**基于大语言模型建立企业本地知识库应用研究招标技术文件**

1. **系统工程概况**

本项目基于开源大语言模型建设本地化智能应用系统，实现通用聊天、知识库问答、供应商资质评审、采购合同评审、投标文件评审等功能。系统需对企业内部文档及业务资料进行整理和结构化处理，结合智能检索、语义分析与自动评审技术，提供高效、精准的问答与评审能力，并与现有信息系统集成，确保数据安全与隐私保护，提升知识利用和业务管理的智能化水平。

1. **招标工作内容范围及要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目/服务名称** | **项目实施范围及内容** | **交验需达到的功能要求** | **甲供、乙供** | **备注说明(需技术方案、施工安全方案或其他要求说明)** |
| 1 | 大模型智能体基础平台 | 开发搭建公司大模型智能体基础平台（甲方提供服务器） | 详见技术要求 | 乙供 | 提供技术方案 |
| 2 | 大模型智能体知识库调优服务 | 提供专业的知识库调优服务方案并负责实施，以提升智能体应用的准确性和效率。 | 详见技术要求 | 乙供 | 提供技术方案 |
| 3 | 智能体构建开发服务（包含通用聊天助手、知识库问答智能体、供应商资质评审智能体、采购合同评审智能体、投标文件评审智能体） | 开发实现通用聊天助手、知识库问答、供应商资质评审、采购合同评审、投标文件评审五个AI智能体应用。 | 详见技术要求 | 乙供 | 提供技术方案 |

1. **技术标准和规范**

本项目执行以下标准和规范要求：

1.国家及行业标准

* 《GB/T 25000.51-2016 信息技术 软件工程 软件产品质量要求与评价（SQuaRE） 第51部分》
* 《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
* 《GB/T 35273-2020 信息安全技术 个人信息安全规范》
* 《GB/T 25000.10-2016 信息技术 软件工程 软件质量模型》
* 《GB/T 8567-2019 信息技术 软件工程 文档编制规范》
* 《GB/T 28827.1-2012 信息技术服务 运行维护 第1部分：通用要求》
* 《GB/T 31167-2014 云计算 服务安全能力要求》
* 《GB/T 31168-2014 云计算 服务质量评价方法》

2.信息安全及数据保护法规

* 《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》
* 《关键信息基础设施安全保护条例》
* 工业和信息化部《工业数据分类分级指南》

3.人工智能与软件开发相关要求

* 《人工智能伦理规范》（国家新一代人工智能治理专业委员会）
* 《信息安全技术 机器学习模型安全能力要求（征求意见稿）》
* 软件开发须遵循 OWASP Web 安全标准，防范 SQL 注入、跨站脚本（XSS）、文件上传漏洞等常见安全风险。
* 所有引用的第三方开源组件必须采用商业友好的开源许可协议（如 MIT、Apache 2.0、BSD），不得使用具有强传染性的 Copyleft 协议（如 GPL、AGPL），以保障招标方知识产权安全。

4.硬件与网络设备规范

* 所有硬件设备应符合国家强制性产品认证（CCC认证）要求，并满足原厂技术规格。
* GPU、服务器、网络交换机等硬件应符合相关国际标准（如 IEEE、PCI-SIG 等）。
* 所有硬件需为全新原装产品，提供可追溯序列号及官方验证方式。

5.企业内部标准与管理制度

* 系统应符合招标方信息化建设管理制度、数据安全管理制度及知识产权保护制度的相关要求。
* 系统与现有公司OA系统、数据中心及网络安全体系对接时，应符合公司现有接口规范及安全策略。

6.文档与交付规范

* 所有交付的技术文档、培训材料及报告必须使用中文简体编写，并符合《GB/T 8567-2019》文档编制规范。
* 所有技术文档中使用的计量单位必须符合国家法定计量单位要求。
1. **技术要求**
2. 总体要求

本项目建设基于公司本地私有化部署的大语言模型应用系统，开发大模型智能体基础平台、知识库调优服务及四个核心业务智能体，实现知识库问答、供应商资质评审、采购合同评审、投标文件评审等功能，并与公司 OA 系统集成，提升业务智能化水平。交付内容包括平台、调优服务、业务智能体、GPU 硬件及安装调试、培训、质保等。系统须在招标方本地部署，数据不得出公司内网，项目成果的全部知识产权归招标方所有。中标方应按期交付，确保系统稳定、功能完善、满足需求。

1. 系统硬件配置要求及硬件设备规格清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **购买设备名称** | **型号规格** | **数量** | **品牌、生厂商** | **产地** | **要求及说明** |
| 1 | 专业级图形处理器（GPU） | NVIDIA RTX A6000 48G | 2 | 英伟达 | 美国 | 或其他性能相当，且兼容公司服务器的品牌 |

1. 系统软硬件指标要求

所列技术参数为技术上的基本要求，若招标文件中涉及品牌、资质、专利、商标、技术要求等含有倾向或者排斥潜在供应商的内容均不作为必须的技术要求，但投标人拟投货物须相当于或优于招标文件中技术要求，投标人在中标后，需严格遵照投标文件相应承诺执行。

文件中加★条目不允许负偏离，若出现负偏离，投标将被否决；其余均允许正偏离、负偏离。

1. 大模型智能体基础平台

| **序号** | **技术指标** | **技术参数及指标** |
| --- | --- | --- |
|  | 功能要求 | **模型管理**：支持添加和管理多种国产主流开源大语言模型（如 DeepSeek、通义千问 Qwen、智谱 ChatGLM 等）并本地部署；管理员可统一设置默认模型并管理启停。 |
|  | ★**知识库管理**：支持知识库创建、文档导入、文档分片管理、可视化列表展示、标签化管理与检索。（提供截图证明） |
|  | **智能体管理**：支持手动、模板、导入三种创建方式；支持编辑、复制、置顶、删除、导出配置及标签管理。 |
|  | ★**流程编排：**提供低/无代码图形化流程画布，支持 DAG 流程定义，预置不少于 19 类标准流程节点（如开始、LLM、知识检索、条件分支、HTTP 请求等）。（提供截图证明） |
|  | ★**智能体发布：**支持发布为 API、Iframe 嵌入代码、独立应用；支持对话式与任务式应用模式，具备文件上传、历史记录、重新提问、流式输出等功能。（提供截图证明） |
|  | 产品维保 | ★提供不少于一年的免费技术支持和模型优化服务（自整体项目验收合格之日起计算）。并出具的售后服务承诺函（加盖投标人公章）。 |
|  | 性能要求 | 支持并发用户不少于 50个，可扩展至 250 并发。（投标人提供承诺函并加盖投标人公章）。 |
|  | 安全合规要求 | 系统本地私有化部署，禁止外网访问。 |
|  | 基于角色的访问控制（RBAC），支持精细化授权。 |
|  | 数据静态加密存储，传输采用 TLS 1.2 及以上协议。 |
|  | 具备审计日志功能，记录用户登录、文件上传、查询、评审、导出等关键操作。 |
|  | 开发遵循安全编码规范，防范常见 Web 安全漏洞。 |
|  | 开源许可声明 | 平台所使用的所有第三方开源组件，需遵循业界主流的、商业友好的开源许可协议，如MIT License、Apache 2.0或BSD Licenses等。不得采用具有强传染性（Copyleft）的协议（如GPL、AGPL），以保障招标方的知识产权安全与商业使用的灵活性。 |
|  | 部署要求 | **部署方式：**部署于公司提供的服务器，数据不得出公司内网。 |

1. 大模型智能体知识库调优服务

| **序号** | **技术指标** | **技术参数及指标** |
| --- | --- | --- |
|  | 服务要求 | **数据预处理：**图片方向校正、文本格式规范、文件分类与打标、关键信息提取与标注。（需在调优方案中描述具体调优方法） |
|  | **分段策略：**对分段标识符、最大长度、重叠长度各进行不少于 3 种配置的对比调优。（需在调优方案中描述具体调优方法） |
|  | **文本清洗：**调优空格/换行符、URL/邮箱处理策略，支持 Q&A 模式开关调优。（需在调优方案中描述具体调优方法） |
|  | **嵌入与重排模型：**适配不少于32种嵌入模型及8种向量检索 Rerank 模型。（需在调优方案中描述具体调优方法） |
|  | **LLM 参数与流程调优：**优化温度、TopP、存在惩罚等 8 类参数，多/单知识库调用模式优化，问题分类器指令优化。（需在调优方案中描述具体调优方法） |
|  | **业务流程构建：**构建不少于3种不同业务智能体流程，并验证有效性。 |
|  | **检索策略：**向量检索、全文检索、混合检索三种模式均需调优 TopK 值、Score 阈值及语义与关键词权重组合。（需在调优方案中描述具体调优方法） |

1. 智能体构建开发服务

| **序号** | **技术指标** | **技术参数及指标** |
| --- | --- | --- |
|  | 功能要求 | **通用聊天助手：**提供基于大模型的通用智能对话能力，支持员工快速获取信息、解决问题，并辅助日常工作；支持用户多轮对话，并支持用户上传文件后基于文件内容进行问答；通用聊天助手与公司OA系统集成。 |
|  | **知识库问答**：构建一个能够深度理解公司内部知识（OA系统中的规范制度等）的智能问答机器人，为员工提供精准、快速的知识查询服务；支持对指定文件夹内的文档进行自动学习，实现知识库的自动构建和增量更新；能够准确理解用户的自然语言查询意图，返回最相关的答案，并必须附上答案来源的原文片段及文档出处，以供溯源。对于知识库无法覆盖的问题，能做出明确、友好的提示。 |
|  | **供应商资质评审**：自动评审供应商提交的各类资质文件（如营业执照、体系认证证书、财务报表），高效完成初步筛选，并生成结构化的评审报告；利用OCR和NLP技术，自动从扫描件或电子文档中提取关键字段（如：公司名称、注册资本、经营范围、证书有效期、关键财务指标、法律纠纷、风险信息等）；支持根据预设的评审规则对提取的信息进行自动比对和判断，输出结构化的评审报告，报告中需高亮显示不满足项、潜在风险项或关键信息的缺失项，评审结果可通过OA系统以富文本HTML形式展示。 |
|  | **采购合同评审：**对采购合同草案进行自动化分析，与公司标准合同模板和法务风险点进行比对，识别招标技术文件要求并提示潜在的法律和商务风险；能够精准识别并提取合同文本中的核心要素，包括但不限于：合同双方主体、标的物、价格与支付条款、交付期限、违约责任、争议解决方式等；系统需内置公司法务部门定义的风险点清单，对合同条款逐一进行合规性检查和风险评估；必须生成清晰的评审意见，其中应明确列出高、中、低不同等级的风险条款，并尽可能提供相应的修改建议。自动提炼、归集已审批合同信息并进行统一记录。 |
|  | **投标文件评审：**通过对比招标文件及投标文件，智能分析投标方案满足情况，根据评分规则自动为投标文件打分并给出得分/扣分依据，为评标提供AI辅助。 |
|  | 产品维保 | ★提供不少于一年的免费技术支持和模型优化服务（自整体项目验收合格之日起计算）。并出具的售后服务承诺函（加盖投标人公章）。 |
|  | 部署要求 | **部署方式：**部署于公司提供的服务器，数据不得出公司内网。 |

1. 专业级图形处理器（GPU）

| **序号** | **技术指标** | **技术参数及指标** |
| --- | --- | --- |
|  | 服务要求 | ★**型号：**NVIDIA RTX A6000 或性能更优的同等品牌。 |
|  | ★**显存：**不低于 48GB GDDR6。 |
|  | ★**核心：**CUDA 核心≥10752，Tensor 核心≥336，RT 核心≥84。 |
|  | **接口：**支持 PCIe 4.0 x16 或更高版本。 |
|  | **原厂正品：**全新原装，提供可追溯序列号及官方验证方式。 |
|  | **安装服务：**负责 GPU 安装、驱动部署及调试，确保稳定运行。 |
|  | ★**保修服务：**不少于三年保修，自终验合格之日起计算。 |

1. 与现场在用的其他供货商供应的系统和设备协调、接口的工作要求。
* 本项目需与公司OA系统（蓝凌OA）中的规范制度模块及采购评标系统进行集成对接。所有与接口、协调相关的工作及由此产生的费用均由中标供应商负责，并通过与相关方协商解决，确保系统稳定、兼容运行。
* 专业级图形处理器（GPU）安装在公司DELL Precision 7960 Tower服务器上，确保系统稳定、兼容运行。

5．维修服务要求

 专业级图形处理器（GPU）免费质保三年。

6.技术服务要求

 软件开发服务免费技术支撑一年。

7. 技术方案要求

投标人应根据招标文件要求，提交可实施性强、结构完整的技术方案，内容应至少包括：

1. 项目总体设计
* 对项目目标、范围和关键功能的理解。
* 系统总体架构、硬件架构、网络拓扑、部署模式。
* 技术路线选择及所用模型的理由。
1. 功能实现方案
* 针对五个核心业务功能的实现思路、关键技术及预期效果。
* 知识库构建流程（采集、清洗、分段、嵌入、检索）。
* 智能体流程编排及集成方案。
1. 系统集成
* 与 OA 系统的集成方式（流程衔接、数据回写）。
1. 性能与安全保障
* 确保满足性能指标的技术措施。
* 数据安全保障（访问控制、加密、日志、防攻击）。
1. 硬件配置与部署
* GPU 硬件选型依据及性能说明。
* 安装部署方案。
1. 实施计划与进度
* 阶段划分、关键任务、里程碑、交付物及时间表。
1. 培训与技术支持
* 培训计划（用户及管理员）。
* 售后支持及质保服务方案。
1. 风险分析与应对
* 可能风险（技术、数据、安全、进度）。
* 风险预防与应急措施。

8. 其他要求

**五．工程服务**

1．施工区域安全要求（防火防爆、防尘防水、连续生产、连锁保护等要求）

2. 施工安全方案要求

3．昆纤安全要求: 详见附件。

1. 项目施工时施工单位除严格执行国家相关安全规范外，还应严格遵守执行但不限于昆纤安全管理制度及《现场施工检查、监护表》《移动电器检查（监护）表》及《临时用电申请表》《昆纤公司项目隐蔽工程随工验收单》的安全要求。施工单位应指定安全员进行监督，并每周进行不少于1次检查填写《现场施工检查、监护表》上报项目负责人。
2. 如果乙方违反施工安全方案、操作规程或违反甲方防火、防静电及其它厂纪厂规，将视为违反《承包商环境、健康、安全协议》。
3. 报价时注意：施工中涉及搭拆脚手架工程的，脚手架需选用昆纤提供的承插型盘扣式钢管支架（含钢管、扣件、钢跳板等），乙方报价时只报搭设和拆除的人工费及安全网等费用（安全网由乙方提供）、否则在报价预算书审核时，由昆纤扣减。

4．项目实施进度要求（设备材料供货进度、施工进度、施工工期时间要求）

1. 项目对设备材料供货进度、施工进度、施工工期、施工时间点要求。

项目实施期限： 90天

1. 签订合同后，中标方需在3个工作日内编制满足招标文件要求的《施工进度计划表》《施工安全方案》提交项目负责人。

**六．调试及验收**

1．系统调试要求

中标人需指派具有相关AI项目经验的资深工程师负责硬件安装、软件部署和系统联调，确保智能体在招标方环境中顺利运行。

2．验收要求、检查内容

项目验收分为两个阶段：初验和终验。在项目实施完毕后，硬件安装到位，五个智能体基本功能按技术要求上线运行，即可进行初验;系统在初验后，无故障试运行1个月，期间业务部门使用顺畅，各项功能稳定、准确，满足业务需求，即可组织终验。中标人在终验前提交所有项目交付文档。验收过程中出现不符合标书和合同要求的严重质量问题时，招标人保留索赔权利。

3．质保期及故障响应时间

 质保保期7X24小时响应，现场或远程技术支持。

**七．资料及培训**

1．项目需交付的图纸、资料、\*证书、报告的数量和方式

本项目需在终验前一次性交付系统部署拓扑图、功能架构图、业务流程图等设计图纸，系统设计说明书、开发文档、源代码、用户与管理员手册、知识库调优策略等资料，硬件原厂合格证、质保证书、CCC 认证等证书，以及系统测试报告、GPU 安装调试报告、培训报告、项目验收报告等文件，纸质文件须加盖公章，电子版需提供 PDF 和可编辑源文件，并通过加密介质提交至招标方指定部门备案。

2．培训时间、地点、人数要求

 中标人需为招标方提供至少一次技术培训，内容包括：智能体日常使用操作、后台知识库更新与管理、系统基本维护等。

**八．技术专有权**

本项目中开发的所有智能体软件系统、代码及相关知识产权，均归昆明醋酸纤维有限公司所有。

投标人所提供的产品涉及的专有或专利技术，甲方认为知识产权使用费已经包括在投标总价中，甲方不会因为任何理由而单独支付额外的费用。

**九．保密协议**

实施方在项目过程中接触到的所有招标方业务数据、文档和资料，必须严格保密，不得以任何形式泄露、拷贝或用作本项目之外的任何目的，项目实施前须签署保密协议。

**十．其他要求（施工资质、授权等要求）**

**附件一：**

承包商入厂基本安全要求：

一、承包商PPE要求

1. 穿着符合施工区域要求的工作服，如防静电、防酸碱、防烫、防尘等；
2. 穿着符合施工区域安全要求的劳保鞋，如防静电鞋、绝缘鞋等，劳保鞋需具有防砸、防穿刺功能；
3. 佩戴符合国家标准的安全帽；
4. 根据项目风险识别，配备防冲击眼镜、防护面罩、防尘口罩、防有机气体口罩、劳保手套、五点式安全带、防坠器等；

二、承包商行为要求

1. 严禁游动吸烟；
2. 严禁在防火防爆区内使用非防爆手机及非防爆电气设备；
3. 严禁进入与工作无关的区域或房间；
4. 严禁触碰或操作与工作无关的设备和设施；
5. 严禁在施工现场就餐、睡觉或做其它与工作无关的事；
6. 严禁用饮料瓶盛装化学品带入工作现场；
7. 带入公司的电动工器具均需要维修保障部对应的专业工程师进行检查，并张贴合格标识。
8. 承包商在昆纤公司工作，工作时长为工作日8:30—17:00，如需要加班，需得到昆纤公司工作联系人/项目负责人的许可。如周末需要加班，需得到安环部的许可。
9. 承包商进入昆纤公司工作的人员，年龄需符合《劳动法》相关要求，并且需全员购买意外伤害险。

三、项目作业要求

1. 承包商人员需接受昆纤公司三级安全培训教育，经考核合格后，方可开展工作；
2. 承包商在开工前，必须识别作业风险，遵守昆纤公司《工作许可及危险作业管理制度》，动火、有限空间、登高、吊装、临时用电和带电作业等，须办理相关作业许可证。
3. 涉及电焊、登高、架设、电气（含临时用电）等作业时，作业人员需持有应急管理局颁发的特种作业许可证，并在有效期内。
4. 施工区域须设置红白危险警示带；
5. 施工现场工具材料分类堆放整齐，并设置黄黑警戒线；
6. 承包商专职或兼职安全员必须穿着橘红色（动火作业监护）或黄色（有限作业、登高作业监护）的反光背心，不得离开工作现场。专职安全员不得参与施工工作；
7. 施工废物和垃圾按昆纤公司规定及时进行处理；