

惠州亿纬锂能股份有限公司人工智能（AI）使用管理政策

一、政策目的

为规范惠州亿纬锂能股份有限公司（以下简称“公司”）内部人工智能（AI）工具的使用，提升 AI 应用的安全性与合规性，切实保护公司、客户及合作伙伴的数据安全与知识产权，公司特制定本政策。本政策作为公司 AI 治理体系的重要组成部分，旨在为负责任创新与可持续经营提供坚实支撑。

二、适用范围

本政策适用于公司全体正式员工、实习生、外包人员，以及使用公司 IT 资源访问 AI 工具的第三方合作人员。

三、AI 治理责任

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》和欧盟《通用数据保护条例（GDPR）》等业务运营所在国家或地区适用的数据保护法规。公司已建立经高级管理层批准的内部 AI 管理机制，并设立专职部门统筹 AI 应用的推广与日常管理工作；各部门则负责落实本领域的 AI 使用风险管理，确保责任到岗、措施到位。

公司围绕 AI 合规与安全应用，全面部署并持续推进以下治理工作：

（一）健全技术管控与审计机制

建立并完善 AI 使用技术管控与审计体系。针对 AI 工具准入，制定并动态更新公司级 AI 工具准入清单，定期开展第三方 AI 工具安全风险评估；针对已部署的 AI 模型，实施定期评估与审查，防范模型运行过程中潜在偏见的产生。

（二）提升 AI 系统透明度与可靠性

主动披露 AI 工具的使用场景、能力范围及功能局限，增强使用透明度。对已部署的 AI 模型进行持续验证与监测，严格规范训练数据来源，及时发现并纠正模型随时间产生的漂移或性能退化，定期实施系统维护与更新，保障 AI 系统的稳定可靠运行。

（三）深化 AI 应用评估与风险防控

建立常态化 AI 应用评估机制，定期追踪各部门 AI 使用情况与效能评分，同步开展信息泄露风险专项评估，确保 AI 技术在全类业务场景中安全、合规落地。

（四）强化全员 AI 安全培训与责任意识

组织开展 AI 安全专项培训，推动全员签署《AI 使用承诺书》。将数据安全与 AI 合规要求纳入新员工入职教育体系，从源头强化员工对 AI 风险的认知与防范能力。

（五）明确责任归属与追责机制

为 AI 产生的结果建立清晰的责任归属体系，各部门负责人为本部门 AI 数据安全第一责任人，负责监督执行与定期自查。对因违规使用 AI 导致错误或造成损害的，公司将依法依规启动调查程序，实施分级追责，并及时采取有效补救措施，切实防范风险扩大。

四、AI 使用规范与工具准入

为明确 AI 工具的授权使用范围与能力边界，公司已建立基于三层数据分类的分级管控机制，据此设定差异化的 AI 使用规则，确保各类 AI 应用在可控预期内安全运行。具体分类及要求如下：

数据类别	定义	使用要求
红线数据	涉及核心技术、未公开专利、敏感经营数据等	严禁以任何形式输入公有 AI 工具
低风险数据	不含具体商业秘密但需脱敏后方可使用	必须脱敏处理，仅限使用公司批准的 AI 工具
通用公开数据	与公司具体业务无关的通用知识	可使用 AI，但不得涉及公司内部信息

注：红线数据示例，如核心配方、工艺参数、未公开研发信息、核心客户/供应商名单及价格等。

（一）AI 生成内容的标识与使用原则

公司对 AI 生成内容实行分类管理，根据内容形态与应用场景设定差异化的标识要求，以提升 AI 生成内容与 AI 交互的透明度。对外发布或交付使用的 AI 生成内容（含文本、图像、音视频等），均应予以显著标注，确保利益相关方能够清晰辨识内容来源，保障其知情权与决策有效性。

AI 输出结果在公司关键业务决策中仅作为辅助参考，最终决策须由具备相应权限的人员做出，确保问责制的有效落实。

（二）敏感 AI 功能的访问管控

对人脸识别、生物特征分析等敏感 AI 功能实施权限管控，仅限经审批的特定场景使用，未经授权不得部署。

（三）AI 工具准入与风险管理

公司对 AI 工具实行准入清单管理，基于安全评估结果实施差异化管控。经评估认定存在显著安全风险（包括但不限于提示词注入、数据泄露、系统漏洞等）的 AI 工具或智能体，原则上禁止在公司内网及办公设备中部署使用。

因技术研究等特殊业务场景确需使用上述工具的，须确保不涉及公司敏感数据、风险可控、网络隔离及权限管控到位的前提下，经授权后使用。

五、AI 应用承诺

公司秉持负责任的 AI 应用理念，做出以下承诺：

（一）致力于尊重数据隐私，保护网络安全。不将 AI 用于可能侵害数据隐私、网络安全、知识产权、商业秘密或用户隐私的行为。

（二）不使用或部署从事操纵性行为、利用弱势群体漏洞、社会评分或未经授权的生物特征识别的 AI 系统。

（三）建立 AI 使用日志与定期审计机制，支撑内部治理与外部监督

（四）根据技术与风险变化，动态更新 AI 工具准入清单与使用规范

（五）优先使用公司统一部署的私有化 AI 平台，确保数据安全可控

（六）推进自有数据中心节能改造，优化基础设施能耗管控，降低包括但不限于碳足迹、水足迹的 AI 生态足迹。

（七）探索设立用户及第三方申诉机制，为受 AI 决策或结果影响的利益相关方提供反馈渠道，保障其合法权益。

六、政策解释与生效

本政策经公司战略与可持续发展委员会（董事会层级委员会）审议批准，通过官网等渠道进行正式对外发布，自发布之日起生效。本政策的最终解释权归公司所有。

惠州亿纬锂能股份有限公司

2026 年 8 月