甲方合同编号：豫财磋商采购-2024-849-4

河南工业职业技术学院2024网络基础设施保障及运维项目-4包-网络安全运维和服务采购合同

采购方：河南工业职业技术学院

供货商：河南安服网络科技有限公司

日期：2024年9月

采购合同

		合同编号：	豫财磋商采购-2024-849-4
甲方：	河南工业职业技术学院	采购合同：	2024 网络基础设施保障及运维项目-4 包-网络安全运维和服务采购合同
乙方：	河南安服网络科技有限公司	签约地点：	河南. 南阳. 宛城区

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》的规定，甲乙双方根据豫财磋商采购-2024-849 号“河南工业职业技术学院 2024 网络基础设施保障及运维项目-4 包-网络安全运维和服务”中标通知书和招投标文件要求，经甲、乙双方协商，本着平等自愿、诚实信用的原则，签订本合同。

第一条　购买服务的内容及期限

1、甲方以公开招标方式采购乙方提供以下服务：

内容包括：承担学校网络安全设备监测与维护、网络安全问题处置、安全策略的调整、安全加固与应急响应等相关网络安全服务。

服务地点：河南工业职业技术学院

第二条　服务事项（详见附件 1）

第三条　服务期限

本服务期限为　一年　。自合同签订之日起。

第四条　甲方权利义务

1、甲方有对乙方提出改进服务意见的权利，监督乙方工作。

2、甲方负责为乙方提供正常工作环境和工作条件。

3、乙方在工作中需要甲方工作人员协助的，甲方应积极配合。

第五条　乙方权利义务

1、乙方应接受甲方的监督和考核，遵守甲方的规章制度，根据合同约定，服从甲方安排。

2、在工作区域内乙方人员提供管理服务过程中，因乙方人员的故意或过失，造成甲乙双方或任何第三方的人身损害或财产损失，乙方承担一切法律责任与赔偿。

第六条　服务目标

乙方根据甲方的具体服务事项及招标文件要求提供服务。工作标准和考核标准按照招标文件要求执行。

第七条　服务费用

本合同以人民币付款，总计 175900 元(大写：拾柒万伍仟玖佰元整)。

结算方式为：分两个阶段验收和付款，合同签订正式进场服务 2 个月后开展第一次验收，验收合格乙方开具增值税发票，甲方收到发票后支付总款的 30%。合同签订正式进场服务 9 个月后开展第二次验收，验收合格乙方开具增值税发票，甲方收到发票后支付总款 70%的款项。

3. 合同签订前，乙方需向甲方支付合同总金额 5%的履约保证金，该履约保证金在乙方履行项目相应运维服务且甲方对项目最终验收合格后无质量问题无息退还。

第八条　验收方法

甲方应当按照政府采购合同规定的技术、服务、安全标准组织对乙方履约情况进行验收，并出具验收书。验收书应当包括每一项技术、服务、安全标准的履约情况。验收不合格的，乙方应负责改进或重新提供服务达到本合同约定的质量要求的标准；验收合格的，验收书作为支付货款的重要依据。

第九条 违约责任

1、甲方违反本合同的约定，使乙方不能完成服务目标，乙方有权要求甲方在一定期限内解决，逾期未解决的乙方有权终止合同；造成乙方经济损失的，甲方应给予乙方经济赔偿。

2、乙方违反本合同的约定，不能完成服务目标，甲方有权要求乙方限期整改，逾期未整改的，甲方有权终止合同；造成甲方经济损失的，乙方应给予甲方经济赔偿。

3、乙方违反本合同的约定，擅自提高收费标准的，甲方有权要求乙方清退；造成甲方经济损失的，乙方应给予甲方经济赔偿。

4、甲乙双方任何一方无法律依据提前终止本合同的，违约方应赔偿对方合同全额的违约金；造成对方经济损失的，应给予经济赔偿。

第十条 其他事项

1、本合同自甲乙双方签字盖章后生效。

2、合同执行期内，甲乙双方均不得随意变更或解除合同。合同如有未尽事宜，须经双方共同协商，做出补充规定，补充规定与本合同具有同等效力，也可按照《中华人民共和国民法典》的规定执行。

3、本合同执行期间，如遇不可抗力，致使合同无法履行时，双方按有关法律规定及时协商处理。

4、本合同如发生纠纷，当事人双方应当及时协商解决，协商不成时，任何一方均可请政府采购监督管理机关调解，调解不成，按以下第(1)项方式处理：(1) 根据《中华人民共和国仲裁法》的规定向南阳仲裁委员会申请仲裁。(2)向合同签订地有管辖权的人民法院起诉。

5、采购双方必须严格按照招标文件、投标文件及有关承诺签订采购合同，不得擅自变更。对任何因双方擅自变更合同引起的问题市政府代理机构概不负责，合同风险由双方自行承担。

6、在此合同期满后，如甲乙双方均无异议，合同自动顺延一年。

7、本合同一式 陆 份， 甲方 肆 份、乙方 贰 份。经双方签字盖章后生效，具有同等的法律效力。

第十一条 下列关于采购文件及有关附件是本合同不可分割的组成部分，与本合同具有同等法律效力，这些文件包括但不限于：(1) 招标文件(2)乙方提供的投标文件(3) 服务承诺；(4) 甲乙双方商定的其他文件。以上附件顺序在前的具有优先解释权。

甲 方：	河南工业职业技术学院	乙 方：	河南安服网络科技有限公司
开户行：	中原银行南阳兴宛支行	开户行：	中国民生银行郑州农科路支行
账 号：	5000209494000010	账 号：	637916054
委托代理人：		委托代理人：	
地 址：	河南. 南阳. 杜诗路 1666 号	地 址：	郑州高新技术产业开发区金菊街 30 号 1 幢 1 单元 15 层 301 号

签约时间：	2024年 9月 10日	签约时间：	2024年 9月 10日

合同签订地：南阳市宛城区

附件 1

一、服务项目

包括并不仅限于以下内容：

服务项目	服务内容
网络安全运维和服务	一、身份信息及口令管理 ★1.通过防火墙和 VPN 系统，每月检查学校各信息化应用系统管理员的登录情况，并进行身份鉴别；配置信息化应用系统管理员的登录地址，使之能够被相应限制；对 VPNETYN 用户的口令进行定期检查，杜绝用户使用初始密码或简单密码；定期检查信息化应用系统是否启用远程管等功能，设备进行远程管理时，是否采用了相应的安全措施。 2.每季度检查是否启用访问控制功能，依据安全策略控制用户对资源的访问。 二、安全漏洞管理 ★3.漏洞扫描与验证：每月针对服务范围内的设备的系统漏洞和软件漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害，要具备全局风险统计能力，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。每个月对扫描结果出具一份扫描报告，及时将存在问题反馈给相关部门管理人员，督促相关部门进行处理。 4. 每半年完成一次全面扫描，包括资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查等任务类型。 5. 漏洞优先级排序：能够从高危、中危、低危、信息四个安全级别展示漏洞风险等级的分布情况，提供客观的漏洞修复优先级指导。 6.漏洞修复建议：针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。 7.漏洞状态追踪：对发现的漏洞建立状态追踪机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，做

	到漏洞的可视、可管、可控。 8. 最新漏洞预警与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。 9. 最新漏洞处置指导：一旦确认漏洞影响范围后，提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。 10. 及时升级各安全设备的特征库，确保安全设备能够及时对新型病毒及攻击进行识别和防护。 三、安全威胁管理 ★11. 能充分利用学校的网络安全设备，包括态势感知平台、IPS 防火墙、上网行为审计等设备和系统，识别和发现存在的安全威胁，并及时应对处置。 12. 提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态，发现各类安全事件，并自动生成报表。 13. 实时监测网络安全状态，对攻击事件自动化生成报表，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件等。 14. 每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议。 15. 实时监测网络安全状态，对病毒事件自动化生成报表，及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发 DOS 型、C&C 访问型、文件感染型、木马型，结合威胁情报，投标方需排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固。 16. 投标方需每月主动分析病毒类的安全事件：提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀。

	17. 投标方需每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置。 18. 投标方需每月主动分析失陷类的安全事件并协助用户处置，并提供溯源服务。 19. 策略定期管理：投标方需每月对安全设备组件上的安全策略进行统一管理工作，确保安全设备组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，通过全网大数据分析，发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为。 四、安全事件管理 21. 实时监测异常流量、攻击日志和病毒日志，通过海量数据分析、多平台聚合发现安全事件。 22. 入侵原因分析：还原攻击路径，分析入侵事件原因加固建议指导：结合现有安全防御体系，进行安全加固、提供整改建议、防止再次入侵。 23. 针对信息系统突发的重大安全事件，以最快的时间进行故障排查定位和应急处理。

二、服务要求

1．响应时间

（1）基本时间要求：供应商提供服务期内每周 5*8 小时至少 1 名工程师驻场服务，7×24 小时的全天候随时响应服务，并根据采购人工作需要，参与值班加班，特殊时段最大限度增派后备人员保障采购人的临时应用需求,保障校园网安全正常运行。供应商提供 7×24 小时畅通的热线联系电话。响应时间指采购人发现问题，供应商须在 1 小时内完成以下内容的初步判定：问题级别、影响范围、解决所需资源、解决时长，并尽快完成故障排查和故障处理。如果驻场工程师无法进行故障处理，采购人要求供应商临时指派后备或协调原厂工程师现场处理时，供应商必须协助采购人完成相关工作及人员的调配安排。

（2）现场不间断工作支持服务：在校园网安全发生重大事件、关键时点或重大活

动及紧急工作等情况下，供应商应派相应级别且能解决问题的后备工程师提供支持，按采购人要求，立即开始不间断服务，直至系统能够满足采购人业务及工作正常进行的要求。

2．维保人员要求

（1）热爱教育事业，热爱本职工作，遵纪守法，品德优良，身心健康。

（2）遵守校纪校规，服从采购人管理，供应商所提供的各种服务及派驻的工程技术人员需严格遵守采购人的各项管理及规章制度。供应商所提供的各种服务及派驻人员需接受采购人的直接管理，配合采购人的各项工作。供应商不经采购人同意不得安排驻场人员回供应商所在公司从事各类业务。

（3）驻场人员资质要求：要求驻场人员具有普通高等教育本科及以上学历，有学校网络安全运维经验人员优先。

（4）驻场人员的技能要求：熟悉网络设备、安全设备的操作及维护等运维管理操作；

3．维保相关工作管理要求

（1）驻场人员人数及上岗要求：驻场人员在驻场期间内，严格按照采购人的考勤制度，每日记录考勤，驻场人员不得随意脱岗离岗，如需请假，须通报采购人同意，履行正式请假手续；驻场人员接受采购人要求的在职责范围内调整安排工作，驻场期间如有重大事件，须按照要求 7*24 小时在岗，保证采购人设备及网络的正常运行，值班加班原则上安排在寒暑假进行调休。

（2）供应商不得临时调换驻场人员，以保障运维工作的连续性，供应商变更驻场人员须向采购人提出书面正式申请，采购人有权扣减运维服务费，每人次扣减服务费 2 万元。

由采购人对相关服务及驻场人员进行考核、监督及评价。驻场人员服务效果由采购人评价，每月一次，技术能力不足或不适应驻场工作需要，供应商应及时调换，每人次扣减服务费 1 万元。

（3）文档管理和信息支持服务：供应商应每月对日常安全运维中的问题及各种记录、日志进行分析和总结，同时以月报的形式将结果反馈给采购人。要求每月提供一份月报，报告本月工作及网络运行情况和安全运维总结。

（4）保密要求：服务期内，供应商必须签订保密协议，供应商承诺严格保护采购

人系统、数据、信息的安全，在服务期满后永久不得泄露采购人所有信息。由于供应商违反保密协议而导致的泄密或破坏，由供应商负全责，并由供应商赔偿采购人所有损失，若构成犯罪的由公安部门依法追究当事人相关责任。供应商需提供服务期内保护采购人系统、数据、信息的安全， 以及服务期满后永久保守采购人信息秘密的承诺书。

（5）监督与投诉受理要求：采购人应对供应商所提供服务质量及驻场人员工作表现进行监督，结合故障处理的用户回访满意率做出综合评价。如因供应商服务质量对采购人造成重大影响，采购人根据供应商服务考核表现有权利要求供应商撤换驻场工程师或改善服务质量，直至要求终止服务合同，并提供相应赔偿，供应商向采购人支付合同总额 10%的赔偿金。

违反保密规定、泄露系统信息、影响数据安全的，采购人有权终止合同，并对于构成犯罪的由公安部门依法追究当事人相关责任，同时，供应商向采购人支付合同总额 20%的违约金。

(6) 针对本项目建立技术交流、培训机制，合同期内开展不少于两次安全培训，培训包括网络安全、应急处理及相关网络新技术的介绍等内容。

4.服务效果

（1）要求通过日常网络安全运维及安全隐患的妥善处置，保障校园网络安全设备及系统稳定、可靠地运转，校园网不出现重大网络安全事件。

（2）当校园网遇到重大网络安全故障时，要求供应商能够快速响应进行修复，供应商后备工程师需在 4 小时内赶赴现场，并在尽可能短的时间里对故障进行处置。