

江西金力永磁科技股份有限公司

负责任人工智能政策要点

引言

江西金力永磁科技股份有限公司（下称“金力永磁”“公司”或“我们”）严格遵守业务运营所在司法管辖区的所有法律法规。本政策声明旨在规范公司在人工智能（AI）技术的开发、部署及使用过程中的行为准则，确保 AI 的应用符合道德规范、法律法规及国际标准。

此政策适用于公司内部所有涉及 AI 的业务活动，包括但不限于生产质量控制、供应链优化、客户服务及内部运营管理等场景。

第一部分：负责任人工智能政策要点

1. 数据隐私保护：在 AI 系统的开发与使用全生命周期中，公司尊重并保护个人隐私。数据的收集、存储、处理及传输应遵守适用的数据保护法律法规（如《中华人民共和国个人信息保护法》及相关地区法规）。AI 系统处理的数据应当具有明确的合法基础，并采取适当的技术和组织措施确保数据安全。

2. 网络安全保障：公司在 AI 系统的开发与使用中实施网络安全措施，防止未经授权的访问、攻击或数据泄露。这些措施包括但不限于渗透测试、安全事件响应、加密传输、安全编码规范及对恶意输入的防范机制。AI 系统的安全架构应与公司整体信息安全管理体系统衔接。

3. 公平性与偏见防范：公司在 AI 系统的设计与开发中采取措施识别和缓解潜在偏见。这包括使用多元化、具有代表性的数据集训练

模型，在模型部署前进行偏见检测与评估，并在运行过程中持续监控模型输出的公平性。如发现模型存在对特定群体的不公正待遇，应启动纠正流程。

4. 人工监督与干预机制：对于可能导致重大业务影响、法律后果或对个人权益产生重大影响的 AI 决策，实施人工监督机制。根据风险程度实施事前审批或事后审查，高风险决策须经人工复核方可执行，并保留人工干预权。

5. 透明度与可解释性：公司对 AI 系统的使用情况、能力、局限性、数据来源及潜在风险进行披露，使相关方能够理解 AI 系统如何影响其决策或结果。当用户与 AI 系统交互时，以适当方式告知其正在与 AI 而非人类交互。对于 AI 驱动的重要决策，提供与利益相关方需求相匹配的解释说明。

6. 责任界定与问责：公司就 AI 模型或工具产生的结果建立清晰的责任体系。明确指定负责 AI 项目全生命周期管理的责任人员及其职责范围，包括风险评估、合规审查与纠正措施的执行。对于 AI 系统引发的错误或损害，建立调查与处理机制，确保可追溯至具体责任主体。

7. AI 能力边界：公司明确界定 AI 系统的授权使用范围、功能能力及局限性，制定相应的使用政策与防护措施，防止误用、范围蔓延或非预期用途。

8. 生态可持续性要求：公司要求自有或第三方 AI 数据中心及模型训练环境在能源消耗、水资源使用及碳排放方面达到合理的效率水

平。在选择 AI 基础设施和服务供应商时，将能效指标纳入评估维度，优先选用采用可再生能源且能效达标的方案。

9. 禁止性 AI 应用：公司不使用或部署从事以下行为的 AI 系统：通过潜意识、故意操纵或欺骗性手段实质性扭曲个人行为；利用个人年龄、身体状况、经济困境等漏洞实施损害；对个人进行社会评分；实施未经授权的实时远程生物特征识别。

第二部分：负责任人工智能政策管理要求

1. 敏感 AI 能力管控：对于人脸识别、生物特征识别、行为监控等敏感 AI 能力，实施严格的访问控制。仅允许经授权的人员在明确的业务场景和履行审批程序后方可使用。建立这类技术的使用登记与审计记录，确保可追溯。

2. AI 生成内容标注：对于 AI 系统生成的文本、图像、视频或其他内容，以及 AI 驱动决策的结果，实施明确标注。这有助于用户区分人工创作与 AI 生成内容，并使其能够就影响自身的 AI 决策作出明智判断。

3. 模型漂移监测与纠正：建立机制监测 AI 模型在部署后的性能变化。当输入数据分布或业务环境发生变化导致模型准确率下降或输出偏离预期时，触发预警并启动纠正措施，包括但不限于重新训练、参数调整或模型更新，以确保 AI 系统持续可靠运行。

4. 公平性定期评估：对已部署的 AI 模型开展系统性的公平性与偏见评估。评估包括审查、偏见测试及各类人群的待遇分析，确保模型不因性别、年龄、地域等因素产生不合理差异。评估结果记录在案，

并作为模型优化的依据。

5. 生态足迹降低举措：公司就 AI 运算的环保影响采取管控措施，包括优化算法以降低计算量需求、采用高效硬件设施、优先使用可再生能源供电的数据中心。在与供应商合作时，将环保表现纳入供应商评估体系。

6. 申诉处理流程：建立透明的申诉渠道，使受 AI 决策影响的个人或组织能够就不当结果提出异议。申诉流程应具备可访问性、公正性及及时响应特征，提供清晰的补救或说明路径。对于涉及个人权益的重大决策，确保受影响方获知并能够行使申诉权。

7. 可持续影响量化：对 AI 举措及工具在可持续发展方面的影响进行定期评估与量化，覆盖碳排放、资源效率及社会影响等维度，支撑公司对 AI 投入产出效率的判断。

8. 员工培训：开展针对员工的 AI 伦理与安全培训，内容涵盖数据隐私保护、AI 决策的伦理影响、以及 AI 系统安全防护措施等。开展分层级、针对性的 AI 伦理与安全培训，确保员工具备相应能力。

9. 外部验证：公司 AI 管理体系将根据业务发展情况，引入第三方机构进行适当的标准化评估，以验证管理措施的有效性。

第三部分：附则

本政策经公司高级管理层审议批准并监督执行，内容由公司负责解释。本政策每年至少复审一次，或在监管规定、技术环境发生重大变化时及时修订。如本政策条款与上位法规冲突，以法规为准。