

益海嘉里金龙鱼食品集团股份有限公司

负责任的人工智能使用政策

随着数字经济的蓬勃发展与新一代技术革命的加速，人工智能（AI）正以前所未有的深度重塑商业逻辑与社会形态。益海嘉里金龙鱼食品集团股份有限公司（以下简称“公司”）将安全、可控、负责的人工智能治理作为公司数字化转型的重要组成部分。为此，公司特制订本政策，旨在明确公司在人工智能领域的伦理边界与行动准则，确保技术进步始终与维护个人权益、增进公众信任、推动环境友好同向而行。

1. 适用范围

本政策适用于公司及子公司，以及代表公司提供 AI 相关产品或服务的供应商和合作伙伴。

2. 数据隐私

公司在 AI 全生命周期尊重并保护个人信息、重要数据、商业秘密、知识产权和其他受保护数据，遵循合法、正当、必要、目的明确、最小化和安全保障原则。在 AI 系统的开发、训练与应用过程中，落实数据分类分级管理。未经必要的安全评估与明确授权，严禁将涉及用户隐私、商业机密、核心算法及依法受保护的经营数据输入公共 AI 工具或未经认证的第三方模型，确保数据资产在 AI 时代的安全。

3. 信息安全

公司已建立符合 ISO27001 要求的信息安全管理体系，并将 AI 相关的基础设施、系统和服务参照信息安全管理要求，并按照 PDCA 原则实施持续管理与改进。针对提示注入、数据投毒、模型窃取、敏感信息泄露、不安全输出和不当内容等 AI 特有风险，公司已建立与风险相适应的输入输出护栏、内容过滤、安全测试和监测措施。公司根据 AI 的风险，实施身份认证、最小权限、加密、安全编码、漏洞管理、渗透测试、日志审计、事件响应及业务连续性管理。发现重大漏洞、失控行为或不可接受风险时，公司有权立即限制、回滚、中止或停用相关 AI 系统。

4. 公正与偏见防范

公司在设计、开发和使用 AI 时，应避免基于种族、民族、国籍、性别、年龄、残障、

宗教、健康状况或其他受保护特征产生不公平、歧视或排斥性影响。

公司应识别训练数据、特征选择、标签、模型设计和应用场景中的潜在偏见，优先使用充分、准确、多样且具有代表性的数据集。对于可能影响个人权益的重要场景，应开展分群性能测试、偏见审计和不利影响评估，并根据评估结果采取数据修正、参数调整、重新训练、人工复核、限制用途或停止使用等纠偏措施。

5. 人类监督与干预

公司坚信 AI 是辅助决策的工具。在涉及重大经营决策、财务披露、质量安全、人才评价及生命健康等高敏感、高风险领域，AI 的输出仅作为辅助参考。公司承诺在上述关键业务链路中保留有效且有记录的“人类监督（Human-in-the-loop）”机制，确保人类始终拥有对 AI 系统进行审查、介入、否决及中止使用的最终决定权。

6. 透明度

根据适用法律法规和具体场景，公司将采用清晰、易识别的方式标识 AI 生成或实质性合成的文本、图像、音频和视频，避免用户将 AI 生成内容误认为真实人员创作或客观事实。对影响个人权益或关键事项的 AI 辅助决策，应在合理范围内说明 AI 的参与方式、主要影响因素、能力局限和人工复核安排，并保留系统或模型版本、重要输入、输出结果、人工复核及最终决定等必要记录。

7. 责任与问责

业务负责人是具体 AI 场景的第一责任人，负责业务目的、合法性、适当性、输出使用和影响管理。技术团队负责架构、数据、模型、测试、部署、监控、变更和退出等技术控制。职能部门按职责独立审查、监督和提出整改要求。AI 不承担法律或管理责任，批准、开发、部署、监督或使用 AI 的人员对其行为、决定及后果负责。此外，因违规使用 AI 或因管理不到位造成不良影响的，公司将依照内部事故管理相关制度追究责任。

8. 能力边界与可接受使用

公司为每项 AI 系统明确相关使用人员范围、数据范围、能力与性能局限、人工监督要求、异常升级和停用退出等条件。AI 不得超越授权范围介入本应由人工进行独立判断的关键事项及在不受控情况下应用于高风险和敏感场景。公司员工不得擅自将 AI 连接至生产系统、敏感数据源或可执行高影响操作的工具；未经人工核验的 AI 输出，不得直接用于对外承诺。

9. 低生态足迹与绿色 AI

在满足安全、质量、合规和业务要求的前提下，降低自有或第三方 AI 能力、模型训练和推理的能源、水资源、碳排放及硬件资源足迹。采购或选择模型、平台和数据中心时，将经济投入、能源效率、碳排放与水资源信息、设备利用率等纳入评估。优先采用与任务相匹配的较小或更高效模型、复用已有模型、优化调用与缓存、合理设置训练频率和保存策略，避免无必要的重复训练和过度算力消耗。

10. 第三方与采购管理

公司引入第三方 AI 模型、平台、代理或开发服务前，应充分评估人工智能系统的合规性，确保 AI 系统在开发及应用过程中满足包括数据使用与再训练、数据位置与跨境、留存删除、网络与数据安全、模型能力与局限、公平性、透明度等公司要求。

公司在第三方采购合同中应明确数据权利与用途限制、不得擅自训练、保密与安全措施、事件通知、服务连续性、模型或条款变更通知等。

11. 持续监测与改进

建立适当的性能、准确性、稳健性、公平性、安全性、可用性和资源效率指标，持续监测性能退化、异常输出和控制失效等能力。重大模型、数据、用途、接口、供应商或基础设施变化，应触发重新评估、测试与批准。重要或高风险系统至少按年度或风险要求复审。

任何人员发现 AI 造成或可能造成隐私泄露、安全事件、歧视、不实信息、重大错误、失控行为或其他伤害，应立即通过公司内部事件报告、合规举报或其他举报渠道报告。

12. 禁止的 AI 实践

公司禁止开发、采购、使用或部署下列不可接受的 AI 系统或实践：

- A. 使用潜意识、操纵、诱导或欺骗技术，实质性扭曲个人行为并造成或可能造成重大伤害。
- B. 利用因年龄、残障或特定社会经济处境形成的脆弱性，对个人或特定群体实施剥削、误导或不当影响，实质性扭曲其行为并造成或可能造成重大伤害。
- C. 基于个人或群体的社会行为、人格特征、个人特征或推断特征实施社会评分、社会排序，进而导致在与数据收集目的无关的场景中受到不利待遇，或者受到不合理、不成比例的差别待遇。
- D. 无差别抓取互联网或闭路电视图像，以建立或扩充人脸识别数据库。

E. 未经合法授权开展实时远程生物特征识别、面部识别监控或其他生物特征监控。

F. 其他违反法律法规、基本权利、商业伦理或公司制度的 AI 系统和实践。

13. 培训与意识

公司定期根据角色和风险开展 AI 素养、AI 风险、可接受使用、数据隐私、网络安全、知识产权和事件报告等多维度培训。开发人员、审批人员、监督人员及高风险场景使用者接受与职责相匹配的专项培训并定期更新。

14. 附则

本政策由公司 IT 部负责解释和实施。

本政策至少每年审查一次，并在法律监管、公司战略、技术能力、风险环境或重大事件发生变化时及时修订。

益海嘉里金龙鱼食品集团股份有限公司

二〇二六年九月十六日