合同编号：豫财磋商采购-2024-1348包2

郑州大学信息化办公室、网络管理中心采购数据治理深化提升建设项目采购合同

甲方（全称）： 郑州大学

乙方（全称）： 郑州顺腾科技有限公司

根据《中华人民共和国民法典》《中华人民共和国政府采购法》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，双方就郑州大学信息化办公室、网络管理中心采购数据治理深化提升建设项目采购项目及有关事项协商一致，同意按照下述条款订立本合同，共同信守。

一、 供货内容及分项价格表

1、 本合同所指供货内容详见附件1，此附件是合同中不可分割的部分。

2、 本合同总价款为人民币（大写）肆拾柒万玖仟元整（¥479000元），供货内容的分项价格表详见附件2，此附件是合同中不可分割的部分。合同总价中包括软件购置费（含授权费）、开发服务费、安装部署费、调试费、各类检测费、运行维护费及培训所需费用及税金，甲方不再另行支付任何费用。

二、服务约定

1、 交货时间： 自合同签订之日起30个日历天 。

2、 交货地点： 采购人指定地点 。

3、 交货方式： 现场服务 。

三、质量要求或服务标准，乙方对质量负责的条件和期限

1、 基本要求

(1) 甲乙双方在签订合同的同时，须与项目建设部门签订《郑州大学信息系统建设网络安全责任协议》（附件 3）和《郑州大学信息系统建设信息安全保密协议》（附件 4）。

(2) 乙方须按合同要求提供符合招标标书要求的产品，且应达到乙方投标文件及澄清文件中明确的技术标准。甲方如果发现乙方所供产品不符合合同约定，甲方有权单方解除合同，由此产生的一切后果由乙方承担。

(3) 乙方负责在项目完成后将项目实施所涉及的全部相关技术文件资料（包括但不限于信息标准集、需求说明书、数据表结构、系统详细部署文档、本项目实施中产生的所有开发源代码、全部接口技术文档、后期应用系统相关接口等），以及系统测试、验收报告和系统测试使用的测试数据等文档汇集成册提交给甲方，并提供所有资料的电子文档；同时，提供本项目所有软件产品和数据资源的电子文件。

(4) 乙方负责在项目完成后对甲方人员进行免费的系统运维、二次开发等涉及项目后续发展的有关技术培训。

(5) 乙方应提供完整的项目实施计划、详细的工作内容安排及过程控制和验收方案等。

(6) 乙方应保证甲方在使用其所提供的产品时免受第三方提出侵犯其专利权、商标权或保护期的起诉。

(7) 本项目中甲方定制开发部分，其软件著作权归甲方所有。

(8) 其他：

2、 项目人员配置

(1) 乙方应针对本项目成立由项目经理带队的不低于 3 人的项目团队，其中实施期驻场人员不应少于 1 人，并建立保障本项目顺利实施的各项管理制度和质量保证体系。为了保证项目实施的连续性，项目实施过程中应至少保证 1 名以上核心技术人员不能更换。

(2) 乙方应在项目实施方案中提供项目组成员名单，并详细描述项目组成员的技术能力、项目履历、工作职责和具体工作内容等。

(3) 其他：

3、 进度要求

乙方应针对本项目提交项目实施计划，经甲方确认后严格按计划执行，并按计划要求交付产品和成果。如需变更必须提出书面的实施计划变更手续。

4、 开发管理

乙方应对项目实施进行科学严格的管理，能够对项目进行系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施。

5、 文档管理

乙方应根据开发进度及时提供有关开发文档，包括但不限于需求说明书、系统设计说明书、测试计划、测试分析报告、系统部署手册、操作手册、系统安装手册等。

6、 用户培训

乙方对甲方人员的培训应贯穿于整个项目的实施过程中，包括从项目准备、研发到项目运行维护和使用的全过程。乙方提供详细的培训方案、培训内容、培训计划、人员数目、开发工具、软件使用和后期维护等。

(1) 培训内容

1) 乙方应对甲方人员进行系统的研发管理培训，即项目开发的各阶段技术培训，具体包括但不限于项目准备、用户需求分析、系统概要设计、系统详细设计、程序编制和运行建立等。

2) 乙方应对甲方人员进行系统的技术培训，使甲方人员能掌握项目相关系统的使用、维护和管理方法，能独立进行系统使用、管理、故障处理、日常测试和维护等工作，以保证所建设的系统能够正常、安全、平稳地运行。

(2) 培训要求

1) 培训教师应具有丰富的应用实践经验和教学经验，中文授课。

2) 乙方提供培训使用的文字资料和讲义等相关材料。

3) 如果培训地点在外地，乙方应向甲方承诺为所有培训人员提供食宿。

(3) 培训方式

乙方根据培训内容提供不限于课堂讲解、实际操作、专题交流、现场实施指导等培训方式。

7、 产品运行支持与服务保证

质量保证期内乙方提供免费上门服务，服务内容包括但不限于软件系统和数据资源的维护、优化、升级、服务响应、使用培训等。质量保证期内，自接到甲方的故障报修后，乙方2小时内派遣专业技术人员到达故障现场，技术人员在24小时内解决问题，直至软件系统正常运行及相关资源正常使用。

四、**验收标准、方法**

1、含有定制开发内容的专用类软件验收标准和方法

（1）软件产品已经完整地部署在甲方提供的指定服务器资源上，配置学校内网测试IP地址，使用安全合规的测试数据，并在此运行环境上进行信息系统的功能测试、性能测试、安全测试等工作。

（2）功能测试。乙方提交软件产品的功能测试报告，并对功能测试报告的真实性承担责任。乙方依据软件产品开发需求、设计文档、采购时的技术参数要求并结合功能测试用例等完成软件产品的功能测试，形成功能测试报告。

（3）性能测试。乙方提交软件产品的性能测试报告，并对性能测试报告的真实性承担责任。乙方依据软件产品开发需求、设计文档、采购时的技术参数要求，在用户量、数据量的超负荷下，对软件运行时的相关数据进行分析测试，形成性能测试报告。

（4）代码安全审计。乙方提交软件产品完整的、真实的、功能一致的源代码并进行代码安全审计。如因特殊原因无法提供源代码并经甲方同意的，由乙方委托具有中国计量认证（CMA)或中国合格评定国家委员会（CNAS)认可实验室证书等资质的第三方软件代码测评机构出具的代码审计合格报告。报告中的软件源代码要和实际部署的软件产品完全一致。

（5）安全风险评估。1）乙方提交委托具有中国信息安全测评中心颁发的信息安全服务资质（风险评估类）或中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质的第三方测评机构出具的渗透测试报告；2）乙方提交由甲方网络管理中心出具的安全基线配置核查报告和系统漏洞扫描报告。

（6）其他验收文档。乙方提交软件产品包括需求分析文档、系统设计文档、接口技术文档、数据字典文档、配置文档、运行维护文档和用户使用指南等相关验收资料。

2、成品通用类软件（例如操作系统、办公软件、数据库、防病毒软件、开发工具类软件等）的验收标准和方法

（1）由乙方提供相应软件产品的安全合格报告或证书。

（2）由乙方提供相应软件产品的安装配置文档、运行维护文档和用户使用指南等相关验收资料。

五、结算方式及期限

根据本项目的具体情况，经甲乙双方协商后，结算费用按照阶段进行相应的比例支付，具体如下：

验收合格并经审计后，甲方向乙方支付合同总价款的70%，即人民币（大写）<u>叁拾叁</u>

万伍仟叁佰元整（¥ 335300 ）；质保期内，甲方对乙方所提供服务的质量进行阶段评价，合格后支付合同总价款的 25%；质保期满，乙方服务质量合格，甲方向乙方支付剩余 5%的货款。

六、免费质保约定

1、 免费质量保证期为自项目验收合格之日起 三 年，质量保证期内乙方提供免费上门服务和 7×24 小时全年无休电话服务，服务内容包括但不限于软件系统和数据资源的维护、优化、升级、服务响应、使用培训等。

2、 质量保证期内乙方对产品提供 7×24 小时全年无休的安全运维监测和告警服务，并提供专业的解决方案建议。乙方每月进行一次安全检测和病毒扫描，及时调整安全策略和安全规划，备份重要数据，升级系统和安装补丁等。

3、 其他：

七、售后服务承诺（包括服务的内容、方式、响应的时间、电话、质保期满结束后的维保等相关内容）

1、服务内容

1） 乙方承诺提供原厂商 三 年（不少于三年）的免费质保。质保期自项目验收合格之日起开始计算。

2） 乙方承诺在质保期内免费提供产品的运维、优化、升级以及非模块级的功能需求变更、部署结构变化等服务。

3） 乙方承诺对于本项目中存在的 Bug、缺陷、安全风险隐患等，在质保期内外均提供持续的修补和消除服务。

4） 乙方承诺根据甲方所有业务系统的需求和运作规律，有针对性地制定项目系统平台的运维和售后服务保障方案，建立完善的售后服务体系。

5） 乙方承诺在售后服务过程中提供完善的文档记录，包括故障处理报告、健康巡检报告、系统性能检测调优报告、系统安全检测报告、服务年度报告等。

6） 乙方承诺提供故障分级响应机制，按照售后服务计划和质量保证承诺向甲方提供优质的技术支持服务。

2、响应方式和响应时间

故障级别	响应时间	技术人员到场时间	解决时间

I 级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失、网络安全事件和安全隐患。	7*24 小时 实时响应	2 小时内到达现场	3 小时
II 级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。	7*24 小时 实时响应	2 小时内到达现场	8 小时
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但系统能继续运行且性能不受影响。	7*24 小时 实时响应	2 小时内到达现场	12 小时
IV级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	7*24 小时 实时响应	2 小时内到达现场	即时

3、响应电话：

许奔 18530979067

4、质保期外服务：

乙方承诺提供质保期外的 有偿 服务，所提供服务与质保期内服务相同，并承担同样的责任与义务。质保期外服务须另行签订合同。

八、履约担保

履约担保金额为合同总额的 5%。

履约担保方式：承包人以银行转账或银行保函方式在合同签订前向发包人提供履约担保，验收合格，正式交付使用后退还。

九、违约责任

1、乙方违约：乙方提供的服务内容不符合约定的质量要求，甲方有权解除或终止合同，并要求乙方按合同总价款的 5%支付违约金，给甲方造成经济损失的，乙方还应如数赔偿；乙方未按约定期限交付投标物，每迟延一天须按合同总价款的 5‰向甲方支付违约金。因为乙方原因造成合同迟延履行的，甲方有权解除或终止，并且要求乙方赔偿由此造成的经济损失。

2、甲方违约：甲方未能按双方约定的方式和期限支付货款，按有关规定承担违约责任。

十、其他

1、组成本合同的文件及解释顺序为：投标书（响应文件）及其附件、本合同及补充条款；招标文件（采购文件）及补充通知；中标（成交）通知书；国家、行业或企业（以最高的为准）标准、规范及有关技术文件。

2、双方在执行合同时产生纠纷，协商解决，协商不成，向甲方所在地人民法院提起诉讼。

3、本合同未尽事宜，由甲乙双方协商后签订补充协议，与本合同具有同等法律效力。

4、本合同共 19 页，一式 九 份，甲乙双方各 四 份，招标代理公司 一 份。

5、本合同由双方签字盖章后生效，合同签署之日起至合同内容执行完毕为本合同有效期。

甲方（盖章）：

法定代表人或授权代表：

单位地址：郑州市高新区科学大道 100 号

电话：0371-67781505

开户银行：工商银行郑州中苑名都支行

户名：郑州大学

账号：1702021109014403854

签订日期：

审核：李润东

签约地点：郑州

乙方（盖章）：郑州顺腾科技有限公司

法定代表人或授权代表：王慧杰

单位地址：河南省郑州市金水区东风路街道天明路 86 号凯瑞大厦 5 层 510 号

电话：17634835686

开户银行：中国银行股份有限公司郑州银基王朝支行

户名：郑州顺腾科技有限公司

账号：91410105MA3X6A2N3J

签订日期：2025.1.2

附件 1：

供货内容、技术规格参数及主要功能性能描述

序号	供货内容类别	子系统/功能模块名称	具体技术规格参数、主要功能、性能及配置描述	单位	数量
1	数据分类分级	数据安全分类分级服务	1、满足总体要求：调研学校数据中台涉及重要系统的业务条线，梳理业务部门对应的关键业务流程以及业务活动，分析各业务流程涉及的关键敏感数据。提供本次项目数据安全分类分级与服务所需软件工具平台，含数据源资产管理、分类分级管理、数据库安全评估、系统数据安全管理、API 接口、数据安全展示等。完成交付数据安全分类分级规范的制订，交付《数据安全分类分级指南》《数据安全分类分级管控策略》《数据安全分类分级逻辑框架》《数据资产分类分级清单表》。	项	1
			2、满足基于当前已有的数据中台系统数据分类基础，进行全面多维度的数据安全现状调研，包括不限于合规要求、业务部门、数据资产、业务流程、技术工具、控制措施等多个方面。		
			3、满足收集数据中台涉及重要系统产生、采集、加工、使用或管理的数据，对数据进行明确的定义，并根据数据安全分类分级方法对数据进行分类分级并标识，建立数据资产分类分级清单。		
			4、满足根据国家以及教育行业数据安全标准和法律法规要求，依据《GB/T43697-2024 数据安全技术数据分类分级规则》《教育系统数据分类分级工作指南（征求意见稿）》《JY/T1002-2012 教育管理信息教育管理基础信息》中给出的模板进行数据分类分级标识服务。		
			5、满足支持依据对数据安全分类分级服务结果的人工校验，归纳提取识别规则，将新的识别规则或优化后的识别规则配置到相应分类分级清单表；优化调整数据分类分级逻辑框架，扩展至学校分类分级模板规则。		
		AI 大模型服务	1、满足提供一套 AI 安全垂直领域大模型系统，用于数据分类分级的实施，使用期限：项目交付验收阶段结束三个月内。基于数据的保密性考虑，需提供硬盘不返还服务。		
			2、系统性能满足推理速度不低于 30 字符/s，支持打字机模式输出，在模拟真实场景的输入和输出情况下，同时处理的请求数不低于 20 个。支持不少于 5 万字上下文的总结。		

			3、大模型满足支持 PEFT（Parameter-Efficient Fine-Tuning）参数微调；支持多个 LoRa 任务的在多个 GPU 卡上的并行推理。支持自定义敏感词，支持拦截试图诱导模型生成敏感内容的恶意问题，支持实时过滤模型输出内容并撤回敏感回答，支持用户限流（并发数和 Token 数）。		
			4、支持对于缺少字段中文注释和表注释的字段内容，利用大模型的核心推理能力，进行字段内容推测和分类分级打标。		
			5、结构化数据分类分级支持同表多级上下文推理纠偏，形成最终的分类分级结论，结论包含判断依据、分类结果、分级结果、字段解释。		
			6、满足所提供服务的安全垂域大模型具备自主知识产权证明以及大模型安全性测评。		
		数据安全分级及风险管理系统平台	1、支持数据库类型包括但不限于 MySQL、Oracle、PostgreSQL、UXDB、MSSQL、MariaDB、Informix、Sybase、DM、DB2、GBase、CacheDB、KingBase、Oscar、Oceanbase、GoldenDB、TiDB、MyCat、DBLE、DRDS、Hive、Inceptor、Impala、MongoDB、Elasticsearch、ClickHouse、GreenPlum、Hbase、ODPS、PolarDB、TeraData、Vertica、Gauss100、Gauss200、HANA 等。		
			2、支持通过 FTP/SFTP/LOCAL 文件协议对 csv、txt 等文件进行分类分级。支持对于已经创建的数据源上传其对应的数据字典信息，用于对表注释及字段注释进行补充。		
			3、支持对于数据源中所包含的数据质量进行评估，评估指标包含：字段总数、字段注释存在数、有含义的字段注释数、有含义的字段注释去重数、表总数、表注释存在数、有含义的表注释数、有含义的表注释去重数。		
			4、支持通过联动数据库审计设备，解析被审计语句中的数据库资产信息，实现数据库资产的被动发现。		
			5、支持以库、表、列方式对于数据资产目录进行可视化展示，数据表资产信息包含：数据源、主机、库名、Schema、行业模版、分类、分级、是否梳理、业务系统、部门、责任人、最后梳理时间、字段数、敏感字段数、已梳理占比，数据字段资产信息包含：字段名、字段注释、类型、规则名称、分类、分级、是否敏感、是否梳理、最后梳理时间、查看样本数据。		
			6、可对于结构化分类分级任务进行相关配置，包括：数据源、抽样策略、执行逻辑、打标方式，其中执行逻辑中包含分类分级规则匹配规则、分类分级模		

			型分析、分类分级框架解析，打标方式包含：推荐列模式和推荐表模式。		
			7、支持结构化分类分级任务流程化执行向导，包括：分类分级预测、人工校验打标、结果自动纠错三个环节。其中分类分级打标环节可自动推荐需要打标数据，并可手动进行打标。打标纠错环节可自动推荐可能存在分类分级打标错误的结果，并可对于结果进行修正。		
			8、支持对相似表、相似字段进行聚合并在页面中统一展示，以便于人工二次确认或修改分类分级结果，提供“梳理向导”功能提高人工效能。		
			9、支持数据分类分级的标准化项目管理流程，涵盖任务分配、数据打标、结果审核、结果验收、结果发布等环节。		
			10、支持通过调用大模型（LLM）能力，提升分类识别率与准确率，并给出大模型输出结果的“识别说明”帮助人工更好地判断其结果是否准确。同时，支持以自然语言方式输入专家经验，以对于大模型的识别效果进行调优。		
			11、满足提供数据安全分类分级可视化，包含数据源数、表数、列数、已梳理列数、列梳理率、数据源风险评分 TOP、数据源弱密码风险数 TOP、数据源基线风险数 TOP、数据分级分布、数据源敏感列数 TOP 和数据分类分布情况等信息。		
			12、数据安全分级及风险管理系统工具软硬件配置：支持 100W 数据库列数，CPU12 核 24 线程*2，内存 128G ，硬盘容量 8T*4 带 RAID5，千兆 RJ45 网口*2（管理口*2）、千兆 RJ45 网口*4、万兆业务 SFP+光口*2；满足系统工具部署学校，永久使用，3 年软硬件质保；		
		数据共享与对接安全检测系统	1、支持与学校数据治理平台数据共享与对接，实现数据资源的分类、分级，实现数据资源不同安全等级、不同形态的校内共享。		
			2、提供 RPA 流程自动化技术服务工具，工具软件配置要求 CPU10 核 20 线程*2，内存 128GB，硬盘 4T*2；满足系统工具部署学校，3 年质保期内永久使用；		
			3、RPA 技术服务工具支持以非侵入式实现与学校相关系统的数据交互，按照预设的规则和流程自动执行繁琐重复的任务，不需要人为干预，减少人为因素对数据安全的影响；在数据对接和共享过程中不泄露业务数据，提升组织数据协同能力的同时保障数据安全性。		

			4、RPA 技术服务工具支持通过设定能够对数据的共享访问和处理进行跟踪和监控，以及时发现异常行为和安全风险，并采取相应的措施，防止未经授权的访问和操作，保障数据安全。		
2	数据安全风险评估	数据安全风险评估服务	1、满足梳理学校数据中台涉及重要系统内外部 API 使用情况，基于 OWASP API Security Top 10 的安全风险进行检测发现，评估该系统数据通过 API 造成数据泄露的情况，分析原因并提供加固建议。	项	1
			2、满足基于国家《数据安全法》《个人信息保护法》《GB/T 43697-2024 数据安全技术数据分类分级规则》等法规标准，针对学校数据安全治理现状进行调研，评估调研着重于合规要求、数据资产总体情况（各业务流程涉及的关键敏感数据）、数据相关业务总体情况、数据涉及部门总体情况、数据安全技术能力总体情况、数据安全管理支撑总体情况。		
			3、以模拟黑客入侵的方式对目标场景进行模拟入侵测试，结合测试结果与典型数据流图，形成重要场景下的敏感数据威胁风险图。		
			4、基于项目实施范围，明确数据中台涉及重要系统典型业务场景覆盖的重要业务系统，系统数据安全现状评估调研着重于系统本身的数据安全管理现状、部署位置、系统数据安全情况、数据安全防护能力等。		
			5、针对 Github 上可能泄露在外的数据中台涉及重要系统的邮件配置信息、数据库配置信息、FTP 配置信息、SVN 配置信息等等系统敏感数据进行识别发现，以及对百度网盘、百度文库、csdn 等互联网侧重点区域进行敏感数据发现及暴露面识别。		
			6、针对暗网中出现的数据信息或者交易信息进行实时搜集分析,全面搜集并监控暗网中出现的我校数据中台涉及重要系统相关的新增泄露的个人信息数据、业务数据等。		
			7、围绕重点业务场景，以重点业务场景的重点功能模块、数据集及 IT 资源环境实体为主体，识别业务流程中涉及的关键敏感数据，确认关键敏感数据集的全生命周期流向，梳理输出系统业务逻辑、系统功能模块间的数据流向关系。		
			8、基于典型数据流图，梳理场景下敏感数据的数据处理活动，从数据梳理活动出发，基于数据处理活动进一步完善数据流图，并作为数据安全风险评估基线的输入。数据处理活动的梳理包括各采集、传输、存储、使用等活动阶段的梳理。		

			9、围绕数据处理活动、资产维度，从数据安全建设要求角度，建立数据安全风险评估基线，形成针对重要场景、典型数据流程下的数据安全风险评估渗透要点。		
			10、依据《数据安全风险评估基线》进行数据安全测试，以验证相关业务场景的数据安全性；实施过程需结合智能扫描、数据分类分级、AI 大模型等工具，并结合人工测试、分析等手段。		
			11、结合评估发现的数据安全风险，明确所面临的各类数据安全问题严重程度，选取数据安全保护最佳实践，针对具体问题提出具体整改建议。		
			12、根据评估结果及安全分析结论编制评估报告，对评估内容、过程、结果、问题等进行总结和分析，并给出总体评估结论。		
			13、满足质保期 3 年内每年不少于 2 次数据安全风险评估服务，投标人具备风险评估相关资质要求，每次不少于 1 人驻校现场服务 30 天；		
			14、交付物：《数据安全合规评估基线》《数据安全合规现状调研表》《数据安全合规评估表》《数据安全合规优化提升方案》《数据安全合规评估报告》。		
		数据库安全评估服务	1、提供数据库脆弱性检查服务，脆弱性检查至少包括数据库漏洞检查、配置项检查、弱口令检查等手段实现安全评估，并提供图表分析结果和数据源安全排名，实现对数据库状况的安全监控和评估。		
			2、提供账号权限发现服务，至少包括但不限于数据库账号、数据源名称、拥有权限、禁止权限、状态和密码有效期等信息，同时支持检测账号动态变化和权限变更。		
			3、提供数据库漏洞库，提供风险检测的数据库漏洞检测，至少包括但不限于漏洞名称、CVE 编号、漏洞等级、漏洞描述、解决建议、数据库类型、数据库版本、操作等信息。		
			4、提供数据库的自动发现工具服务；支持大 B 段、跨网段 IP 扫描；支持指定端口范围扫描。支持 20 余种数据类型资产的发现识别；包含常见的 mysql、Oracle、DB2、kingbase 等数据库类型。		
			5、提供数据库检测服务；可提供 T1-T5 五种检测参数。提供最小并发数、最小 IP 检测数、检测超时时间设置项。		

		数据安全评估系统平台	1、提供统一数据安全评估工具集系统，配置 CPU 8 核 16 线程；内存 64G；磁盘 1T-SSD；满足系统工具部署学校，永久使用，3 年软硬件质保；覆盖包括数据资产识别、敏感数据发现、数据接口风险监测（API）、Linux 主机配置检测、Windows 主机配置检测、弱口令安全检测、系统漏洞检测及 WEB 应用安全检测等检查工具，以自动化的方式快速完成检查指标的符合性判定。重点支持数据载体的弱点扫描。		
			2、支持工具管理和任务下发，支持对检查过程中动态的添加检查对象，例如：数据库、应用系统、服务器和终端等，可以选择已有的检查对象或录入新的检查对象。		
			3、支持数据安全检测评估项统一设置：情况问询、资产调查、现场检查、检查报告。从被检单位基础情况获取到资产摸底，再到模板调查及技术检查，并输出多维度检查报告。		
			4、支持对已检查的数据评估模板进行评分，根据实际检查结果给予相关分数，体现该类检查模板综合符合情况，映射在该类检查模块下的风险情况。		
			5、支持对所有的数据安全评估检查任务进行结果的分析，包括符合项、不符合项、部分符合项以及不适用项等的结果统计以及此次检查任务的结果得分，最终出具具有标准性和普适性的检查报告。		
			6、数据接口行为风险识别，支持通过多种指标自定义新增风险策略，例如：访问次数、访问时间、访问敏感数据等、上传下载文件、访问账号等。支持对点滴泄漏行为、慢速爬取行为进行监测，以 IP、账号、IP 应用、账号应用纬度进行风险监测。		
			7、支持以数据为维度进行风险监测，以数据为线索关联分析相关 API、相关应用、相关主体等内容，可适用于洞察二次封装风险场景。		

附件 2：

供货内容及分项价格表

单位：元

序号	供货内容类别	子系统/功能模块名称	产品名称及型号	制造厂（商）	单位	数量	单价	合价	质保期	备注
1	数据分类分级	数据安全分类分级服务	数据安全分类分级服务（亚信安全定制）	亚信科技（成都）有限公司	项	1	86000	86000	3 年	含税
		AI 大模型服务	AI 大模型服务	亚信科技（成都）有限公司	项	1	65037	65037	3 年	含税
		数据安全分级及风险管理系统平台	数据安全分级及风险管理系统平台 AISDC v1.0	亚信科技（成都）有限公司	套	1	54000	54000	3 年	含税
		数据共享与对接安全检测系统	数据共享与对接安全检测系统（亚信安全定制）	亚信科技（成都）有限公司	套	1	30000	30000	3 年	含税
2	数据安全风险评估	数据安全风险评估服务	数据安全风险评估服务（亚信安全定制）	亚信科技（成都）有限公司	项	1	100663	100663	3 年	含税
		数据库安全评估服务	数据库安全评估服务（亚信安全定制）	亚信科技（成都）有限公司	项	1	50000	50000	3 年	含税
		数据安全评估系统平台	数据安全评估系统平台 AIS VP V3.0	亚信科技（成都）有限公司	套	1	93300	93300	3 年	含税

供应商：郑州顺腾科技有限公司（盖章）

法定代表人或委托代理人：王慧杰（签字或盖章）

附件 3：

郑州大学信息系统建设网络安全责任协议

甲方： 郑州大学

乙方： 郑州顺腾科技有限公司

甲、乙双方现就 郑州大学信息化办公室、网络管理中心采购数据治理深化提升建设项目 （以下简称“项目”）进行建设合作。根据《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》等相关法律法规和《信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）》《信息安全技术 个人信息安全规范（GB/T 35273-2020）》等相关国家标准，本着平等、自愿、公平、诚信的原则，经双方协商一致，就该项目实施及后续合作过程中的网络信息安全责任事项达成本协议。

第一条 乙方严格遵守《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》等相关法律法规和国家相关标准的要求，执行郑州大学网络安全管理相关规定和办法。

第二条 乙方承诺在项目调研、开发、管理、实施、运维、售后服务及后续合作过程中，承担相应的网络信息安全责任。

第三条 乙方不得在其提供的软件产品中留有或设置漏洞、后门、木马等恶意程序和功能；如果发现其软件产品存在安全风险时，应当及时告知甲方，并立即采取补救措施。

第四条 乙方应采取技术措施和其他必要措施，保障所提供软件产品的自身安全和稳定运行，有效应对网络安全攻击，保护数据的完整性、保密性和可用性。如因软件产品自身安全问题造成的一切责任和后果（包括法律、经济等）由乙方全部承担。

第五条 乙方应当为其软件产品运行所依赖的操作系统、数据库系统、中间件、开发框架、第三方组件、容器等持续提供安全维护，并承担相应的安全责任；在合同约定的质保期内外，均不得终止提供安全维护。

第六条 如果软件产品涉及密码技术的应用，应确保密码的使用符合国家密码主管部门的相关要求。

第七条 软件产品具有收集用户信息功能的，乙方应当提前征得甲方同意；涉及用户个人敏感信息的，还应当遵守《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》等法律法规和国家标准的相关规定。

第八条 乙方应根据信息系统数据的重要性和系统运行需要，制定数据的备份和恢复策略

与程序等。

第九条 软件产品应对以下活动进行日志记录，包括权限管理日志、账户管理日志、登录认证日志、业务访问日志、数据访问日志等；提供新闻、出版以及电子公告等服务的软件产品，还应记录并留存用户注册信息和发布信息审计功能；所有日志记录留存应至少保存 60（）天记录备份。

第十条 乙方应制定针对信息系统的网络与信息安全管理制度，对安全策略、账号管理、密码策略、配置管理、日志管理、日常操作、升级与补丁修复等方面做出规定。

第十一条 乙方应制定针对信息系统的网络安全事件应急预案，包括预案启动条件、应急处置流程、系统恢复流程等，并定期对应急预案进行评估和修订完善。

第十二条 乙方应对其工作人员的技术行为承担责任，包括：（1）不得在甲方服务器上安装各类与项目建设、运行、维护无关的软件；（2）必须按照甲方提供的安全方式进行信息系统及其运行环境的访问，并向甲方报备访问的 IP 地址；（3）在软件产品上线运行后，未经甲方允许，乙方不得对信息系统及其运行环境进行任何操作；（4）做好所属账号管理工作，防止账号泄露、侵入等事件的发生；（5）履行甲方规定的安全责任相关要求；（6）因乙方工作人员造成的损失由乙方承担相关责任。

第十三条 乙方应对软件产品的安全检测、应急响应和安全事件处置承担责任，包括：（1）对软件产品及其运行环境进行定期性的安全检测，并将结果以书面形式报告给甲方；（2）软件产品及其运行环境被检测出或发生安全问题时，乙方须在 1 小时内做出应急响应，并在 24 小时内完成应急处置，防止损失的进一步扩大。

第十四条 乙方如若无法在规定时间内做出响应和完成相关安全工作，甲方可自行组织开展相关工作，乙方承担由此产生的所有费用。

第十五条 乙方的网络安全责任自本协议盖章之日起开始生效。

第十六条 本协议一式三份，甲方建设部门和乙方各一份，报备学校信息化办公室一份。

甲方（盖章）：郑州大学　　乙方（盖章）：郑州顺腾科技有限公司

部门负责人（签字）：　　法人或授权代表（签字）：王慧杰

签字日期：　　签字日期：2025.12

附件 4：

郑州大学信息系统建设信息安全保密协议

甲方： 郑州大学

乙方： 郑州顺腾科技有限公司

甲、乙双方现就 郑州大学信息化办公室、网络管理中心采购数据治理深化提升建设项目 （以下简称“项目”）进行建设合作。根据《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》等相关法律法规和《信息安全技术 网络安全等级保护基本要求（GB/T 22239-2019）》《信息安全技术 个人信息安全规范（GB/T 35273-2020）》等相关国家标准，本着平等、自愿、公平、诚信的原则，经双方协商一致，就该项目实施及后续合作过程中的数据安全保密责任事项达成本协议。

第一条 乙方严格遵守《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》等相关法律法规和国家相关标准的要求，执行郑州大学网络安全管理相关规定和办法。

第二条 本协议中的“保密信息”是指乙方在项目调研、开发、管理、实施、运维、售后服务及后续合作过程中，对所接触到来源于甲方以任何方式获取、不为公众所知的所有信息、数据、资料和技术等，包括与项目规划有关的建设规划、实施方案、项目合同、其他内部文件等，与运行环境有关的网络拓扑、设备信息、网络协议、部署结构等，与系统开发有关的技术参数、软件架构、开发文档、配置文档、业务软件及源代码、管理手册、知识产权信息及产品专利等，与运维管理有关的各类设备及系统账号口令、密码管理策略、日志数据、用户手册、内部管理规章制度等，与业务数据有关的教职员工、学生、注册用户等个人信息以及教学、科研、管理、办公、财务、人事等业务数据。乙方以任何形式全部或部分从保密信息中获得的任何信息、数据、资料和技术等均被视为保密信息。

虽然不属于上述所列情形，但信息、数据、资料和技术自身性质表明其明显是保密的。

第三条 乙方保证该保密信息仅用于与双方合作项目有关的用途或目的。未经甲方同意，乙方不得对保密信息进行复制、修改、重组、逆向工程等，不得利用保密信息进行新的研究或开发利用。

第四条 未经甲方同意，乙方不得向任何第三方传播或披露甲方的保密信息。

第五条 乙方应采取必要措施保护和妥善保存从甲方获知的保密信息，防止保密信息被盗窃和/或泄露，乙方保存保密信息的存储介质应由乙方指定的专人进行管理，并向甲方报备。

第六条 乙方不得刺探与本项目无关的甲方保密信息。

第七条 保密信息仅可在乙方范围内仅为项目之目的而使用，乙方应保证相关使用人员在知悉该保密协议前，明确保密信息的保密性及其应承担的义务，并以书面形式同意接受本协议条款的约束。乙方应对上述人员的保密行为进行有效的监督管理，如发现保密信息泄露，应采取有效措施防止泄密进一步扩大，并及时告知甲方。若乙方上述人员出现岗位调动或离职的情形，乙方有义务立即通知并配合甲方终止其与甲方有关的信息访问权限，收回其所持有的甲方保密资料和涉密介质，并确保该人员在离职后继续履行好保密义务。

第八条 存有保密信息的存储介质如需送到单位外维修时，要将涉密资料备份后，对介质进行技术处理，以防泄密。

第九条 乙方所承担项目建设工作完成后或中途不再从事本项目相关工作，不得保留任何保密信息的副本。

第十条 甲乙双方一致认同，对于本协议签订及履行过程中、项目的商谈及合作过程中所接触到的甲方及其所属单位所有机构的保密信息，乙方应根据本协议约定履行保密义务、承担责任。

第十一条 乙方同意：若违反本协议书内容，甲方有权制止乙方行为并要求其消除影响，视行为严重程度进行处罚；后果严重者，甲方将通过法律途径要求乙方进行经济赔偿，并向司法机关报案处理。

第十二条 乙方的保密义务自本协议盖章之日起开始生效。

第十三条 乙方的保密义务并不因双方合作关系的解除而免除。

第十四条 本协议书一式三份，甲方建设部门和乙方各一份，报备学校信息化办公室一份。

甲方（盖章）：郑州大学　　乙方（盖章）：郑州顺腾科技有限公司

部门负责人（签字）：　　法人或授权代表（签字）：王慧杰

签字日期：　　签字日期：2023.12.12

附件 5：

中 标（成交）通 知 书

郑州顺腾科技有限公司：

你方递交的郑州大学信息化办公室、网络管理中心采购数据治理深化提升建设项目(数据分级分类、数据安全风险评估)投标文件，经专家评标委员会（或询价小组、竞争性磋商小组、竞争性谈判小组）评审，被确定为中标人。

主要内容如下：

项目名称	郑州大学信息化办公室、网络管理中心采购数据治理深化提升建设项目(数据分级分类、数据安全风险评估)
采购编号	豫财磋商采购-2024-1303
中标（成交） 价	479000 元(人民币) 肆拾柒万玖仟元整(人民币)
供货期（完工期、服务期限）	自合同签订之日起 30 个日历天。
供货（施工、服务）质量	符合国家或行业规定的合格标准且满足采购人要求。
交货（施工、服务）地点	采购人指定地点。
质保期	自验收合格之日起 3 年。

请你方自中标通知书发出之日起 3 日内与招标人洽谈合同事项。联系人及电话：李润知 18530017799

特此通知。

采购单位(盖章)　　代理单位（盖章）

2024年 12月 11日

中标单位签收人：程延钠 17634835686