



天合光能股份有限公司

负责任 AI 管理政策

主导部门	流程数字化部		
支持部门	风险控制管理部		
制度审批	ESG 管理委员会		
文档编号	TSL-ESG-001	生效日期	2026-09-01

1. 目的

天合光能股份有限公司及其分公司、全资或控股子公司（以下简称“天合光能”或“公司”）坚持以科技创新驱动可持续发展，积极探索人工智能（Artificial Intelligence, AI）在研发创新、智能制造、运营管理、供应链协同、客户服务、风险管理等领域的应用。公司充分认识到 AI 技术在创造价值的同时，也可能带来数据安全、隐私保护、算法偏见、透明度不足、责任归属以及环境影响等风险。为规范 AI 系统的开发、采购、部署、使用与管理活动，确保 AI 技术在公司业务运营中的安全、合规、公平、透明和可持续应用，防范 AI 相关风险，公司秉持合法合规、安全可控、公平透明、人类监督、问责有据、可持续发展的原则，依据公司运营地所适用的法律法规，并参照 AI 相关国家及国际标准，特制定本政策。

2. 范围

本政策适用于天合光能股份有限公司及分公司、全资或控股公司在全球范围内开展的 AI 相关活动，涵盖公司全体员工、管理人员，以及公司自主开发、参与开发、采购、部署或使用的 AI 系统、产品、模型和服务，包括但不限于：（1）公司内部开发或部署的本地大模型；（2）公司采购、部署或使用的外部第三方大模型及 AI 服务；（3）公司自研或参与开发的 AI 系统。

公司应通过合同、协议、采购条款或其他适当方式，要求以公司名义参与 AI 系统开发、部署、运营或提供服务的供应商、承包商、咨询机构及合作伙伴遵守本政策适用要求，并鼓励供应链伙伴共同提升负责任 AI 管理水平。

3. 定义

名称	定义
人工智能系统（AI 系统）	是指针对人类定义的给定目标，产生诸如内容、预测、推荐或决策等输出的一类工程系统。
大模型（Large-scale Model）	基于大量数据训练得到，具有复杂计算架构，能处理复杂任务，且具备一定泛化性的深度学习模型。
公平性	是指 AI 系统尊重既定事实、社会规范和信仰，且不受偏袒或不公正歧视影响的对待、行为或结果。
透明性	是指 AI 系统与利益相关方交流关于该系统适当信息的特性。
可解释性	是指 AI 系统以人能理解的方式，表达影响其（执行）结果的重要因素的能力。
人工指挥（Human-in-Command）	是指人类拥有对 AI 系统的最终控制权和否决权。
人工监控（Human-on-the-Loop）	是指人类实时或近实时地监测 AI 系统运行。
人工审批（Human-in-the-Loop）	是指 AI 输出须经人类审查批准后方可执行。

适用法律	是指与 AI 管理相关的公司应适用的任何法律、法规、政策、规则、命令、决定、司法解释、条约、判决、裁定、国际/地方/行业/团体标准或其他法定要求。
------	---

4. 管理内容

4.1 基本原则

4.1.1 合法合规原则。严格遵从适用法律要求，确保 AI 系统在全生命周期内的合法性。

4.1.2 安全可控原则。建立覆盖 AI 全生命周期的安全管理体系，确保 AI 系统自身安全及对外部环境的安全性，防范网络攻击、数据泄露、模型滥用等风险。

4.1.3 公平透明原则。确保 AI 系统的决策过程公平公正，杜绝基于种族、性别、年龄、宗教信仰、残疾状况等受保护特征的歧视行为；确保 AI 使用、AI 生成内容的显式披露，保障利益相关方对 AI 决策的知情权。

4.1.4 人类监督原则。重大决策须保持有意义的人类参与和监督。不可逆高级别决策不得完全交由 AI 系统自动执行。

4.1.5 问责有据原则。对 AI 管理履行问责制，对 AI 管理业务范围内各级组织承担职责和义务的履行情况实施责任追究。

4.1.6 可持续发展原则。关注 AI 系统对环境的影响，采取措施降低 AI 计算资源的能源消耗和碳排放，促进绿色低碳发展。

4.2 AI 系统应用规范

4.2.1 公司开发、部署 AI 系统时，需在技术文档中明确其授权使用场景、能力边界和限制条件。使用该 AI 系统时不得超过授权范围。

4.2.2 涉及以下场景时，须由 AI 需求部门依据公司《数据安全风险评估制度》的规定，向公司数据合规与安全评估小组提交风险评估，说明使用场景、目的、涉及的数据类型和预期影响：

- （1）涉及开发新 AI 系统，或引入/部署新的外部第三方开发的新 AI 系统；
- （2）该 AI 系统涉及处理公司 C 级及以上数据；
- （3）该 AI 系统发生重大系统变更或更新时。

4.2.3 当发现 AI 系统发生意外应用或偏离预期时，应立即报告 AI 系统开发团队负责人/AI 系统部署团队负责人。

4.2.4 禁止使用的 AI 行为

- （1）**禁止非法活动。**不得使用、部署或应用 AI 系统从事任何违反适用法律的活动，包括但不限于煽动颠

覆国家政权、危害国家安全和利益、损害国家形象，煽动分裂国家、破坏国家统一和社会稳定，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，暴力、淫秽色情等。

- (2) **禁止侵权活动。**不得使用、部署或应用 AI 系统从事任何侵犯或不当使用第三方知识产权（包括著作权、商标权、专利权、商业秘密等）的行为，以及侵犯他人肖像权、名誉权、荣誉权、隐私权和个人信息权益等合法权益及危害他人身心健康的活动。
- (3) **禁止高风险活动。**不得使用或部署涉及高风险活动的 AI 系统，包括：
 - (a) 实施利用潜意识、故意操纵或欺骗技术，导致或可能导致重大伤害及扭曲行为的系统；
 - (b) 以有害方式操纵他人行为或利用他人弱点，包括利用年龄、残障状况或特定社会经济背景等方面的弱势；
 - (c) 以可能导致歧视或伤害的方式，对他人进行评估或分类，包括基于其社会行为或个人特征的评判；
 - (d) 通过无差别抓取人脸图像，创建面部（情绪）识别数据库；
 - (e) 在工作场所对他人进行情绪识别（基于医疗或安全目的除外）；
 - (f) 实施基于生物识别数据推断特定敏感特征（包括种族、宗教、年龄、性取向、政治观点等）的生物识别分类系统；
 - (g) 在公共场所实施实时远程生物特征识别（RBI）系统。
- (4) **禁止恶意软件。**不得使用 AI 系统生成或传播恶意软件，或任何旨在协助未经授权访问或使用计算机系统或数据的内容。
- (5) **禁止混淆。**不得在部署了 AI 系统的任何应用程序中不当混淆或未向最终用户披露 AI 的存在，以及在缺乏适当保障措施、监督和人工控制的情况下使用 AI 所带来的任何已知风险或危险。
- (6) **禁止依赖。**在未评估其准确性、潜在危害或适用于该使用场景的其他具体风险之前，不得依赖使用 AI 系统生成的任何信息。

4.3 数据合规与个人信息保护

4.3.1 在设计、开发、部署、使用 AI 系统时，应基于合法、正当、必要及安全原则收集、处理数据，确保数据收集合法合规：

- (1) 使用自动化工具收集数据的，评估对他人网络服务带来的影响，不得非法侵入他人网络，不得干扰他人网络服务正常运行；
- (2) 收集、使用开源数据集时，应遵循数据集的开源许可协议或取得使用授权许可；
- (3) 涉及收集、使用个人数据的，应按照本政策第 4.3.3 条的规定执行；

(4) 通过采购或合作等方式从其他外部第三方收集数据时，应对交易方或合作方所提供的数据、承诺及相关合规证明材料进行审核。

4.3.2 在设计、开发、部署、使用 AI 系统时，应加强知识产权保护，在训练数据选择、结果输出等环节防止侵犯知识产权。

4.3.3 在设计、开发、部署、使用 AI 系统的全生命周期过程中涉及处理个人信息的，应当遵循适用法律及公司《个人信息保护管理制度》等相关制度要求，符合以下要求：

- (1) 处理个人数据须取得数据主体同意或具备其他合法性依据；
- (2) 仅收集实现功能所必需的最少数据，避免过度收集、使用、存储个人信息；
- (3) 处理敏感个人信息的，应取得对应个人的单独同意或具备其他合法性依据。

4.3.4 涉及数据跨境的，应遵从适用法律关于数据跨境的规定以及公司《数据跨境合规管理制度》等制度要求。

4.4 网络安全

4.4.1 开发、部署 AI 系统时，应遵循公司《开发安全管理规范》的规定，依据《安全编码规范》进行程序开发工作，编写符合安全要求的代码；AI 系统上线前需进行渗透测试，仅在渗透测试结果符合安全要求后才允许上线。

4.4.2 AI 系统中涉及 B 级及以上数据的存储和传输时应采用加密保护，使用加密算法应符合国家、国际及行业标准。

4.4.3 对于每一种类型的训练数据，如文本、图片、音频、视频等，应在将数据用于训练前，对全部训练数据进行过滤，过滤方法包括但不限于关键词、分类模型、人工抽检等，去除数据中的违法不良信息。

4.4.4 应对 AI 系统输入内容持续检测，采取提示词屏蔽等保护措施，防范恶意输入攻击（如注入攻击、数据窃取、对抗攻击等）。

4.4.5 公司应建立 AI 系统运行监测能力和安全事件应急预案，定期开展应急演练，并根据行业安全事件、重要舆情及监管变化，及时优化应急策略，应对不断变化的安全风险。

4.5 公平性

4.5.1 在使用训练数据时，应对所用数据集的规模、均衡性进行探索性分析和预处理，确保训练数据的多样性和代表性，并根据分析结果采取必要的数据清洗、筛选、补充或均衡处理措施，识别并降低因训练数据分布不合理导致的潜在偏见风险。

4.5.2 在算法设计、模型训练和优化、提供服务等过程中，应结合具体应用场景识别可能涉及的公平性风

险，并采取训练数据筛选、输出校验等方式，降低产生民族、信仰、国别、地域、性别、年龄、职业、健康等方面歧视的风险。

4.5.3 应定期（至少每年一次）对 AI 系统开展偏见审计，识别公平性相关的风险，并采取相应的改善措施。

4.6 人类参与干预

4.6.1 公司实行三级人类监督体系：

监督层级	适用场景	监督内容
第一级：人工指挥	所有 AI 系统	可随时中止、否决或覆盖 AI 输出
第二级：人工监控	涉及自动化决策的 AI 系统	实时干预、暂停 AI 系统运行
第三级：人工审批	涉及不可逆或高风险决策的 AI 系统	审查、批准或回退 AI 系统的辅助建议

4.6.2 当涉及不可逆或高风险的决策时，AI 系统仅可提供辅助建议，最终需由人类管理者进行决策。包括但不限于：

- （1）可能会对个人的就业、信用、健康、安全、自由或其他基本权利产生不可逆或高风险影响时，包括但不限于人员聘用、解雇、晋升、降职等；
- （2）涉及业务重大决策，包括但不限于重大财务决策、关键生产安全决策、法律合规判断等；
- （3）其他可能会对公司业务或个人造成不可逆或高风险影响的活动。

4.6.3 任何人员发现 AI 系统输出存在明显错误或可能造成损害时，应立即暂停该 AI 系统的相关操作，并向 AI 系统开发团队负责人/AI 系统部署团队负责人报告。

4.6.4 受影响的个人对 AI 辅助决策有异议的，公司应及时组织相关业务部门进行人工复核，人工复核须在合理期限内完成，并书面告知该个人复核结果。

4.7 透明度与可解释性

4.7.1 应以显著方式告知用户其交互对象、获得的服务来源等为 AI 系统而非自然人，并应告知用户其输出结果所可能涉及的风险以及局限性。

4.7.2 对外发布的 AI 生成内容（文本、图像、音频、视频等），应按照适用法律要求添加标识（如需）。

4.7.3 应针对不同利益相关方提供便于理解的不同程度的解释，如为用户提供系统意图、决策结果等说明，向产品提供方提供算法模型、运行环境等说明。

4.8 生态可持续性

4.8.1 公司承诺采取有效措施，并结合自身新能源优势，降低 AI 数据中心和大模型的全生命周期生态足迹（包括能源消耗、水资源使用、碳排放），将 AI 可持续发展纳入公司 ESG 战略框架。

4.8.2 公司应将生态可持续性纳入外部第三方 AI 系统/大模型供应商的评估标准，优先与具有较低的生态足迹的供应商合作。

4.9 责任承担机制

4.9.1 AI 系统不得被赋予独立法律主体地位，AI 决策的法律责任应由对应的人类责任主体承担：

- （1）AI 系统开发方：公司内部开发的 AI 系统，由开发团队负责人对 AI 系统的技术设计、训练数据合规性、基本安全性能承担责任；
- （2）AI 系统部署方：部署外部第三方开发的 AI 系统，由部署团队负责人对 AI 系统适配、使用场景合规、最终部署决策承担责任；
- （3）AI 系统使用方：AI 系统的实际使用人对其具体操作、使用行为和使用结果承担直接责任。

4.9.2 任何违反适用法律及本政策，造成公司受到任何行政处罚、争议、经济损失、品牌声誉影响或其他负面影响（合称“负面影响”）的，应参照《天合光能员工手册》、《业务违规及问责管理制度》规定进行调查，并依据违规行为等级及情节轻重，按照处罚等级、处罚程序等具体要求进行处罚；构成犯罪的，公司有权移交主管部门追究其法律责任。

4.10 培训与能力建设

4.10.1 公司应持续提升员工负责任使用 AI 的意识和能力，根据岗位职责和风险水平开展人工智能伦理与合规、数据安全与隐私保护、网络安全与模型安全等培训，推广负责任 AI 实践案例，并加强管理层及关键岗位人员的 AI 治理能力建设。

4.10.2 对参与 AI 系统开发、采购、部署、运营和使用的相关人员，公司可结合业务需要开展专项培训或能力评估，确保其理解 AI 系统的授权范围、能力边界、风险要求及人工监督责任。

4.11 监督、申诉与持续改进

4.11.1 公司应建立 AI 风险监测和持续改进机制，定期开展 AI 管理体系的内部审查、合规检查和风险评估，对发现的问题制定整改措施并跟踪落实；根据适用法律、监管要求、技术发展、行业实践和利益相关方反馈，持续优化 AI 管理要求。

4.11.2 公司应提供 AI 风险事件报告和异议申诉渠道，接受员工、客户、供应商及其他利益相关方的反馈

与监督。对于 AI 辅助决策结果的异议，应按照本政策人类参与干预相关要求组织人工复核和处置。

5. 附则

5.1 参考文件

序号	文件名称	文件编码
1	《生成式人工智能服务管理暂行办法》	
2	EU AI Act（Regulation 2024/1689）	
3	人工智能 可信赖 通则（GBT 47507-2026）	

5.2 修订记录

编码	版本	拟制/修订责任人	生效日期	修订内容及理由
TSL-ESG-001	V01	流程数字化部	2026-09-01	新版本发布

5.3 特别说明

本政策由董事会作为最高决策和监督机构，相关政策与承诺的发布已得到公司董事会和高级管理层的认可。流程数字化部作为负责任 AI 管理工作的主导部门，负责本政策的版本管理、解释、年度审阅与更新；风险控制管理部作为负责任 AI 管理工作的支持部门，负责组织公司相关部门开展 AI 风险识别、评估、监督和持续改进；公司各业务及职能部门按照职责，对其开发、采购、部署和使用的 AI 系统承担相应管理责任。

本政策有效期两年，原则上每年至少开展一次审阅；如适用法律、监管要求、技术发展或公司业务发生重大变化，应及时修订。新制度发布后，旧制度自动废止。公司其他制度文件中关于 AI 管理的规定与本政策规定相冲突的，以本政策的规定为准。