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

晶科能源信息安全与隐私保护政策

版本号：2026V1.1

一、 概述

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 要求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。

二、 适用范围

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。

三、 发布声明

本政策与承诺由风险合规与 ESG 管理委员会做版本管理，信息安全与保密管理部、基础架构&信息安全部等相关部门跟进年度管理进展、执行制度审查及更新，董事会和高级管理层审阅确认。一般情况下本政策审查周期为一年一次，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。本政策公开发布于晶科能源 ESG 专栏，并通过邮件、会议、线上提示等方式告知关键利益相关方。

四、 承诺与目标

本公司基于 ISO 27001 信息安全管理体系、ISO 27701 隐私信息管理体系要求，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，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“合法性、正当性、必要性”原则，密切关注各利益相关方信息安全及隐私保护。本公司承诺，公司会通过相关合同或协议获得授权、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，尊重相关方对信息的知情权、决定权、删除权等权益。

本公司承诺到2030年底，保持网络安全风险评估与核心数据泄漏风险评估覆盖率达100%，核心系统经ISO 27001/ISO 27701 第三方认证覆盖率达到 100%。

五、 行动与实践

（一）管理架构与专职机构

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；建立信息安全与保密委员会作为信息安全与隐私保护议题的最高决策层，由公司高级管理层（CIO/CEO 等）及数据保护官（DPO）组成；管理支撑层为信息安全及隐私保护工作组，由信息安全与保密管理部和信息安全部组成；各体系、各部门负责人和信息安全及隐私保护接口人组成执行落实层；全体员工组成监督参与层。此外，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。

（二）合规管理及体系建设

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，遵循 ISO 27001 信息安全管理体系、ISO 27701 隐私信息管理体系规定，定期开展覆盖全部业务范围的信息安全内部审核，构建覆盖数据采集、存储、传输全链条的防护体系，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。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，并推进整改缺失项与待改进项。

（三）相关方信息安全及隐私保护

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。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。信息收集中，承诺遵循最小必要性原则不额外接收或收集无关信息，以易于理解的方式（如使用表格）明确列出所收集的个人信息类型，明确每一项信息来源、收集目的、收集方法和预期用途，通过文字提示、弹窗或链接等方式提示信息收集用途等事项，确保在数据主体知情和明示同意的前提下完成操作。公司若与第三方（如合作伙伴、服务供应商等）共享数据时，除征得数据主体明示同意外，还将告知其接收方的类型及共享的目的等，并签署保密协议，定期进行安全评审。《晶科能源供应链合作伙伴行为准则》中亦对公司及供应链双方的保密责任和义务做出规定，并定期开展相关方尽职调查，保障合作伙伴信息安全措施的有效性。

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。对于已获取信息，会采取加密存储、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。[1]

本公司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《数据（包含个人信息）存储期限要求》明确规定了各类型档案材料的保存期，如日常运营数据（会议记录等）通常为 3 年、市场调研报告通常为 5 年。

（四）信息与隐私风险管理

本公司负责任地管理机密信息。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。

本公司由信息安全与保密管理部牵头开展信息安全与隐私保护工作，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。其次，依据风险发生的可能性和影响程度进行风险量化评估。基于评估结果，按照风险等级制定相应的应对策略。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。

（五）内部控制与防泄露管理

本公司在全部运营范围内规范操作程序，根据信息等级对数据分类分级，设置不同的受限程度,完善数据创建、收集、变更、使用、传递、存储与销毁等环节的全生命周期管理。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；此外，搭建零信任全球组网以及 EMM 移动安全空间，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。此外，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。

（六）业务连续性保障

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，提升事件响应（IRP）能力。

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，本公司信息安全与保密委员会牵头评

[1] 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。2025 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%。

估年度潜在安全事件，并组织每年 1 次的重要系统网络安全应急演练，以遭受网络安全攻击导致系统异常、隐私信息泄露为核心场景，模拟网络安全紧急事件处理全流程，提升员工应急处置综合能力。

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，本公司将第一时间收集流量、日志、可疑进程等信息，排查、识别原因，评估风险等级，并及时启动并执行对应应急预案，确保业务正常运转。

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），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，并重点开展事件报告的培训与宣传，提升团队安全意识与水平。

（七）信息与隐私安全教育培训

本公司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，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。自入职起全体员工均要求签署《关于使用办公软件的承诺函》《人脸信息授权及免责声明&个人信息隐私政策告知书》，要求全体员工严格遵守《信息安全与隐私保护管理制度》等内部要求，并鼓励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。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。

（八）违反信息安全与隐私管理的处分

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，涉嫌违法犯罪情节的移送至司法机关处理。

六、 信息安全与隐私保护上报程序

本公司充分尊重员工和客户个人权益，数据主体可在合法合规前提下决定如何收集、使用、保留和处理其私人数据。公司提供个人加入或退出的选项，提供清晰便利的渠道响应员工或客户访问公司持有的数据请求，以进行更正或删除等。任何组织、个人有权对任何违法处理数据隐私或违反科技伦理的活动向相关职责部门进行投诉、举报。公司保密工作方针：“相互监督、重点预防、奖惩结合”，每一位晶科员工对信息安全与保密工作都有监督义务，对于发现的违规行为或泄密事件可通过公司信息安全邮箱 JKIS@jinkosolar.com 或直接向部门信息安全接口人、信息安全与保密部进行举报，对于举报人信息不记名、不公开。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，并将处理结果及时告知数据主体。同时，公司鼓励员工积极发现并通过《信息安全合理化建议流程》报告潜在的信息安全问题，提出改进信息安全的创新建议，鼓励各部

门积极参与信息安全合理化建议的实施。对于调查确定举报内容属实的举报人或积极制止泄密事件的人员，以及对于提出信息安全合理化建议的员工或参与合理化建议实施的部门，有重大贡献者公司将酌情给予奖励。

附件：文件修订记录表

文件名称	《晶科能源信息安全与隐私保护政策》		
版本号	修订说明	生效时间	发行单位
2025V1.0	因信息安全与隐私保护法律法规及国际标准要求，发布本政策，旨在规范数据处理活动，健全风险管控，推进隐私数据全生命周期合规管理。	2025.7	风险合规与 ESG 管理委员会
2026V1.1	完善政策审批流程，新增信息安全与隐私保护目标设定，优化行动与实践小节内容，优化上报程序的核心原则。	2026.8	风险合规与 ESG 管理委员会

注：年内因同类事项导致的细微调整将于文件修订记录表中做版本合并管理。如对政策版本或内容有疑问，可邮件 ESG@jinkosolar.com 问询，感谢您对晶科能源 ESG 管理的关注。