负责任人工智能应用政策

第一章　总则

第 1 条 为规范江苏中天科技股份有限公司（以下简称"公司"）在人工智能技术研发与应用过程中的行为，确保 AI 技术安全、可靠、透明、公平地服务于生产经营与可持续发展目标，依据《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》《新一代人工智能治理原则——发展负责任的人工智能》等法律法规及行业标准，结合公司实际情况，制定本政策。

第 2 条 本政策适用于公司及其下属子公司、分支机构在人工智能技术的研发、采购、部署、运营、退役全生命周期中的所有相关活动，包括但不限于：工业视觉检测、设备健康管理、智能排产优化、数据分析预测、大语言模型应用、机器人自动化等各类 AI 场景。

第 3 条 公司坚持以下基本原则：

- 以人为本：AI 应服务提升员工效率与产品质量，不得用于替代关键岗位人员的最终判断权或损害员工合法权益；
- 安全可控：确保 AI 系统在网络、数据、算法层面的安全性，防范外部攻击与内部误用风险；
- 透明可解释：AI 决策过程应有据可查，核心模型具备可解释性，用户能够理解系统输出的逻辑；
- 公平公正：避免因训练数据偏差或算法设计缺陷导致对特定群体或业务环节的歧视性结果；
- 绿色低碳：优先选用生态足迹较低的 AI 数据源和计算资源。

第二章　组织与职责

第四条　决策支持机构

第 4 条 本政策的最高级别决策支持机构为集团技术委员会，负责审批重大 AI 项目立项、年度 AI 战略规划、重大风险事件处置方案以及本政策的修订。

第五条　归口管理部门

第 5 条 公司数字化部为本政策归口管理部门，具体履行以下职责：

- 组织制定、修订并发布本政策及相关配套管理制度；
- 审核各产业板块 AI 项目的合规性，出具合规评估意见；
- 统筹 AI 伦理培训与宣贯工作；
- 受理并协调处理 AI 应用相关的投诉与争议。

第六条　业务部门职责

第 6 条 各业务部门作为 AI 应用的主体责任单位，负责：

- 在本部门 AI 项目中落实本政策各项要求；

• 建立部门级 AI 使用台账，定期向归口部门报送运行情况；

• 配合开展审计、评估与应急响应工作。

第三章　数据隐私保护

第 7 条 公司在 AI 系统的开发与应用过程中应当尊重并严格保护数据隐私：

• 采集数据限于实现预定功能所必需的最小范围，遵循数据最小化原则；

• 涉及个人信息的 AI 应用须事先完成个人信息保护影响评估，获取被采集对象的知情同意；

• 生产类图像/振动信号等不含个人信息的数据，仍按《信息安全管理制度》实行分级分类管理，存储于内网服务器，禁止未经授权外传；

• 数据保留期限以满足业务需求和法规为限，超期按销毁流程处置。

第四章　网络安全保障

第 8 条 公司应保障 AI 应用的网络安全，采取以下措施：

• 训练平台、推理服务器、边缘计算节点均部署于内网隔离环境，严禁直接暴露公网；

• 模型更新与参数下发通过加密通道传输，全程记录操作日志，留存不少于 180 天；

• AI 接口服务须通过统一 API 网关进行访问控制与流量监控；

• 每季度至少开展一次针对 AI 系统的网络安全漏洞扫描与渗透测试，高危漏洞 72 小时内修复。

第五章　公平性与偏见防控

第 9 条 公司应主动避免偏见和不公平结果：

• 训练数据集应在来源、工况条件、时间跨度等方面保持多样性覆盖，避免单一偏差；

• 上线前应开展多维度公平性测试，验证不同批次、不同生产线下的表现一致性；

• 建立定期偏见检测机制，发现显著偏差时立即启动模型审查与修正流程。

第六章　人工干预机制

第 10 条 关键领域 AI 应用必须确保人员参与决策并可人工干预：

• AI 定位辅助工具，不替代专业人员最终判断权和签字确认权；

• 质量判废、停机告警等高等级 AI 结论须经人工复核后方可生效；

• 每个 AI 终端界面应设置"人工接管/暂停"功能键，操作人员可随时中断自动判定流程。

第七章　透明度与可解释性

第 11 条 公司应确保 AI 系统的透明度及决策的可解释性：

• 核心 AI 模型的技术原理、输入输出规格、适用边界在内部知识库备案；

• 每次输出（如检测结果、预警信息）附带置信度评分及诊断依据说明或可视化标注；

• 深度学习模型须配套可解释性分析模块（如特征重要性热力图），使操作人员能理解判断逻辑。

第八章　问责机制

第 12 条 公司明确界定 AI 模型工具产生结果的问责机制：

- 正常运行期间常规输出，由使用该系统的业务部门承担业务责任；
- 因模型缺陷导致批量错误判定，由开发团队调查原因并提出改进方案；
- 违规操作或绕过安全机制导致的损失，由操作责任人承担责任；
- 重大安全事故由执委会成立专项调查组问责认定。

第九章　任务边界界定

第 13 条 明确 AI 部署与无法执行的任务范围：

- 允许事项：数据分析、模式识别分类、趋势预测建议、流程自动化辅助、报表生成；
- 禁止事项：自主决定产品放行拒收最终签字、未经授权人员评分评价、生物特征强制监控、超出预设范围的自主扩展感知或控制行为。

第十章　生态足迹管控

第 14 条 公司鼓励选用生态足迹较低的 AI 数据源及模型：

- 优先采用轻量化架构（剪枝、量化、知识蒸馏），降低推理能耗；
- 充分利用已有标注数据集，减少重复采集资源浪费；
- 算力基础设施优先考虑符合节能型 GPU 集群与绿色数据中心标准的设施。

第十一章　高风险 AI 禁用清单

第 15 条 公司禁止开发或使用具有以下功能的 AI 系统：

- 威胁具身智能行为的恶意操控模块；
- 利用漏洞实施未授权访问或数据窃取的工具；
- 对员工或外部人员进行社会信用评分的系统；
- 未经合法授权的生物特征大规模监控功能。

上述规定参照欧盟《人工智能法案》（EU AI Act）关于高风险及禁止用途条款执行。

第十二章　附则

第 16 条 本政策由公司数字化部负责解释。

第 17 条 本政策自发布之日起施行，有效期三年。期满前六个月启动修订评估程序。

江苏中天科技股份有限公司

2026 年 7 月 10 日