance employees' overall emergency response capabilities.

**Incident response:** To ensure business continuity, the Company has established a comprehensive information security emergency response mechanism and an Information Security Emergency Leadership Team. Guided by the principles of "prevention first, full participation and tiered accountability," the Company conducts emergency management and response. In the event of a major information security incident, it immediately collects network traffic, logs, information on suspicious processes and other evidence; investigates and identifies the cause; assesses the level of risk; and promptly activates and implements the relevant emergency response plan to maintain normal business operations.

**Post-incident improvement:** The Company records the entire information security incident handling process and conducts a post-incident review. When business conditions change, it promptly updates its Business Impact Analysis (BIA) and adjusts the relevant information security Business Continuity Plan (BCP) based on the results, ensuring that the plan meets mainstream standards and the needs of business development. The Company also focuses on training and communications concerning incident reporting to improve the team's security awareness and capabilities.

**5.7 Information Security and Privacy Education and Training**

The Company fosters an information security culture in which "everyone values and everyone participates" by establishing Company-wide mechanisms for information security communications, education, rewards and penalties. Online and offline training, lectures, case studies and other formats are used to enhance the information security and confidentiality awareness of all employees. Information security training is mandatory for all employees, including new hires. Upon joining the Company, all employees are required to sign the Letter of Commitment on the Use of Office Software and the Facial Information Authorization and Disclaimer & Personal Information Privacy Policy Notice. All employees must strictly comply with internal requirements, including the Information Security and Privacy Protection Management Policy, and are encouraged to assume personal responsibility for information security and confidentiality management and to proactively report security vulnerabilities and disciplinary, regulatory or legal violations identified in their daily work. The IT service desk regularly collects suggestions from all employees on improving IT services, and the Company uses this feedback to continuously improve its information security and privacy protection systems.

**5.8 Disciplinary Measures for Information Security and Privacy Violations**

The Company has zero tolerance for disciplinary, regulatory or legal violations involving privacy security. Employees who violate privacy security requirements will be subject to measures commensurate with the severity and impact of the violation. Minor incidents may result in criticism and education; moderate incidents may result in performance-related deductions, disgorgement of improper gains or other penalties; and serious incidents may result in termination of employment. Matters involving suspected criminal or other unlawful conduct will be referred to the judicial authorities.

**6. Information Security and Privacy Protection Reporting Procedure**

The Company fully respects the individual rights of employees and customers. Subject to applicable laws and regulations, data subjects may decide how their private data are collected, used, retained and processed. The Company provides individuals with opt-in and opt-out options and clear, convenient channels through which employees and customers may request access to data held by the Company and request correction or deletion. Any organization or individual has the right to submit a complaint or report to the responsible department regarding unlawful data or privacy processing or conduct that violates technology ethics. The Company's confidentiality principle is "mutual supervision, focused prevention, and a combination of rewards and penalties." Every Jinko Solar employee has a duty to oversee information security and confidentiality. Suspected violations or information leakage incidents may be reported through the Company's information security mailbox at JKIS@jinkosolar.com or directly to the relevant departmental information security liaison or the Information Security and Confidentiality Management Department.

Reports may be made anonymously, and the identity of the reporting person will not be disclosed. Upon receiving a report, the

Information Security and Confidentiality Management Department will arrange for an investigator to contact the reporting person within 24 hours. If the matter is confirmed to involve a disciplinary, regulatory or legal violation relating to information security or privacy protection, the Department will coordinate the investigation. After the investigation is completed, the reward and penalty procedure will be initiated based on the findings, and the data subject will be promptly informed of the outcome. The Company also encourages employees to identify and report potential information security issues through the Information Security Rationalization Suggestion Process, submit innovative suggestions for improving information security, and encourage departments to participate actively in implementing such suggestions. At its discretion, the Company may reward reporting persons whose substantiated reports are confirmed through investigation, individuals who actively prevent information leakage incidents, employees who submit information security rationalization suggestions, and departments that participate in implementing such suggestions, where they have made a material contribution.

**Appendix: Document Revision Record**

| Document | Jinko Solar Information Security and Privacy Protection Policy | | |
|---|---|---|---|
| Version | Revision Description | Effective Date | Issuing Body |
| 2025V1.0 | This Policy was issued in response to information security and privacy protection laws, regulations and international standards. It is intended to regulate data processing activities, strengthen risk controls, and advance compliant privacy data management throughout the data lifecycle. | 2025.7 | Risk Compliance and ESG Management Committee |
| 2026V1.1 | Improved the policy approval process; added information security and privacy protection targets; refined the Actions and Practices section; and enhanced the core principles of the reporting procedure. | 2026.8 | Risk Compliance and ESG Management Committee |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Note: Minor adjustments arising from similar matters during the year will be consolidated by version in the Document Revision Record. For questions regarding the version or content of this Policy, please contact ESG@jinkosolar.com. Thank you for your interest in Jinko Solar's ESG management.