晶科能源信息安全与隐私保护政策

Information Security and Privacy Protection Policy of Jinko Solar

一、 概述 Introduction

晶科能源股份有限公司（以下简称“晶科能源”或“本公司”）严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《信息安全等级保护管理办法》等法律、法规，以及相关规定要求，参考 ISO/IEC 27001 信息安全、网络安全和隐私保护-信息安全管理体系-要求（以下简称“信息安全管理体系”）建立信息安全管理体系，以健全信息风险管控，落实信息安全防护。同时，本公司重视隐私信息保护，参考 ISO/IEC 27701 安全技术-ISO/IEC 27001 和 ISO/IEC 27002 的隐私信息管理扩展-要求和指南（以下简称“隐私信息管理体系”）全面推进隐私数据全生命周期合规管理。晶科能源信息安全与隐私保护政策（以下简称“本政策”）旨在规范本公司数据处理活动，确保信息与隐私安全得到有效管治，维护本公司及各利益相关方的合法权益。

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、 适用范围 Scope of Application

本政策规定适用于本公司及旗下分子公司的所有业务与运营活动，并鼓励本公司所有董事、高级管理层及员工，以及价值链伙伴（包括服务提供商、供应商、合作伙伴等）遵循本政策，共同保护信息与隐私安全。本政策规定同时适用于本公司在全球范围内开展的兼并、并购等商业活动及尽职调查活动。本公司亦承诺对非控股合资企业施加影响，敦促其根据本政策相关规定行事。

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、 发布声明 Release Statement

本政策由风险合规与 ESG 管理委员会负责编制，相关政策与承诺的发布已得到本公司高级管理层及业务归口部门人员的认可。一般情况下本政策调整周期为一年一

次，以确保政策的时效性与适用性。本政策以中文和英文版本制备，若中英文版本不一致的，以中文版本为准。

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、 信息安全管理承诺与行动 Commitments and Actions for Information Security Management

晶科能源承诺不断推进信息安全管理体系完善、升级，将信息安全管理政策与相关工作的实施整合融入全公司范围的风险与合规管理环节，定期对信息安全管理政策的合规性开展内外部审计，确保信息安全政策能够有效实施。

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.

- **信息安全与保密组织体系：**本公司搭建了信息安全与保密委员会，统筹管理信息安全与保密工作。本公司董事会是信息安全与保密管理工作的最高统筹层，负责确定信息安全与保密管理战略与方针，审阅信息安全与保密政策，监督信息安全与保密议题实施进展，由董事陈康平[1]先生担任最高负责人；CXO 和各

[1] 陈康平先生，1973 年出生，硕士研究生学历。2003 年至 2006 年，担任浙江苏泊尔股份有限公司首席财务官。2007 年至 2022 年 12 月，担任晶科能源控股有限公司董事。2008 年 12 月至 2020 年 12 月，担任晶科能源控股有限公司首席执行官，负责公司整体战略规划和运营管理，包括但不限于战略规划、信息安全、财务稳定、合

体系负责人共同构成信息安全与保密委员会最高决策层，其中 CIO 为主要负责人，负责统筹管理和监督信息安全与保密战略实施过程；CEO 办公室和信息技术体系组成的信息安全与保密工作组为管理支撑层；各体系、各部门负责人和信息安全接口人组成执行落实层；全体员工组成监督参与层。各层级相互配合，切实保障信息安全与保密管理责任层层压实。

- **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, 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

规治理等。自 2014 年 9 月起，担任晶科电力科技股份有限公司董事。自 2020 年 12 月起，担任晶科能源股份有限公司董事兼总经理。（此段信息参考晶科能源股份有限公司 2024 年年报信息进行编制）

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.)

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.

- **完善信息安全管理体系建设：**本公司承诺动态优化信息安全相关制度框架与技术标准，构建覆盖数据采集、存储、传输全链条的防护体系。承诺引入前沿技术，持续提升信息安全风险预警与应急响应能力。承诺常态化开展全员安全培训，增强全体员工信息安全意识与操作规范。本公司致力于通过全方位的管控举措，不断优化升级信息安全管理体系建设。

- **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.

- **信息安全管理体系审核：**本公司每年开展覆盖全部业务范围的信息安全内部审核。本公司每年邀请第三方机构审核 IT 相关系统及基础设施的安全性，并每年邀请专业测评机构开展信息系统等级保护专项审核。本公司参考 ISO 27001 完善信息安全管理体系建设，并承诺到 2025 年底，实现核心系统 ISO 27001 第三方认证覆盖率达到 100%。

- **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.

- **信息安全风险管理：**本公司负责任地管理机密信息，承诺到 2025 年底，实现网络安全风险评估与核心数据泄漏风险评估覆盖率达 100%。同时，本公司不断建立健全漏洞分析机制，按照“识别与收集、优先级排序、修复与验证、闭环管理”等流程，系统化识别信息系统中可能存在的安全缺陷，形成“识别-评估-修复-验证”的持续改进体系，为组织构建主动防御的安全屏障。本公司要求所有系统上线前开展渗透测试及漏洞扫描，包括模拟黑客测试等，确保无中高危风险。每半年扫描服务器漏洞，并限期完成漏洞修复。针对发生重大变更的系统，根据重要程度平均每年开展 1-2 次渗透测试。

- **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.

- **防止数据被非法存取或披露：**本公司采取多种内部控制措施，限制内部数据被不当获取或访问，确保数据安全。

- **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）要求全体员工任何时候均须保护内部数据和专有及机密信息，以防止对内部数据及其他将其信息授权给本公司保管的个人或第三方带来伤害。

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）在全部运营范围内规范操作程序，根据信息等级设置不同的受限程度，实行数据分类分级管理。

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）设定内部数据访问权限，员工仅可在授权范围内进行各项访问、编辑、上传等操作，且系统实时记录操作痕迹，确保操作流可追溯。

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）依托远程办公零信任等安全技术，实现员工工作空间与私人空间分离，降低非可信终端远程接入本公司内部系统的风险。

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.

- **信息安全文化培育：**本公司视信息安全文化建设为企业稳健发展的重要基石，并通过建立覆盖全员的信息安全沟通、宣教、奖惩等机制，营造“人人重视、人人参与”的信息安全文化氛围。

- **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）全体员工主体责任：全体员工均为信息安全与保密管理的监督参与层。全体员工均应当严格遵守本公司信息安全与保密管理相关制度，主动履行信息安全与保密管理主体责任，积极上报日常工作中发现的安全漏洞与违纪、违规、违法行为。

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）员工信息安全培训：通过线上线下培训、讲座、案例分享等方式，提升全体员工信息安全与保密意识。信息安全培训为全体员工培训计划中的必修课，包括新入职员工。

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）员工信息安全意见收集：通过 IT 服务台定期收集全体员工的 IT 服务改善建议，结合反馈意见持续完善信息安全与隐私保护体系建设。

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.

- **业务连续性保障：**本公司积极制定信息安全相关业务连续性计划（BCP），通过构建“事前预防、事中响应、事后改进”的风险管理机制，将信息安全事件对业务的影响降至最低，保障组织运营的连续性、稳定性和合规性。

- **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）业务影响分析（BIA）：本公司积极梳理核心业务场景，明确其依赖的信息系统、数据和资源，并评估各系统潜在安全风险，分析系统中断对财务、合规、声誉的具体影响，按影响程度划分系统管理优先级，据此确定业务恢复的时间目标。

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）事先预防：本公司持续推进技术项目与业务管理整改，及时更新和升级安全防护设备、数据加密系统、访问控制软件等配套，提高信息系统的安全性和保密性，从源头保障业务连续性。此外，本公司每年开展 1 次针对重要系统的网络安全应急演练，以遭受网络安全攻击导致系统异常为核心场景，模拟网络安全紧急事件处理全流程，提升信息安全专兼职岗位员工应急处置综合能力。

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）事中响应：为确保业务连续性，本公司建立了完善的信息安全应急处理机制，成立信息安全应急领导小组，按照“预防为主、全员参与、分级负责”的原则，开展突发事件应急管理和应急处置。当发生重大突发信息安全事件时，本公司将第一时间排查、识别原因，及时启动并执行应急预案，确保业务正常运转。

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）事后改进：本公司全程记录信息安全事件处置过程，并做好总结。针对业务发生变化的情况，本公司及时更新业务影响分析（BIA），并根据分析结果调整信息安全相关业务连续性计划（BCP），确保相关业务连续性计划符合主流标准要求及业务发展需要。

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.

- **合作伙伴管理：**本公司要求合作伙伴（包括供应商等）积极配合信息安全与隐私保护相关制度与要求。在与重点供应商确立合作之前，本公司积极开展信息安全相关尽职调查，确保不存在重大风险。本公司将信息安全与隐私保护要求纳入《晶科能源供应链合作伙伴行为准则》，要求全体供应商签署并遵守。同时，要求合作伙伴签署保密协议，明确双方保密责任和义务。此外，定期评估和监督合作伙伴信息安全措施的有效性，以降低合作过程中的信息安全风险。

- **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、 隐私保护承诺与行动 Commitments and Actions for Privacy Protection

保护利益相关方隐私信息的安全性与秘密性，对于晶科能源至关重要。因此，本公司在开展业务时将严格遵守与隐私保护相关的法律法规。希望下述政策有助于您理解本公司可能收集哪些信息、怎样使用和保护这些信息，以及将与谁共享这些信息。

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.

- **隐私安全治理：**本公司在 CEO 办公室下设信息安全与保密管理部，作为隐私数据全生命周期合规管理的归口部门，并配套制定《保密管理制度》《数据安全管理制度》等制度，加强数据全生命周期安全管理，确保数据的保密性与完整性，切实保护内外部利益相关方隐私安全。

- **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.

- **隐私安全风险管理：**本公司将核心利益相关方信息安全与隐私保护相关风险纳入全面风险管理规划，按照“风险识别、风险评估、风险控制与应对”的逻辑开展信息安全与隐私保护相关风险管理。

- **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）风险识别：由信息安全与保密管理部牵头开展全面信息安全与隐私保护相关风险识别。在数据收集环节，审视收集渠道是否合法合规，收集范围是否遵循最小必要原则。在数据存储环节，评估存储系统的安全性，包括设备故障风险、网络攻击风险、权限管理漏洞等。在数据传输环节，关注加密技术应用是否到位，防范数据在传输途中被窃取或篡改。

  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）风险评估：依据风险发生的可能性和影响程度进行风险量化评估。高可能性且高影响的风险，列为高风险等级，需优先处理；低可能性且低影响的风险，列为低风险等级，但仍需持续监控。

  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）风险控制与应对：按照风险等级制定相应的应对策略，包括细化数据全生命周期各阶段操作规范、严格执行数据分类分级存储策略、建立数据访问审批流程、定期开展隐私安全与合规培训、隐私安全风险监督检查等。针对重大风险，本公司还制定了专项应对策略，包括紧急应对、恢复应对、补救应对、预防应对等。

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.

- **隐私安全管理体系审核：**本公司将隐私安全管理纳入内外部信息安全审计重要关注项，每年随内外部信息安全审计开展专项审查，审计内容主要涵盖隐私政策的合规性、遵守执行情况等。本公司积极开展隐私信息管理体系认证，承诺到 2026 年底，核心系统 ISO 27701 隐私信息管理体系第三方认证覆盖率达到 100%。

- **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.

- **隐私安全管理原则：**本公司将核心利益相关方（包括客户、员工、供应商等）隐私信息视为核心机密，严格遵守“公开性、合法性、正当性”原则，密切关注各利益相关方信息安全及隐私保护，全面防控隐私泄露风险。本公司承诺，客户可以决定如何收集、使用、保留和处理其个人隐私数据。

- **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）信息收集前：通过在合作协议中获得授权、单独签署隐私协议或其他书面说明等方式，确保获得利益相关方 100%授权或同意，并为不同意信息收集的利益相关方提供退出选项。

  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）信息收集中：遵循最小必要性原则，不额外接收或收集无关信息。本公司亦充分尊重利益相关方的信息控制权，确保利益相关方可以访问已共享的数据、将已共享数据转移给其他处理者，以及有权结合实际情况对信息进行更正或删除。

  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）已获取信息：采取加密存储、严控提取流程、行为审计等方式确保信息合规管理。同时，承诺不将核心利益相关方（包括客户、员工、供应商等）的信息用于非主要用途，及时删除不必要的信息。[2]

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.

- **隐私信息管理概况：**本公司尊重利益相关方的知情权，充分告知其以下隐私保护相关问题。
- **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）所获取信息的性质：包括但不限于利益相关方的名称、属性、联系方式、基本介绍、特别注意事项等。

[2] 近年来通过系统化监测，本公司未识别到有任何核心利益相关方（包括客户、员工、供应商等）的信息被用于非主要用途。2024 年，本公司核心利益相关方（包括客户、员工、供应商等）的信息被用于非主要用途的比例为 0%。

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%.

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

（2）信息收集的渠道：包括但不限于官网官微、线上会议、论坛及研讨会、问卷调查、第三方提供等。

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）信息收集的用途：包括但不限于建立利益相关方档案、日常联系等。

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

（4）信息保存的期限：依据业务需求和法律义务保存相关数据（包含个人数据等），通常不超过实现目的所需的期限，即满足业务所需的最短期限。本公司的《档案管理制度》明确规定了各类型档案材料的保存期限。以业务活动重要会议纪要为例，通常其保存周期为十年。

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.

- **第三方披露政策：**本公司承诺，在将相关数据分享、转移或提供给第三方时，严格遵守相关法律法规和隐私保护准则，以确保数据转移活动符合法律规定并尊重数据主体的权利。数据转移的目的和范围不能超出收集时所声明的目的和

范围。高影响数据的传输须采用安全传输通道或加密后传输。数据输出者必须获得接收者的明确承诺。如涉及数据的跨境传输，需遵从当地法律法规的要求。

- **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.

- **隐私安全保护举措：**本公司参照各项隐私安全管理要求，在全部运营范围内落实标准化操作程序，通过各类隐私数据保护举措，确保隐私安全管理体系的有效运转。

- **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）数据传输技术：搭建零信任全球组网以及 EMM 移动安全空间，在云端与本地服务器交互、传输用户隐私数据等过程中实现数据流转全程隐匿。

  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）数据全生命周期管理：加强数据创建、收集、变更、使用、传递、存储与销毁等环节的全生命周期管理。

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

（3）隐私安全应急演练：将隐私数据泄漏纳入年度网络安全应急演练预案，以持续加强本公司对隐私数据泄露事件的应急响应能力以及敏捷性。

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.

- **违反隐私安全规定的处分：**本公司对隐私安全违纪、违规、违法行为持“零容忍”态度，对于违反隐私安全的员工，将视情节影响严重性程度予以处置。对于轻微事件，进行批评教育；对于中等事件，可能处以扣除绩效、返还不当得利等惩罚；对于严重事件，可能解除其劳动合同，要求员工赔偿损失，并追究法律责任；对于触犯法律的，可能会通过法律途径追究其责任。

- **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.

- **合作伙伴管理：**本公司要求合作伙伴（包括供应商等）配合本公司的隐私安全保护制度。本公司亦要求涉及隐私数据处理的供应商签署专项数据治理合规协议，确保对数据处理活动保持高标准的合规性。

- **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、 信息安全与隐私保护上报程序 Information Security and Privacy Protection Reporting Procedures

本公司为内外部利益相关方提供信息安全与隐私保护问题反馈渠道（举报邮箱：jubao@jinkosolar.com），鼓励内外部利益相关方积极识别、报告风险。为鼓励内外部利益相关方参与信息安全与隐私保护上报工作，实名上报且调查事件属实的上报人员，将给予适当的奖励，并由本公司信息安全与保密管理部负责监督、指导和跟踪落实奖励。对于经查实上报人通过蓄意造谣、欺诈或篡改制作假证据等行为诬告他人、骗取举报奖金的，本公司坚决从严惩处，对于触犯法律的将直接移送司法机关追究其责任。

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.

本公司《信息安全与保密举报及建议管理办法》对信息安全与隐私保护事项上报流程进行了详细规定。内外部利益相关方应当通过本公司指定的渠道提交上报信息。上报渠道已披露在本政策及其他公开、透明的渠道，以确保利益相关方可获得。本公司信息安全与保密管理部在收到举报后，24 小时内安排调查人员与上报人取得联系，确认属于信息安全与隐私保护相关的违纪、违规、违法事项的，由信息安全与保密管理部协调展开调查。完成调查后，根据调查结果启动奖惩程序。

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.