TCL 中环新能源科技股份有限公司

负责任人工智能管理政策

1. 引言

作为全球领先的新能源光伏企业，TCL 中环新能源科技股份有限公司及其下属公司（以下简称“TCL 中环”“我们”“公司”）坚持以科技创新驱动可持续发展，持续推进智能制造与数字化转型，积极探索人工智能技术在晶体生长工艺控制、智能品质检测、生产计划排产、数字孪生工厂、供应链协同、运营管理及客户服务等领域的应用。

我们充分认识到，人工智能技术在提升生产效率、产品质量和资源利用效率的同时，也可能带来数据安全、隐私保护、算法偏见、透明度不足、责任归属不清以及环境影响等风险。为此，公司秉持“安全可信、以人为本、公平透明、权责清晰、绿色发展”的原则，制定《负责任人工智能管理政策》（以下简称“本政策”），明确公司在人工智能治理方面的管理架构、原则要求与行动措施，确保人工智能技术的开发、采购、部署和使用符合适用的法律法规、国际准则及公司可持续发展目标，推动人工智能安全、可靠、合规和可持续地应用。

2. 范围

本政策适用于TCL 中环本部及全部下属全资、控股子公司；公司全体董事、高级管理人员及在岗员工须严格遵照执行。本政策覆盖公司自主开发、联合开发、外部采购、部署或使用的全部人工智能系统、模型、算法、工具及服务（以下统称“人工智能系统”），贯穿其规划设计、数据准备、开发训练、测试验证、部署上线、运行监控直至退役下线的全生命周期。

同时，本政策适用于参与公司人工智能系统开发、部署或运营的供应商、承包商、技术服务商及合作伙伴。我们鼓励外部战略合作方、上游供应商、下游渠道伙伴共同遵守本政策，携手构建负责任的人工智能生态。

3. 承诺

TCL 中环高度重视人工智能应用可能对员工、客户、合作伙伴、供应商、社区及社会公众（以下统称“利益相关方”）产生的影响。我们承诺以负责任的方式开发和使用人工智能，确保人工智能始终服务于人、辅助于人，坚决反对任何侵犯个人隐私、危害网络安全、造成不公平歧视或损害利益相关方合法权益的人工智能开发与应用行为。

我们致力于遵守所有适用的法律法规及监管要求，包括但不限于《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》《生成式人工智能服务管理暂行办法》《人工智能生成合成内容标识办法》等；积极参考《新一代人工智能伦理规范》、经济合作与发展组织（OECD）人工智能原则、联合国教科文组织《人工智能伦理问题建议书》等准则；并持续关注包括《欧盟人工智能法案》（EU AI Act）在内的境内外监管动态，及时更新公司管理要求。

公司将人工智能治理纳入整体风险和合规管理之中，依托已通过 ISO 27001 体系认证的信息安全管理体系及公司《隐私保护政策》，将数据安全、隐私保护与网络安全要求延伸至人工智能全生命周期。公司积极参照 ISO/IEC 42001 人工智能管理体系标准完善治理框架，并探索开展外部独立验证，以确保治理体系的专业性与国际合规性。

公司承诺以2026年为基准年，到2030年实现每年重大人工智能安全与伦理事件发生率为0起、新上线人工智能应用风险评估覆盖率100%、人工智能相关岗位员工负责任人工智能培训覆盖率100%，作为核心管控目标，持续强化人工智能风险防控能力。

4. 策略

4.1 管理架构

本公司负责任人工智能管理工作由董事会作为最高决策和监督机构，负责审议公司人工智能治理相关重大事项，并监督本政策的执行情况。

公司数字化转型委员会（以下简称“数委会”）由总经理担任委员会主要责任人（最高决策层负责人），作为公司人工智能战略与负责任人工智能管理的最高管理层负责人，负责审批本政策、制定人工智能发展战略与治理原则、审批高风险人工智能应用，并定期听取人工智能风险管理情况汇报。

数委会下设负责任人工智能工作组，由信息安全技术组牵头，联合数字化/信息技术、法务合规、审计、人力资源、可持续发展（ESG）及相关业务部门组成，负责落实本政策及相关制度，组织开展人工智能应用的登记备案、风险评估、合规审查、监测审计与培训宣贯等工作。

各业务部门及子公司是本单位人工智能应用的第一责任主体，须为每一个人工智能系统明确模型所有者和业务责任人，负责系统的日常运行管理、性能监测、风险识别与问题整改。公司审计部负责对本政策执行情况开展独立监督与审计。

4.2 数据隐私与个人信息保护

公司在人工智能系统的开发、训练、部署和运营全过程中严格保护个人信息和数据安全，相关要求与公司《隐私保护政策》保持一致：

（1）坚持合法、正当、必要和诚信原则，训练与运行数据须具备合法来源和使用授权；涉及个人信息的数据实施最小化收集和授权管理，未经信息主体同意不得超出原定目的使用；

（2）建立数据分类分级管理机制，对敏感个人信息及商业秘密采取脱敏、匿名化、加密和访问控制等保护措施；

（3）建立覆盖数据收集、存储、使用、共享、归档和删除全过程的数据生命周期管理机制；涉及数据跨境传输的，严格履行适用法律法规规定的安全评估、备案或认证程序；

（4）禁止员工将公司商业秘密、个人信息及其他受保护数据输入未经公司批准的外部人工智能工具或服务；

（5）定期开展人工智能相关的数据隐私风险评估和内部审查。

4.3 人工智能安全与网络安全

公司将人工智能系统纳入整体信息安全与网络安全管理体系，确保人工智能系统稳定、可靠、可控：

（1）建立人工智能系统安全设计和安全开发要求，将安全要求嵌入系统规划、开发和上线评审流程；

（2）对模型、训练数据、算法代码及运行环境实施分级访问控制和操作日志审计；

（3）开展模型安全测试和漏洞管理，防范数据投毒、模型窃取、对抗样本攻击、提示注入及越权访问等风险；

（4）对工业控制场景中的人工智能应用实施网络隔离与异常流量监测，保障生产系统安全运行；

（5）对第三方人工智能产品和服务开展网络安全尽职调查；

（6）建立人工智能安全事件应急响应机制，并将人工智能系统纳入公司定期漏洞扫描、网络安全攻防演练及内外部审计范围。

4.4 人工监督与人为干预

公司坚持以人为本，确保人工智能始终辅助而非取代人类判断。涉及人身安全、员工权益、客户利益以及重大经营、财务、法律和合规事项的决策，不得完全依赖人工智能系统独立作出：

（1）根据应用场景的风险等级，明确人工审核、人工干预和最终决策机制，确保关键决策能够由授权人员复核、调整或否决；

（2）在生产制造场景中，人工智能工艺控制系统运行时须由授权人员实施监控，并保留随时人工干预、切换至人工控制或紧急停止的权限；人工智能品质检测等系统识别的异常结果，须按规定程序经人工复核确认；

（3）明确人工干预权限和升级流程，建立人工智能异常输出的识别、纠正与回退机制；

（4）防止员工对人工智能输出形成不合理依赖，确保使用人员具备理解和评估人工智能输出结果的能力。

4.5 透明度与可解释性

公司致力于提高人工智能系统的透明度、可追溯性和可信度：

（1）建立人工智能应用台账，对公司人工智能应用的场景、用途、责任人及风险等级、模型版本、部署状态及合规评估结果进行登记管理，并通过可持续发展报告等渠道对主要人工智能应用场景及治理情况进行必要披露；

（2）在用户与人工智能系统进行交互时（如智能客服等），明确告知其正在与人工智能系统交互；禁止向未经批准的公共人工智能服务上传公司商业秘密、客户信息及敏感业务数据。

（3）对人工智能生成或合成的内容，依据适用法律法规和使用场景采取审核、标识或说明措施，对外发布前须经人工审核；

（4）建立模型开发、训练数据、版本变更及部署上线的记录机制，保留关键决策过程的可追溯信息；

（5）在技术可行的情况下提升模型可解释性，优先采用可解释的特征与方法，并为重要业务场景提供必要的决策依据说明。

4.6 公平与非歧视

公司致力于推动公平、公正、包容的人工智能应用。公司人工智能应用目前主要集中于工业制造场景；对于招聘、绩效评价、考勤管理等可能影响个人权益的人工智能应用，公司实施更为严格的公平性管理：

（1）在模型设计、训练和验证过程中识别潜在偏见，提高训练数据的代表性和质量；

（2）禁止人工智能系统基于性别、年龄、民族、种族、国籍、宗教信仰、婚育状况、残障等因素对个人产生不合理的差别对待；

（3）对涉及个人权益的高影响场景开展算法公平性测试，建立偏见识别、监测和纠正机制；

（4）定期评估已部署人工智能系统输出结果的公平性和一致性。

4.7 问责机制与责任治理

公司坚持“责任明确、权责统一、全程可追溯”的原则，确保人工智能应用结果可问责：

（1）明确董事会、数委会、负责任人工智能工作组、业务部门及职能部门在人工智能治理中的职责；

（2）每一个人工智能系统须明确模型所有者和业务责任人，对系统的合规性、安全性及运行结果承担管理责任；

（3）人工智能系统的使用人员对其依据人工智能输出所作出的决定承担相应责任；

（4）建立人工智能风险事件的报告、调查、整改和持续改进机制，对因人工智能应用引发的问题开展原因分析和责任追溯；

（5）为受人工智能决策影响的员工、客户及其他相关方提供说明、异议申诉和人工复核渠道。

4.8 风险评估与分级管理

公司对人工智能应用实行全生命周期风险分级管理：

（1）人工智能系统在立项或采购前，须由业务责任部门完成登记和初步风险识别，并根据其对人身安全、生产安全、员工及客户权益、个人信息、经营决策及环境的潜在影响程度，划分为高、中、低风险等级；

（2）对高风险人工智能应用（包括但不限于涉及生物特征识别或敏感个人信息处理、影响员工或客户重大权益、可能对人身安全或生产安全造成重大影响的应用），须在部署前开展人工智能影响评估，评估内容涵盖数据安全与隐私保护、算法公平性、安全可靠性、透明度、人权及环境影响等方面，并经数委会审批后方可上线；

（3）中、低风险人工智能应用须纳入公司信息系统上线评审流程，完成安全评估和合规审查；

（4）人工智能系统发生重大变更、用途扩展或出现重大风险事件时，须重新开展风险评估。

4.9 模型监控与审计

公司建立人工智能模型的持续监控与审计机制，确保模型在全生命周期内保持可靠、有效：

（1）人工智能模型上线前须完成功能、性能、安全性及可靠性测试验证，达到预设指标后方可部署；

（2）模型上线后建立持续监测机制，针对准确率、误检率、漏检率、稳定性等关键指标以及模型漂移、性能退化情况开展监控，发现异常及时预警、纠正或回退；

（3）建立模型版本管理机制，模型重新训练和迭代更新须经测试验证和审批，并保留完整版本记录；

（4）定期复核模型性能、适用性和风险水平，对不再满足要求的模型予以优化或退役；

（5）将人工智能管理纳入公司内部审计和合规检查范围，由审计部定期对本政策执行情况开展审计。

4.10 应用边界与禁止性应用

公司确保人工智能系统在授权、可控和适用范围内运行，人工智能不作为独立决策主体，也不替代法律法规规定的人类职责。公司明确各人工智能系统的用途、权限和适用场景，禁止超出授权范围使用；对人脸识别、生物特征识别等敏感人工智能能力实施审批、权限控制与日志审计。公司禁止开发、采购、部署或使用人工智能开展以下活动：

（1）操纵、误导或不当影响个人自主决策；

（2）利用弱势群体的脆弱性实施剥削或不公平影响；

（3）对个人进行社会评分并据此实施不利对待；

（4）未经授权或超出法定目的的生物特征识别与监控、非法人脸识别和个人画像；

（5）非法收集、使用或共享个人数据；

（6）生成或传播虚假信息，实施欺诈或制作恶意内容；

（7）侵犯人权或违反国际公认伦理原则的活动；

（8）法律法规禁止的其他人工智能应用。

4.11 绿色低碳人工智能

作为新能源企业，公司将绿色发展理念融入人工智能全生命周期管理：

（1）在采购和部署人工智能产品与服务时关注其能源效率和碳排放表现，优先选择能效较高的解决方案以及使用可再生能源的数据中心和云服务；

（2）持续优化模型训练和推理的算力资源使用，降低人工智能运行的环境影响；

（3）推动人工智能赋能节能降耗、良率提升、绿色制造和资源高效利用，并逐步量化人工智能应用对公司可持续发展目标的贡献。

4.12 第三方与供应链管理

公司将负责任人工智能要求延伸至人工智能相关的第三方合作：

（1）对人工智能供应商及技术服务商开展尽职调查，评估其数据保护、网络安全、模型安全及相关国际法规符合性及伦理管理能力，并在合同中明确合规责任。

（2）在合作协议中明确数据保护、安全保密、知识产权、责任划分及本政策相关要求；

（3）定期评估第三方人工智能产品和服务的风险与绩效表现，发现重大风险时及时采取整改、暂停或终止合作等措施。

4.13 投诉与处罚

我们持续完善已有的内部报告与沟通机制和渠道，以供员工、客户、合作伙伴、供应商及其他相关方报告人工智能相关的风险事件或违规行为，或对人工智能决策结果提出异议和申诉，并定期审查和改进我们的负责任人工智能实践。相关方可直接报告主管领导、公司审计部或通过以下电话、邮箱进行投诉反馈。

电话：022-23789766-8022

邮箱：jubao@tzeco.com

地址：天津市西青区华苑产业园海泰南道 10 号

公司支持匿名举报，同时承诺将严格保密举报人的个人信息，切实保障举报人的合法权利，严禁公司对举报人进行任何直接或间接的歧视、刁难、压制或打击报复等行为。

对于任何违反本政策以及人工智能相关法律法规的行为，我们采取零容忍态度，就违法违规行为及时开展调查和整改行动，并根据事件造成的影响程度和范围，针对主责部门及人员进行相应纪律处分。

4.14 教育与培训

公司持续提升员工负责任使用人工智能的意识和能力：

（1）将人工智能相关的数据安全、隐私保护与合规使用要求纳入全员年度信息安全培训；

（2）面向人工智能开发、运维及使用人员开展人工智能伦理、模型安全及生成式人工智能合规使用等专项培训；

（3）提升管理层和关键岗位员工的人工智能治理能力，推广负责任人工智能实践案例。

5. 政策审阅及修订

本公司负责任人工智能管理工作由董事会作为最高决策和监督机构。本政策与相关承诺的发布已得到本公司高级管理层的认可，由负责任人工智能工作组负责版本管理，并至少每年审阅一次，适时更新修订。审查内容涵盖相关法律法规变化、国际标准与技术发展、客户及监管要求变动，以及公司内部人工智能应用和管理情况。如遇重大变化，将及时更新发布，以确保政策内容的时效性和适用性。

本政策刊载于TCL 中环官网供各利益相关方查阅，并通过邮件、会议、内部学习平台等方式向员工及关键利益相关方宣贯；政策的落实情况及相关关键绩效指标将每年在公司可持续发展报告中披露。