Information Security and Privacy Protection Policy of Jinko Solar

一、 Introduction

Jinko Solar Co., Ltd. (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 Graded Protection of Information Security* and other information security-related laws, regulations, as well as relevant provisions. With reference to ISO/IEC 27001 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements (referred to as "Information Security Management Systems"), the Company has established an information security management system to strengthen information risk control and implement information security protection measures. At the same time, the Company attaches great importance to privacy information protection. With reference to ISO/IEC 27701 Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management - Requirements and Guidelines (referred to as "Privacy Information Management Systems"), the Company comprehensively promotes compliance management throughout the entire lifecycle of private data. The Information Security and Privacy Protection Policy of Jinko Solar (referred to as "the Policy") aims to regulate the Company's data processing activities, ensure effective governance of information and privacy security, and safeguard the legitimate rights and interests of the Company and all of the Company's stakeholders.

二、 Scope of Application

The Policy applies to all business and operational activities of the Company and its subsidiaries. It also encourages all directors, senior management, and employees of the Company, as well as value chain partners (including service providers, suppliers,

business partners, etc.) to adhere to the Policy and jointly protect information and privacy security. The Policy is applicable simultaneously to all business activities of the Company such as mergers and acquisitions and due diligence activities carried out globally. The Company also undertakes to exert influence on non-controlling joint ventures and urges them to act in accordance with the relevant provisions of the Policy.

三、 Release Statement

The Policy is compiled by the Risk Compliance and ESG Management Committee. The release of relevant policies and commitments has been approved by the Company's senior management and employees of the business focal department. Generally, the review and revision cycle of the Policy is yearly, to ensure the timeliness and applicability of the Policy. The Policy is prepared in both Chinese and English versions. Any inconsistency between the Chinese and English versions, the Chinese version shall prevail.

四、 Commitments and Actions for Information Security Management

Jinko Solar commits to continuously promoting the improvement and upgrading of its information security management system, integrating the implementation of information security management policies and related work into the risk and compliance management processes throughout the Company. The Company regularly conducts internal and external audits of the compliance of information security management policies to ensure their effective implementation.

- **Information security and confidentiality organization system:** The Company has established an Information Security and Confidentiality Committee to centrally coordinate the information security and confidentiality efforts. The Board of Directors is the highest coordinating level for information security and confidentiality management. It is responsible for determining the information security and confidentiality management strategy, reviewing the information security and confidentiality policy, and supervising the implementation progress of

information security and confidentiality issues. Mr. Chen Kangping[1], the director of the Company, serves as the top responsible person. The highest decision-making level of the Committee is composed of the CXO and the heads of various business systems. Among them, the CIO is the main responsible person, responsible for the overall management and supervision of the implementation process of the information security and confidentiality strategy. The management support level is represented by the Information Security and Confidentiality Working Group, which is composed of the CEO Office and the Information Technology System. The execution level is composed of the heads of various systems and departments as well as the information security interface personnel. The supervision and participation level is composed of the entire employees. These levels work in close coordination to ensure that information security and confidentiality management responsibilities are effectively reinforced at every level.

- **Improving the information security management system construction:** The Company commits to dynamically optimizing the system framework and technical standards related to information security, and building a protection system covering the entire chain of data collection, storage and transmission. The Company commits to introducing cutting-edge technologies and continuously enhancing the capabilities of information security risk early warning and emergency response. The Company commits to conducting regular safety training for all staff to enhance their awareness of information security and operational norms. The Company commits to continuously optimizing and upgrading the construction of the information security management system through all-round control measures.

[1] Mr. Chen Kangping, was born in 1973 and holds a master's degree. From 2003 to 2006, he was the CFO of Zhejiang Supor Co., Ltd. From 2007 to December 2022, he served as a director of JinkoSolar Holding Co., Ltd. From December 2008 to December 2020, he served as the CEO of JinkoSolar Holding Co., Ltd., in charge of the overall strategic planning and operation management, including but not limited to strategic planning, information security, financial stability, compliance governance, etc. Since September 2014, he has served as a director of Jinko Power Technology Co., Ltd. Since December 2020, he has been the director and General Manager of Jinko Solar Co., Ltd. (This paragraph is compiled with reference to the information in the 2024 annual report of Jinko Solar Co., Ltd.)

- **Information security management system audit:** The Company conducts internal information security audits covering all business scopes every year. Additionally, the Company invites third-party institutions to audit the security of IT-related systems and infrastructures yearly, and also invites professional evaluation institutions to conduct special audits for National Cybersecurity Level Protection yearly. The Company enhances its information security management system construction by referring to ISO 27001 Information Security Management Systems and commits to achieving a 100% coverage rate of third-party certification of the ISO 27001 Information Security Management Systems for core systems by the end of 2025.

- **Information security risk management:** The Company responsibly manages confidential information and commits to achieving a 100% coverage rate of cybersecurity risk assessment and core data leakage risk assessment by the end of 2025. Meanwhile, the Company has been constantly establishing and improving the vulnerability analysis mechanism. According to the processes of "identification and collection, priority ranking, repair and verification, and closed-loop management", the Company systematically identifies potential security flaws in the information system and forms a continuous improvement system of "identification - assessment - repair - verification" to build an active defense security barrier for the organization. The Company requires that all systems undergo penetration testing and vulnerability scanning before launching, including simulated hacking tests, etc., to ensure that there are no medium-to-high-level security risks. Server vulnerabilities are scanned every six months, with mandatory remediation within a set timeframe. For systems undergoing significant changes, penetration tests are conducted 1-2 times per year on average, based on their importance.

- **Preventing unauthorized access or disclosure of data:** The Company implements various internal control measures to restrict the unauthorized acquisition or access of internal data and ensure the security of data.

  （1） All employees are required to protect internal data and proprietary and confidential information at all times to prevent potential harm to internal data

and any other individuals or third parties who have authorized their information to be kept by the Company.

（2） The Company standardizes operational procedures across all operational scopes, sets different levels of restriction according to information classification, and implements a categorized and graded data management approach.

（3） The Company has set internal data access permissions. Employees can only perform various operations such as access, editing, and uploading within the authorized permissions. The system records the operation traces in real time to ensure the traceability of the operation flow.

（4） The Company has used security technologies such as Zero Trust Remote Work to separate the employees' workspace from the private space, reducing the risk of untrusted terminals remotely accessing the Company's internal systems.

- **Cultivation of information security culture:** The Company regards the information security culture as an important cornerstone for sound development. Through the establishment of information security communication, publicity and education, reward and penalty systems covering all employees, the Company fosters an all-round information security culture atmosphere.

  （1） The primary responsibility of all employees: All employees are at the supervision and participation level in information security and confidentiality management. All employees should strictly abide by the Company's systems on information security and confidentiality management, proactively fulfill their responsibilities for information security and confidentiality management, and actively report any cybersecurity vulnerabilities and disciplinary violations, regulatory violations and illegal acts discovered in daily work.

  （2） Employee information security training: The Company enhances all employees' awareness of information security and confidentiality through various methods, including online and offline training sessions, lectures, case

studies, etc. Information security and confidentiality training is a compulsory course in the all-staff training plan of the Company, including newly hired staff.

（3） **Employee information security feedback collection:** The Company regularly collects IT-related service improvement suggestions from all employees through the Online IT Service Desk and continuously enhances the construction of the information security and privacy protection system based on the feedback received.

- **Business continuity guarantee:** The Company actively formulates the information security-related Business Continuity Plans (BCP). By establishing a risk management mechanism of "prevention before the incident, response during the incident, and improvement after the incident", the Company minimizes the impact of information security incidents on business activities, ensuring the continuity, stability, and compliance of organizational operations.

（1） **Business Impact Analysis (BIA):** The Company actively sorts out the core business scenarios and clarifies the information systems, data and resources business activities rely on. Additionally, the Company actively assesses the potential security risks of each system and analyzes the specific impact of system disruptions on finance, compliance and reputation. The Company classifies the priority of system management according to the degree of impact, and determines the time target for business recovery accordingly.

（2） **Prevention before the incident:** The Company continuously promotes the rectification of technical projects and business management, promptly updates and upgrades supporting facilities such as security protection equipments, data encryption systems, access control softwares, etc., to enhance the security and confidentiality of its information systems and ensure business continuity from the source. Additionally, the Company conducts a cybersecurity drill for critical systems every year. With system abnormalities caused by cybersecurity attacks as the core scenario, the Company simulates the whole cybersecurity

emergency responding process, to improve the emergency responding capabilities of full-time and part-time employees in cybersecurity positions.

（3）**Response during the incident:** To ensure business continuity, the Company has established a complete information security emergency management mechanism. The information security emergency leading group has been set up to carry out emergency management and response in accordance with the principles of "prevention first, full participation, and hierarchical responsibility". When any major information security incidents occur, the Company will investigate and identify the cause of incidents immediately, and promptly start and implement the emergency response plans to ensure normal business operation.

（4）**Improvement after the incident:** The Company records the entire responding process and summarizes the information security incidents. In response to changes in business operations, the Company updates the Business Impact Analysis (BIA) in a timely manner and adjusts the information security-related Business Continuity Plans (BCP) based on the results of Business Impact Analysis (BIA) to ensure that the relevant Business Continuity Plans (BCP) comply with mainstream standards and business development needs.

- **Business partner management:** The Company requires its business partners (including suppliers etc.) to actively comply with its information security and privacy protection relevant systems and requirements. Before establishing cooperation with key suppliers, the Company actively conducts due diligence related to information security to ensure that there are no significant risks. The Company incorporates information security and privacy protection requirements into the *Jinko Solar Supply Chain Partner Code of Conduct*, and requires all suppliers to sign and abide by it. The Company also requires its business partners to sign a confidentiality agreement to clearly define the confidentiality responsibilities and obligations of both parties. Additionally, the Company regularly evaluates and monitors the effectiveness of business partners' information security measures to mitigate information security risks during the cooperation process.

五、 Commitments and Actions for Privacy Protection

Protecting the security and confidentiality of the privacy information of stakeholders is of crucial importance to Jinko Solar. Therefore, the Company will strictly comply with the laws and regulations related to privacy protection when conducting business activities. It is hoped that the following policies will help you understand what information the Company may collect, how to use and protect this information, and with whom this information will be shared.

- **Privacy security governance:** The Company has set up the Information Security and Confidentiality Management Department within the CEO Office as the centralized department for the entire lifecycle compliance management of privacy data. At the same time, the Company has formulated regulations such as the *Confidentiality Management System*, and the *Data Security Management system* to strengthen security management throughout the entire data lifecycle, ensure data confidentiality and integrity, and effectively protect the privacy of internal and external stakeholders.
- **Privacy security risk management:** The Company incorporates risks related to information security and privacy protection of core stakeholders into comprehensive risk management, and conducts risk management related to information security and privacy protection in accordance with the logic of "risk identification, risk assessment, and risk control and response".

  （1） **Risk identification:** The Information Security and Confidentiality Management Department takes the lead in conducting a comprehensive identification of risks related to information security and privacy protection. In the data collection phase, it examines whether the collection channels are legal and compliant, and whether the scope of collection adheres to the principle of minimality and necessity. During the data storage phase, it assesses the security of storage systems, including risks of equipment failures, cyber attacks, permission management vulnerabilities, etc. In the data transmission phase, it

focuses on whether encryption technologies are properly applied to prevent data from being stolen or tampered with during the transmission process.

（2）**Risk assessment:** The Company conducts quantitative risk assessment based on the likelihood of risk occurrence and the degree of impact. Risks with a high likelihood of occurrence and significant impact are classified as high-risk levels and require priority handling. Risks with a low likelihood of occurrence and minimal impact are classified as low-risk levels but still need continuous monitoring.

（3）**Risk control and response:** Corresponding response strategies are formulated according to risk levels, including refining operation specifications at each stage of the entire data lifecycle, strictly implementing the data classification and grading storage strategy, establishing a data access approval process, regularly conducting privacy security and compliance training, and carrying out supervision and inspection of privacy security risks. For major risks, the Company has also developed special response strategies, including emergency response, recovery response, remedial response, and preventive response.

- **Privacy security management system audit:** The Company includes privacy security management as a significant issue in both internal and external information security audits. Professional privacy security audits are carried out yearly along with internal and external information security audits, which mainly cover the compliance and the implementation of privacy policies. The Company actively pursues certification of the privacy information management system and commits to achieving a 100% coverage rate of third-party certification of the ISO 27701 Privacy Information Management Systems for core systems by the end of 2026.
- **Privacy security management principles:** The Company regards the privacy information of core stakeholders (including customers, employees, suppliers, etc.) as core confidential information, strictly adheres to the principles of "transparency, legality, and legitimacy", closely monitors stakeholder information security and privacy protection, and comprehensively prevents and controls privacy leakage risk.

The Company promises that customers have the right to determine how their personal data is collected, used, retained, and processed.

（1）**Before information collection:** The Company ensures 100% authorization or consent from stakeholders before collecting information by obtaining authorization in cooperation agreements, signing privacy agreements, or providing other written notices. Additionally, stakeholders who do not consent to information collection are given the option to opt out.

（2）**During information collection:** The Company adheres to the principle of minimality and necessity, refraining from receiving or collecting any irrelevant information. The Company also fully respects stakeholders' control rights over their information, ensuring stakeholders have the right to access the shared data, transfer the shared data to other processors, and request corrections or deletions of their information as appropriate.

（3）**Collected information:** The Company ensures compliant management of collected information through encrypted storage, strict extraction controls, and activity audits. Additionally, the Company commits not to use the information of core stakeholders (including customers, employees, suppliers, etc.) for secondary purposes and to delete unnecessary information in a timely manner.[2]

- **Overview of privacy information management:** The Company respects the right-to-know of stakeholders and fully informs them of the following privacy protection-related issues.

（1）**Nature of information captured:** Including but not limited to stakeholder names, attributes, contact information, basic introduction, special precautions, etc.

[2] In recent years, through systematic monitoring measures, the Company has not identified any information of core stakeholders (including customers, employees, suppliers, etc.) being used for secondary purposes. In 2024, the proportion of information of the Company's core stakeholders (including customers, employees, suppliers, etc.) used for secondary purposes was 0%.

（2） **Channels of information collection:** Including but not limited to official website and WeChat, online meetings, forums and seminars, questionnaires, providing from third parties, etc.

（3） **Use of the collected information:** Including but not limited to the establishment of stakeholder files, daily contact, etc.

（4） **Retention period of information:** The Company retains relevant data (including personal data and other information) in accordance with business needs and legal obligations, generally not exceeding the period necessary to achieve the business purpose, that is, the shortest period required for business needs. The Company's *Archive Management System* clearly stipulates the retention periods for various types of archival materials. Taking the minutes of important business meetings as an example, the usual retention period is ten years.

- **Third-party disclosure policy:** The Company undertakes that when sharing, transferring, or providing relevant data to third parties, it will strictly comply with relevant laws and regulations and privacy protection guidelines to ensure that data transfer activities are legally compliant and respect the rights of data subjects. The purpose and scope of data transfer shall not exceed the declared at the time of collection. Transmissions of high-impact data must use secure transmission channels or be encrypted before transmission. Data providers must obtain explicit commitments from recipients. In the event of cross-border data transmission, local laws and regulations must be complied with.

- **Privacy security protection measures:** The Company follows various privacy security management requirements and implements standardized operating procedures across its entire operational scope. Through various privacy data protection measures, the Company ensures the effective operation of the privacy security management system.

（1） **Data transmission technology:** Establish a Zero Trust global network and EMM mobile security space to ensure full concealment of data flow during

interactions between cloud and local servers, as well as in the transmission of user privacy data.

（2） **Entire data lifecycle management:** Strengthen the entire lifecycle management of data, including creation, collection, modification, usage, transfer, storage, and destruction.

（3） **Privacy security emergency drill:** Incorporate privacy data leakage emergency drill into the annual cybersecurity emergency drill plan to continuously enhance the Company's emergency responsiveness and agility in handling privacy data leakage incidents.

- **Penalties for violations of privacy security regulations:** The Company adopts a "zero-tolerance" attitude towards disciplinary violations, regulatory violations, and illegal acts related to privacy security. Employees who violate privacy security regulations will be taken in accordance with the severity of the incident's impact. For minor incidents, they will receive criticism and education. For moderate incidents, penalties such as performance deduction and restitution of unjust benefits may be imposed. For serious incidents, the labor contract may be terminated, and the employees may be required to compensate for losses and be held legally accountable. For those who violate the law, legal liability may be pursued through legal channels.
- **Business partner management:** The Company requires its business partners (including suppliers etc.) to comply with its privacy security protection policies. Additionally, the Company requires suppliers involved in privacy data processing to sign a dedicated data governance compliance agreement to ensure high standards of compliance with data processing activities.

六、 Information Security and Privacy Protection Reporting Procedures

The Company provides feedback channels (reporting email: jubao@jinkosolar.com) for information security and privacy protection issues to internal and external stakeholders, and encourages stakeholders to actively identify and report risks. To encourage internal

and external stakeholders to participate in information security and privacy protection reporting, those who report issues with real names and whose reported issues are verified to be true will be given appropriate rewards. The Company's Information Security and Confidentiality Management Department is responsible for supervising, guiding, and tracking the implementation of rewards. Where it is verified that a reporter has falsely accused others or fraudulently obtained reporting bonuses by means of deliberate defamation, fraud, tampering with or forging false evidence, etc., the Company will resolutely impose severe penalties. Those who violate the law will be directly transferred to judicial authorities for legal accountability.

The Company's *Information Security and Confidentiality Reporting and Suggestion Management Measure* details the procedures for reporting information security and privacy protection issues. Internal and external stakeholders shall submit reports through the channels designated by the Company. Reporting channels have been disclosed in the Policy and other public and transparent channels to ensure accessibility for stakeholders. Upon receiving a report, the Company's Information Security and Confidentiality Management Department will arrange for investigators to contact the reporter within 24 hours. If the reported issues are confirmed to involve disciplinary violations, regulatory violations, or illegal acts related to information security and privacy protection, the Information Security and Confidentiality Management Department will coordinate the launch of investigations. After completing the investigation, reward and punishment procedures will be initiated based on the investigation results.