负责任人工智能（AI）政策

为规范人工智能（Artificial Intelligence，以下简称“AI”）技术在中国石油天然气股份有限公司（以下简称“公司”）各业务领域和管理场景中的开发、部署与应用，统筹推进数字化智能化转型与风险防控，推动 AI 技术依法合规、安全可控、以人为本、公平可信、透明审慎和绿色可持续发展，防范 AI 应用可能带来的安全、合规、伦理、数据、环境及社会风险，特制定本政策。本政策阐明公司负责任人工智能管理的基本立场与行动承诺，旨在保障技术创新和业务赋能的同时，维护员工、客户、合作伙伴及其他利益相关方合法权益，保障生产运营安全和公共利益，促进 AI 技术价值与公司高质量发展、可持续发展相协调。

一、基本原则

公司坚持依法合规、以人为本、安全可控、公平公正、透明可信、权责清晰、绿色低碳的原则，将负责任 AI 要求融入技术研发、采购、部署、使用、监督和退出等环节。在勘探开发、炼化新材料、天然气销售、新能源、工程技术、生产运营、供应链、客户服务、科研创新、财务管理及数字化管理等场景推进 AI 应用时，同步识别并管控相关风险，确保 AI 应用与公司发展战略、风险管理要求及可持续发展目标相协调。

二、尊重数据隐私与数据权益

公司尊重并保护 AI 开发和使用过程中涉及的个人信息、重要数据、核心数据、商业秘密、未公开经营信息及其他依法受保护的数据，严格遵守业务所在国家和地区适用的数据安全、个人信息保护及隐私保护法律法规。公司根据数据分类分级和授权管理要求，明确 AI 应用的数据来源、使用目的、处理范围、保存期限和访问权限；未经合法授权或合规审查，不得将涉及个人信息、敏感信息、商业秘密、重要生产经营信息及其他受保护数据输入未经批准的外部 AI 工具、第三方模型或服务。

三、保障网络、信息与生产安全

公司将 AI 系统、模型、工具、接口及相关服务纳入网络安全、数据安全和信息安全管理体系，并结合油气生产运营特点，加强对工业控制系统、生产网络、关键基础设施及重要业务系统相关 AI 应用的安全管理。根据风险水平采取身份认证、最小权限访问、数据加密、日志留痕、漏洞管理、安全测试、监测预警和应急响应等措施，防范恶意攻击、数据篡改、模型窃取、提示注入、错误调用及其他安全威胁。对于采购或合作使用的第三方 AI 平台、模型及服务，公司审慎评估其服务资质、技术能力、数据安全、网络安全和持续服务能力，并通过合同或协议明确相关安全责任。

四、防范偏见、歧视与误导风险

公司关注 AI 在数据采集、训练、模型设计、算法运行和输出结果中可能产生的偏见、歧视、失真和误导风险，并根据应用场景和影响程度开展必要的公平性、准确性和稳健性评估。对于涉及员工管理、客户服务、供应商管理、合作伙伴评价及其他可能影响利益相关方权益的应用场景，坚持审慎使用，避免因不合理的数据、指标或算法设计造成不公平差别待遇；必要时采取人工复核、结果校验和纠偏措施。

五、保证人类监督与人工干预

公司坚持在重要和高风险事项中保留充分的人类监督与人工干预机制。对于重大经营决策、财务披露、投资决策、合规判断、法律事务、HSE 管理、产品质量、设备安全、生产调度、工艺控制、应急处置、人身安全及其他重要敏感事项，坚持“人类主导决策、AI 辅助支持”的原则。未经授权和充分验证，AI 不得自主作出关键决策，不得直接控制可能对生产安全、环境安全、人身安全或重大资产安全产生实质影响的关键生产设备和系统。相关责任人员应根据具体场景对 AI 运行状态、输出结果和应用过程进行审查、核验、修正、中止或停止使用。

六、确保透明度、可追溯性与可解释性

公司重视 AI 应用的透明度、可追溯性和可解释性，根据不同应用场景及风险等级采取适当的标识、解释说明、过程记录和日志留痕措施。对于生成式 AI 应用以及预测分析、分类识别、异常检测、智能推荐、设备诊断、决策支持等非生成式 AI 应用，合理记录模型或工具来源、适用场景、关键输入输出及必要的人工审核情况。对于缺乏合理依据、逻辑异常、明显偏离事实或无法进行必要解释和验证的 AI 输出，公司坚持谨慎使用，不将其直接作为重要事项的最终决策依据。

七、责任落实与问责管理

公司建立与现有治理和管理体系相衔接的 AI 应用责任机制，按照“谁主管谁负责、谁使用谁负责”的原则，明确业务部门、技术支持部门及相关职能部门的职责边界。业务使用部门对 AI 在本业务场景中的适当性、合规性及结果应用承担相应管理责任；相关职能部门按照职责分工开展技术管理、安全保障、数据管理、合规审核、风险监督等工作。针对第三方 AI 平台、模型及服务，在合作协议中合理明确各方责任。对违反法律法规、公司制度或本政策要求使用 AI，以及因管理不到位造成不良影响的，依规依纪追究相关责任。

八、划定清晰应用边界

公司根据 AI 应用的业务属性、数据敏感程度、影响范围和风险等级，明确不同 AI 工具和应用场景的适用范围、使用限制、审批要求和控制措施，划定 AI “可为”与“不可为”的边界。AI 不得超越授权范围介入应由人员独立判断或依法履职的关键事项，不得在缺乏有效安全控制、人工监督、测试验证和应急机制的情况下用于高风险或敏感场景。对

于涉及油气生产、炼化装置、管网运行、工程作业、危险化学品、安全环保及应急管理等场景的 AI 应用，应实施与其潜在影响相匹配的更严格风险控制。

九、降低生态足迹与提升运营效率

公司倡导在 AI 开发、训练、部署和使用过程中兼顾资源能源消耗、温室气体排放及其他环境影响与业务运营效率。在满足安全、合规、质量和业务需求的前提下，关注 AI 模型、算力平台、数据中心和相关服务的能效与资源利用效率，鼓励通过合理选型、模型优化、算力调度、适度调用和资源复用等方式降低 AI 应用的生态足迹。公司积极发挥 AI 在提高能源资源利用效率、优化生产运营、加强设备预测性维护、提升安全环保管理、支持节能降碳和新能源业务发展等方面的积极作用。

十、禁止性要求

公司禁止开发、部署或使用以下 AI 系统或应用：

（一）通过操纵、诱导、欺骗等方式不当影响他人自主判断和行为的系统；

（二）利用特定群体脆弱性实施剥削、误导或不当影响的系统；

（三）用于不当社会评分、社会排序或基于不合理标准实施歧视性差别待遇的系统；

（四）未经合法授权开展生物特征识别、面部识别监控或其他生物识别监视活动的系统；

（五）未经授权自主控制关键生产设施、工业控制系统，或自主作出可能对生产安全、人身安全、生态环境及重大资产安全产生重大影响的关键决策的系统；

（六）用于伪造、篡改重要生产经营数据、财务信息、合规记录、安全环保记录或其他依法依规应当真实完整信息的系统；

（七）违反法律法规、监管要求、伦理规范及公司制度的其他 AI 系统和应用。

十一、异议与复核机制

对于 AI 生成结果或 AI 辅助决策对员工、客户、供应商、合作伙伴及其他相关方权益产生重大影响的，公司支持相关方按照适用法律法规、公司制度或业务规则提出异议、申诉或复核申请。公司根据具体场景组织人工复核，并视情况采取解释说明、结果修正、重新评估、中止适用或其他必要措施，保障相关方合理权益。

十二、培训、评估与持续改进

公司结合业务发展、技术迭代、风险变化和全球 AI 监管要求，持续完善 AI 治理机制，适时开展 AI 合规、安全、数据保护、伦理和负责任使用等培训，提升员工规范开发和使用 AI 的意识与能力。公司根据 AI 应用的重要性和风险水平开展必要的风险评估、测试验证和持续监测，关注 AI 对能源消耗、碳排放、员工与社会影响、业务效率及可持

续发展等方面的影响；对重要或高风险 AI 工具，可结合实际需要开展独立评估或外部验证。针对 AI 使用过程中发现的问题、风险和缺陷，及时采取整改、优化、限制使用或退出等措施，形成管理闭环。

十三、附则

本政策由公司董事会监督，董事会可持续发展委员会按照职责履行相关监督职责。ESG 管理工作委员会及相关职能部门按照公司现有治理架构和职责分工推动本政策落实、定期检讨和持续完善；各业务及所属单位负责将本政策要求落实到具体 AI 应用场景和管理流程中。公司将结合适用法律法规、监管要求、技术发展和业务实际，适时对本政策进行修订和更新。