电话:(86)21-5180 8777
传真:(86)21-5180 8600
Tel:(86)21-5180 8777
Fax:(86)21-5180 8600
Shanghai, China

Version: 2026V1.1

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 [1]

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

[illegible] Republic [illegible] 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 warning and emergency response capabilities. Each year, the Company engages third-party organizations to review the security of IT-related systems and network 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.

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 accordŸ[1]

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.

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.

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.

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

The Company fosters a [illegible] in which [illegible]

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 sugges

| 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.