

## 晶科能源信息安全与隐私保护政策

版本	生效日期	发布或修订说明	编制或修订/日期	审核/日期	审批/日期
01	2025. 7. 1	新版发布	刘晨辰 2025. 6. 2	陈思颖 2025. 6. 16	姚臣湛 2025. 7. 1

**适用范围：**晶科能源各体系、各事业部、各子公司

## 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 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。

## 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。

#### 四、 信息安全管理承诺与行动

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。

- **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；CXO 和各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。
- **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。
- **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。
- **信息安全风险管理：**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。

- **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。
  - (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。
  - (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。
  - (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。
  - (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。
  
- **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。
  - (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。
  - (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。

- (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。
- **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。
    - (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。
    - (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。
    - (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。
    - (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。

- **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。

## 五、 隐私保护承诺与行动

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。

- **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。
- **隐私安全风险治理：**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。

(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。

- (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。
- (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。
- **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。
  - **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。
- (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。
- (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。
- (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。

- **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。
  - (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) **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。
  - (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。
  - (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。
  
- **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。
  
- **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。
  - (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。
  - (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。

**(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。

- **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。
- **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。

## 六、 信息安全与隐私保护上报程序

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。

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。