郑州信息科技职业学院
网络安全建设及设备续保服务项目

合同编号：WX2024004

合
同
书

甲方：郑州信息科技职业学院

乙方：河南合众信泰科技有限公司

合同编号： WX2024004

签署地点：郑州信息科技职业学院

甲方（需方）：郑州信息科技职业学院

乙方（供方）：河南合众信泰科技有限公司

郑州信息科技职业学院所需 网络安全建设及设备续保服务项目 （采购编号： 豫财磋商采购-2024-164 ）经招标代理机构名称 河南正禄招标代理有限公司 以招标方式 竞争性磋商 进行采购，确定 河南合众信泰科技有限公司 为成交供应商。甲乙双方根据《中华人民共和国民法典》、《中华人民共和国政府采购法》和其他法律、法规的规定，并按照公正、平等、自愿、诚实信用的原则，同意按照以下条款和条件，签署本合同。

一、本合同在此声明如下：

1）本合同总金额为：2376000.00 元；大写：贰佰叁拾柒万陆仟元整。

2）本合同中的词语和术语的含义与合同条款中定义的相同。

3）下述文件作为合同签订的基础，是构成本合同的主要组成部分，并与本合同一起阅读和解释：

附件 1：供货范围及分项价格表

附件 2：产品技术规格表

附件 3：中标通知书

4）服务要求：符合国家或行业规定的合格标准，满足采购人提出的技术标准及要求。

5）服务期限：一次性建设内容在合同签订后 30 日历天内完成交付；服务类内容在合同签订后 30 日历天内完成服务前准备，并从正式服务日期起计算。

6）质量保证期：驻场服务、风险评估及保障服务、安全运营监测服务、网络安全能力服务、等级保护测评服务运维周期为 2 年，上网行为管理系统续保服务和数据中心防火墙续保服务软件续保服务为 3 年，动力环境监控系统质保期为 3 年。

7）合同履行期限：自合同生效起至质保期结束。

二、合同履行的地点及工程进度：合同生效后，乙方应于 30 日内按甲方要求在采购人指定地点（甲方指定地点）完成本项目工作。

三、付款方式：货物类、等保测评服务及设备续保类服务乙方将工作完成试运行 30 日后，由甲方组织进行验收，乙方技术人员参加，验收通过后支付相关货物或服务金额的 100%。网络安全类服务，服务期每满 6 个月（共 4 次）由甲方组织进行验收，乙方技术人员参加，验收通过后支付相关服务金额的 25%。

四、人员培训：乙方免费对甲方人员进行必要的业务及服务培训。

五、申请付款时必须提交以下文件和资料：1、资金支付申请书；2、由需方签字的验收报告；3、国产产品提供增值税专用发票；进口产品需提供形式发票、原产地证明、与国外厂商或代理商的购买协议、水单、报关单和免税表。

六、招、投标文件及其修改、澄清均为本合同的组成部分。

七、本合同签订和履行适用中华人民共和国法律，甲乙双方因质量问题发生争议，由合同签订地质量技术鉴定单位进行质量鉴定；因履行合同发生的争议，由甲乙双方直接协商解决，如协商不成可向合同签订地人民法院诉讼。

八、违约责任

1、除如因战争、严重火灾、水灾、台风、地震和其它甲乙双方认可的不可抗力事件外，甲乙双方不得随意废除合同，否则按违约处理。

2、若乙方所供的货物品牌、型号、规格、运行不符合招标文件和投标文件规定或合同规定的，乙方应负责更换并承担因更换而支付的一切费用，甲方有权拒收并追究乙方责任。因更换而造成逾期交货，则按逾期交货处理。

3、若乙方不能按时供货，除不可抗力事件外，乙方应付给甲方每星期按合同款 2%计算的违约金，不足一星期的按日折算，违约金最高不超过 10%。

4、若逾期超过 30 天仍不能供货，则甲方有权解除合同，并追究乙方责任。

九、合同生效及其他：本合同经甲乙双方代表签字、加盖公章后生效。本合同一式八份，甲方执五份、招标单位执一份、乙方执两份。

（签署页，以下无正文）

甲方名称：郑州信息科技职业学院（印章）

授权代表（签字）：

地址：郑州市郑东新区龙子湖高校区龙子湖北路 36 号

邮政编码：450000

电　　话：0371-65927612

纳税人识别号：12410000572452504K

开户银行：建行郑州龙子湖支行

帐　　户：41050167281709666668

日期：2024.5.14

乙方名称：河南合众信泰科技有限公司（印章）

授权代表（签字）：

地址：河南自贸试验区郑州片区（郑东）商务内环路 9 号楼 9 层 0901 号

邮政编码：450000

电　　话：0371-65616616

纳税人识别号：91410105687236046

开户银行：中国农业银行股份有限公司郑州商务外环路分理处

帐　　户：16048201040004028

日期：2024.5.14

附件 1、供货范围及分项价格表

序号	名称	品牌	规格型号	单位	数量	单价	小计	其它	合计
1	驻场运维服务	合众信泰	技术服务费	年	2	278590	557180	无	557180
2	风险评估及保障服务	合众信泰	技术服务费	年	2	293500	587000	无	587000
3	安全运营监测服务	合众信泰	技术服务费	年	2	137000	274000	无	274000
4	网络安全能力服务	合众信泰	技术服务费	年	2	95000	190000	无	190000
5	等级保护测评服务	合众信泰	技术服务费	套	1	286000	286000	无	286000
6	堡垒机授权服务	安恒	维护服务费	套	1	61000	61000	无	61000
7	上网行为管理系统续保服务	深信服	软件升级	套	1	133110	133110	含 URL&应用识别规则库升级	133110
8	数据中心防火墙续保服务	深信服	软件升级	套	1	171710	171710	含深信服云智订阅软件	171710
9	动力环境监控系统	中广控	集中监控系统平台软件 V2.0 ZGKON-CONTROL	套	1	116000	116000	无	116000
合计：2376000 元；人民币：贰佰叁拾柒万陆仟元整									

附件 2、产品技术规格表

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
1	驻场运维服务	一、服务范围要求	一、服务范围响应	无偏离	满足招标参数要求	无
		1. 基础设施：虚拟化运维服务：虚拟化基础设施、私有云组件运维、技术支持、记录数据；	1. 基础设施：虚拟化运维服务：虚拟化基础设施、私有云组件运维、技术支持、记录数据；	无偏离	满足招标参数要求	无
		2. 操作系统运维服务：操作系统安装、配置、加固、故障排除、记录数据；	2. 操作系统运维服务：操作系统安装、配置、加固、故障排除、记录数据；	无偏离	满足招标参数要求	无
		3. 日常运维工作：日常问题及突发事件的及时响应反馈并解决跟进故障处理；	3. 日常运维工作：日常问题及突发事件的及时响应反馈并解决跟进故障处理；	无偏离	满足招标参数要求	无
		4. 机房硬件运维服务：中心机房硬件设备健康巡检、故障排除、设备保修、记录数据；	4. 机房硬件运维服务：中心机房硬件设备健康巡检、故障排除、设备保修、记录数据；	无偏离	满足招标参数要求	无
		5. 网络和安全运维服务：网络和安全设备运维管理，策略调整、配置优化、记录数据；	5. 网络和安全运维服务：网络和安全设备运维管理，策略调整、配置优化、记录数据；	无偏离	满足招标参数要求	无
		6. 配合学校及校园网管理部门为学校的各种活动及建设提供咨询建议和技术支持；	6. 我公司负责配合学校及校园网管理部门为学校的各种活动及建设提供咨询建议和技术支持；	无偏离	满足招标参数要求	无
		7. 结合校园网的发展建设提供新增设备与原有设备的集成与互联互通提供咨询建议和技术支持；	7. 我公司负责结合校园网的发展建设提供新增设备与原有设备的集成与互联互通提供咨询建议和技术支持；	无偏离	满足招标参数要求	无
		8. 在服务过程中需接受学校及校园网管理部门的管理，并在服务过程中和过程后提供各种相应服务文档；	8. 我公司在服务过程中接受学校及校园网管理部门的管理，并在服务过程中和过程后提供各种相应服务文档；	无偏离	满足招标参数要求	无
		9. 在校园网管理部门的安排下对学校网络运	9. 在校园网管理部门的安排下对学校网络运行	无偏离	满足招标	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		行的各种工作进行劳务支持。	的各种工作进行劳务支持。		参数要求	
		10. 要求服务商具备 ITSS 信息技术服务标准符合性证书认证证书，提供证书扫描件；	10. 我公司具备 ITSS 信息技术服务标准符合性证书认证证书，响应文件中后附证书扫描件；	无偏离	满足招标参数要求	无
		二、服务内容要求	二、服务内容响应	无偏离	满足招标参数要求	无
		11. 提供 7*24H 持续性开展网络安全运维保障工作，构建安全资产治理、安全威胁监测、安全事件响应、安全闭环处置的安全运营体系；	11. 我公司提供 7*24H 持续性开展网络安全运维保障工作，构建安全资产治理、安全威胁监测、安全事件响应、安全闭环处置的安全运营体系；	无偏离	满足招标参数要求	无
		12. 要求当资产发生变更时，运维工程师需对变更信息进行持续跟踪、信息确认与记录更新；	12. 当资产发生变更时，运维工程师将对变更信息进行持续跟踪、信息确认与记录更新；	无偏离	满足招标参数要求	无
		13. 服务商需协助制定并维护一个安全的资产静态基准，创建符合等级保护要求的信息系统安全基线，并将其落实为有效的系统黄金镜像库、安全软件版本库，安全系统配置库等切实可行的输出；	13. 我公司负责协助制定并维护一个安全的资产静态基准，创建符合等级保护要求的信息系统安全基线，并将其落实为有效的系统黄金镜像库、安全软件版本库，安全系统配置库等切实可行的输出；	无偏离	满足招标参数要求	无
		14. 服务商需协助制定有效的漏洞和补丁管理计划。定期对资产安全状态进行检查，对发现的脆弱点依据漏洞和补丁管理流程，经过严格的控制流程和测试流程，进行补丁的安装和修复工作；	14. 我公司负责协助制定有效的漏洞和补丁管理计划。定期对资产安全状态进行检查，对发现的脆弱点依据漏洞和补丁管理流程，经过严格的控制流程和测试流程，进行补丁的安装和修复工作；	无偏离	满足招标参数要求	无
		15. 服务商需协助制定有效的变更管理计划，针对合理的资产配置变更需求，进行深度分析、测试、验证。根据变更管理计划，发起变	15. 我公司负责协助制定有效的变更管理计划，针对合理的资产配置变更需求，进行深度分析、测试、验证。根据变更管理计划，发起变更流	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		更流程，更新安全配置基线，持续优化和维护资产的静态安全性；	程，更新安全配置基线，持续优化和维护资产的静态安全性；			
		16. 服务商需提供主动的威胁监测和处置服务。基于威胁监测和分析平台，持续监测和分析网络流量，对网络中存在的攻击行为、漏洞利用情况，对监测发现的安全漏洞进行分析验证，同时持续跟踪整改情况，结合威胁情报信息，提供威胁持续监测和安全处置服务；针对每一类威胁，进行深度分析和攻击成功与否验证。分析判断攻击威胁程度和影响范围，排查是否存在其他可疑主机、是否对核心资产造成威胁，协助对资产进行安全加固；	16. 我公司提供主动的威胁监测和处置服务。基于威胁监测和分析平台，持续监测和分析网络流量，对网络中存在的攻击行为、漏洞利用情况，对监测发现的安全漏洞进行分析验证，同时持续跟踪整改情况，结合威胁情报信息，提供威胁持续监测和安全处置服务；针对每一类威胁，进行深度分析和攻击成功与否验证。分析判断攻击威胁程度和影响范围，排查是否存在其他可疑主机、是否对核心资产造成威胁，协助对资产进行安全加固；	无偏离	满足招标参数要求	无
		17. 服务商需提供稳定和专业的后台支撑团队，结合现场运维团队，通过管理制度和流程完善、操作系统补丁修复、应用组件配置加固、安全设备策略调整、完善审计跟踪配置方式对安全运维工作中的管理和技术问题进行持续跟踪和处置；	17. 我公司提供稳定和专业的后台支撑团队，结合现场运维团队，通过管理制度和流程完善、操作系统补丁修复、应用组件配置加固、安全设备策略调整、完善审计跟踪配置方式对安全运维工作中的管理和技术问题进行持续跟踪和处置；	无偏离	满足招标参数要求	无
		18. 要求提供服务期内每周 7 天*12 小时两名工程师驻场服务，每个工作日 24 小时的全天候随时响应服务。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，通知服务商，或服务商在巡检当中发现问题时开始计算，服务商必须在 1 小时内完成以下内容的	18. 我公司提供服务期内每周 7 天*12 小时两名工程师驻场服务，每个工作日 24 小时的全天候随时响应服务。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，通知我公司时，或者我公司在巡检当中发现问题时开始计算，我公司将在 1 小时内完成以下内容的	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		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。如果需要协助更换备件或者驻场工程师无法进行故障处理时，采购人有权要求服务商二线工程师现场处理时，服务商必须协助采购人完成相关工作及人员的调配安排；	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。如果需要协助更换备件或者驻场工程师无法进行故障处理时，采购人有权要求我公司二线工程师现场处理时，我公司将协助采购人完成相关工作及人员的调配安排；			
		19. 二线工程师到达现场时间要求：当采购人要求服务商提供二线工程师现场支持服务时，从服务商接到采购人电话请求开始，服务商工程师必须在 4 小时内到达现场，并立即开始现场不间断工作支持服务，如非硬件问题，承诺在 24 小时内解决故障；	19. 二线工程师到达现场时间响应：当采购人要求我公司提供二线工程师现场支持服务时，我公司从接到采购人电话请求开始，我公司工程师将在 4 小时内到达现场，并立即开始现场不间断工作支持服务，如非硬件问题，承诺在 24 小时内解决故障；	无偏离	满足招标参数要求	无
		20. 现场不间断工作支持服务：在用户校园网设备、设施及相关业务及应用系统发生故障、重大事件、关键时点或重大活动及紧急工作等情况下，服务商应派相应级别且能解决问题的二线工程师到达用户现场，按用户要求，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；	20. 现场不间断工作支持服务：在用户校园网设备、设施及相关业务及应用系统发生故障、重大事件、关键时点或重大活动及紧急工作等情况下，我公司将派相应级别且能解决问题的二线工程师到达用户现场，按用户要求，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；	无偏离	满足招标参数要求	无
		21. 提前做好设备巡检等日常维护措施，由驻场专责工程师每天到现场对所有设备进行巡检，检查系统的物理运行环境及运行状态和系统日志，并向网络管理部门汇报巡检情况；	21. 我公司将提前做好设备巡检等日常维护措施，由驻场专责工程师每天到现场对所有设备进行巡检，检查系统的物理运行环境及运行状态和系统日志，并向网络管理部门汇报巡检情况；	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		22.服务商应每日、每周及每月对巡检及日常运维中的问题及各种记录、日志进行分析和总结，同时以日报、周报和月报的形式将结果反馈给采购人。服务商应建立专门的系统维护档案及日志，服务商工程师第一次到现场服务巡检时，要核对并记录所负责维护的设备详细配置清单、所使用的操作系统、版本号、系统的使用情况及系统的配置参数。要建立和完善主机系统的技术档案，同时对用户系统提供相应的技术支持的电子文档。服务商对用户的所有保修设备，均根据每次的电话记录、预防性维修报告和故障维修报告建立技术文档，详细记录设备型号、故障时间、故障类型、所有日志内容包括但不限于校园网设备巡检日志、软硬件及设备配置变动日志、设备维护日志、网络故障处理日志、网络故障受理记录、7*12 小时值班日志、网络运行情况分析及汇总报告、周报及月报等；	22.我公司负责每日、每周及每月对巡检及日常运维中的问题及各种记录、日志进行分析和总结，同时以日报、周报和月报的形式将结果反馈给采购人。我公司将建立专门的系统维护档案及日志，我公司工程师第一次到现场服务巡检时，将核对并记录所负责维护的设备详细配置清单、所使用的操作系统、版本号、系统的使用情况及系统的配置参数。我公司将建立和完善主机系统的技术档案，同时对用户系统提供相应的技术支持的电子文档。我公司对用户的所有保修设备，均根据每次的电话记录、预防性维修报告和故障维修报告建立技术文档，详细记录设备型号、故障时间、故障类型、所有日志内容包括但不限于校园网设备巡检日志、软硬件及设备配置变动日志、设备维护日志、网络故障处理日志、网络故障受理记录、7*12 小时值班日志、网络运行情况分析及汇总报告、周报及月报等；	无偏离	满足招标参数要求	无
		三、人员能力要求	三、人员能力响应	无偏离	满足招标参数要求	无
		23.驻场工程师资质要求：驻场工程师具有计算机或网络相关专业本科毕业，有两年以上工作经验。具体如下：熟悉网络设备、安全设备、机架及线缆等系统集成相关设备的操作及维	23.驻场工程师资质：我公司提供的驻场工程师均为计算机专业本科毕业，具有两年以上工作经验。具体如下：驻场工程师熟悉网络设备、安全设备、机架及线缆等系统集成相关设备的	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		护等运维管理操作；熟悉服务器、存储、虚拟化、数据库等运维管理操作；至少一名工程师具备信息与通信技术类高级工程师级别认证证书，提供工程师证书和所在供应商连续半年的社保证明材料；	操作及维护等运维管理操作；熟悉服务器、存储、虚拟化、数据库等运维管理操作；2 名工程师均具备信息与通信技术类高级工程师级别认证证书，响应文件中后附工程师证书和连续半年的社保证明材料；			
		24. 为保证学校网络、数据中心、业务系统的稳定不间断运行，要求服务商具备稳定和专业的后台支撑团队，工程师需具备专业资格认证、受过良好的技术培训、拥有丰富的工作经验；	24. 为保证学校网络、数据中心、业务系统的稳定不间断运行，我公司具备稳定和专业的后台支撑团队，工程师均具备专业资格认证、受过良好的技术培训、拥有丰富的工作经验；	无偏离	满足招标参数要求	无
		25. 要求服务商至少 5 名工程师通过信息与通信技术厂商认证的数通方向(IE 级别)的认证，提供工程师证书和所在供应商连续半年的社保证明材料；	25. 我公司具有并提供 6 名工程师通过信息与通信技术厂商认证的数通方向（IE 级别）的认证，响应文件中后附工程师证书和连续半年的社保证明材料；	无偏离	满足招标参数要求	无
		26. 要求服务商至少 2 名工程师通过信息与通信技术厂商认证的服务器与存储方向（IE 级别）的认证，提供工程师证书和所在供应商连续半年的社保证明材料；	26. 我公司具有并提供 3 名工程师通过信息与通信技术厂商认证的服务器与存储方向（IE 级别）的认证，响应文件中后附工程师证书和连续半年的社保证明材料；	无偏离	满足招标参数要求	无
		27. 要求服务商至少 2 名工程师通过信息与通信技术厂商认证的安全方向(IE 级别)的认证，提供工程师证书和所在供应商连续半年的社保证明材料；	27. 我公司具有并提供 2 名工程师通过信息与通信技术厂商认证的安全方向（IE 级别）的认证，响应文件中后附工程师证书和连续半年的社保证明材料；	无偏离	满足招标参数要求	无
		28. 要求服务商至少 3 名工程师通过信息与通信技术厂商认证的云计算方向（IE 级别）的认	28. 我公司具有并提供 3 名工程师通过信息与通信技术厂商认证的云计算方向（IE 级别）的认	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		证，提供工程师证书和所在供应商连续半年的社保证明材料；	证，响应文件中后附工程师证书和连续半年的社保证明材料；			
		29. 要求服务商至少 1 名工程师通过数据中心工程师数据库方向认证（OCM 证书）的认证和至少 2 名工程师通过数据中心工程师数据库方向认证（OCP 证书）的认证，提供工程师证书和所在供应商连续半年的社保证明材料；	29. 我公司具有并提供 1 名工程师通过数据中心工程师数据库方向认证（OCM 证书）的认证和 2 名工程师通过数据中心工程师数据库方向认证（OCP 证书）的认证，响应文件中后附工程师证书和连续半年的社保证明材料；	无偏离	满足招标参数要求	无
		30. 要求服务商至少 6 名工程师通过信息安全工程师认证并获得信息安全保障人员证书，提供工程师证书和所在供应商连续半年的社保证明材料；	30. 我公司具有并提供 6 名工程师通过信息安全工程师认证并获得信息安全保障人员证书，响应文件中后附工程师证书和连续半年的社保证明材料；	无偏离	满足招标参数要求	无
2	风险评估及保障服务	1. ★风险评估服务：要求针对业务系统的弱点进行评估。应包含应用系统、操作系统、业务系统部署位置、安全域划分、安全设备防护等等评估内容。在测试过程中将对可能发现的安全隐患给予说明，同时给出该隐患的解决建议。服务完毕后，出具《网络安全风险评估报告》，报告内容包含以上所有项目。服务频率：2 次/年；要求服务商具备信息安全风险评估服务资质证书，提供证书扫描件；	1. 风险评估服务：针对业务系统的弱点进行评估。包含应用系统、操作系统、业务系统部署位置、安全域划分、安全设备防护等等评估内容。在测试过程中将对可能发现的安全隐患给予说明，同时给出该隐患的解决建议。服务完毕后，出具《网络安全风险评估报告》，报告内容包含以上所有项目。服务频率：2 次/年；我公司具备信息安全风险评估服务资质证书，响应文件中后附证书扫描件；	无偏离	满足招标参数要求	无
		2. ★新系统上线前安全评估服务：本服务要求对新上线的系统，进行上线前的安全配置核查及风险评估，新系统评估通过后，才可以正式上线进行系统接入，正式上线运营。完成评估	2. 新系统上线前安全评估服务：本服务对新上线的系统，进行上线前的安全配置核查及风险评估，新系统评估通过后，才可以正式上线进行系统接入，正式上线运营。完成评估后，出	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		后，出具《业务上线评估报告》，频率：1份/次；要求服务商具备信息安全风险评估系统，并提供中华人民共和国国家版权局颁发的计算机软件著作权登记证书，提供证书扫描件；	具《业务上线评估报告》，频率：1份/次；我公司具备信息安全风险评估系统，响应文件中后附中华人民共和国国家版权局颁发的计算机软件著作权登记证书扫描件；			
		3.★日常安全咨询服务：安全咨询服务是教育行业运维人员在对已经信息系统进行安全运维、管理、建设过程中产生疑问的地方进行专业、详尽的安全解答，及时传递安全行业内最新纰漏出的安全漏洞、安全技术、安全热点等信息，提醒信息系统管理人员及时更新、加固系统。并对上级部门下发行业内的信息安全要求、安全指标、安全检查等安全任务进行协助完成；要求服务商具备信息系统安全运维服务资质证书，提供证书扫描件；	3.日常安全咨询服务：安全咨询服务是教育行业运维人员在对已经信息系统进行安全运维、管理、建设过程中产生疑问的地方进行专业、详尽的安全解答，及时传递安全行业内最新纰漏出的安全漏洞、安全技术、安全热点等信息，提醒信息系统管理人员及时更新、加固系统。并对上级部门下发行业内的信息安全要求、安全指标、安全检查等安全任务进行协助完成；我公司具备信息系统安全运维服务资质证书，响应文件中后附证书扫描件；	无偏离	满足招标参数要求	无
		4.网站安全监测服务：a.要求7*24小时实时监测互联网可达的学校门户网站；b.要求通过周期性的监控，持续对网站的文本内容进行检测，以保障网站的安全性和合规性，一旦检测到敏感关键字的存在，则发出告警；c.要求提供多个敏感词字典：内置字典、AI智能检测引擎、自定义字典；触发告警时会提供网页快照，且高亮关键字；d.要求发现网页中存在错链、坏链、异常友链等异常链接情况，则发出告警；e.通过检测网站的文件和代码，识别潜在的挂	4.网站安全监测服务：a.我公司提供7*24小时实时监测互联网可达的学校门户网站；b.通过周期性的监控，持续对网站的文本内容进行检测，以保障网站的安全性和合规性，一旦检测到敏感关键字的存在，则发出告警；c.提供多个敏感词字典：内置字典、AI智能检测引擎、自定义字典；触发告警时会提供网页快照，且高亮关键字；d.发现网页中存在错链、坏链、异常友链等异常链接情况，则发出告警；e.通过检测网站的文件和代码，识别潜在的挂马行	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		马行为。一旦发现挂马现象，立即向用户发送告警通知；f.要求在证书即将到期的15天内，会每日向用户发送告警通知；g.要求支持以微信通知的方式对所有告警事件类别进行实时告警；h.要求支持邮件的方式实时推送所有告警事件类别；i.要求支持钉钉机器人实时推送所有告警事件类别；j.要求支持企业微信器人实时推送所有告警事件类别；k.平台可自动生产监控周报，每周一自动生成上一周期（上周一00:00:00至上周日23:59:59）；l.要求及时发现网站的运行状态、中高危漏洞、暗链、挂马、违规关键字等，经过人工验证后第一时间通知用户整改。每周出具一份《网站监测周报》；	为。一旦发现挂马现象，立即向用户发送告警通知；f.在证书即将到期的15天内，会每日向用户发送告警通知；g.支持以微信通知的方式对所有告警事件类别进行实时告警；h.支持邮件的方式实时推送所有告警事件类别；i.支持钉钉机器人实时推送所有告警事件类别；j.支持企业微信器人实时推送所有告警事件类别；k.平台可自动生产监控周报，每周一自动生成上一周期（上周一00:00:00至上周日23:59:59）；l.及时发现网站的运行状态、中高危漏洞、暗链、挂马、违规关键字等，经过人工验证后第一时间通知用户整改。每周出具一份《网站监测周报》；			
		5.安全事件应急响应服务：当学校发生安全事件，如网络拥塞、中病毒、网站被入侵，服务团队会第一时间响应，协助用户解决问题、查找原因、给出加固建议并协助用户进行加固。技术支持：当上级机关对用户进行安全检查时，或学校收到上级或公安机关通报后，提供技术支持，协助整改。频率：按需服务；每次应急响应结束后，出具《应急响应报告》；	5.安全事件应急响应服务：当学校发生安全事件，如网络拥塞、中病毒、网站被入侵，服务团队会第一时间响应，协助用户解决问题、查找原因、给出加固建议并协助用户进行加固。技术支持：当上级机关对用户进行安全检查时，或学校收到上级或公安机关通报后，提供技术支持，协助整改。频率：按需服务；每次应急响应结束后，出具《应急响应报告》；	无偏离	满足招标参数要求	无
		6.攻击面分析与识别服务：a.要求发现暴露在互联网侧的域名资产及各种属性。包括：域名	6.攻击面分析与识别服务：a.发现暴露在互联网侧的域名资产及各种属性。包括：域名名称、	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		名称、主子域名关系、备案主体等；b.要求发现暴露在互联网侧的IP资产及各种属性。包括：IP地址、端口数量、关联域名、归属地、运营商、ASN等；c.要求支持以微信通知的方式对所有告警事件类别进行实时告警；d.要求支持邮件的方式实时推送所有告警事件类别；e.要求支持钉钉机器人实时推送所有告警事件类别；f.要求支持企业微信器人实时推送所有告警事件类别；g.要求提供监控周报和支持用户任意时间手动生成报告；	主子域名关系、备案主体等；b.发现暴露在互联网侧的IP资产及各种属性。包括：IP地址、端口数量、关联域名、归属地、运营商、ASN等；c.支持以微信通知的方式对所有告警事件类别进行实时告警；d.支持邮件的方式实时推送所有告警事件类别；e.支持钉钉机器人实时推送所有告警事件类别；f.支持企业微信器人实时推送所有告警事件类别；g.提供监控周报和支持用户任意时间手动生成报告；			
		7.安全策略分析和优化加固服务：	7.安全策略分析和优化加固服务：	无偏离	满足招标参数要求	无
		补丁加固：要求对评估过程中发现的系统补丁漏洞进行加固(有条件的情况下会进行测试)，此过程需要与用户进行充分沟通；	补丁加固：对评估过程中发现的系统补丁漏洞进行加固（有条件的情况下会进行测试），此过程要与用户进行充分沟通；	无偏离	满足招标参数要求	无
		配置参数加固：要求对评估过程中发现的配置类问题进行加固，如权限设置、策略配置、参数设置等；	配置参数加固：对评估过程中发现的配置类问题进行加固，如权限设置、策略配置、参数设置等；	无偏离	满足招标参数要求	无
		安全管理加固：要求对评估过程中发现的组织、人员、安全域规划等方面的安全风险提出解决建议；	安全管理加固：对评估过程中发现的组织、人员、安全域规划等方面的安全风险提出解决建议；	无偏离	满足招标参数要求	无
		整改完毕后，出具《整改加固报告》，对所有整改项目做详细说明；频率：2次/年；	整改完毕后，出具《整改加固报告》，对所有整改项目做详细说明；频率：2次/年；	无偏离	满足招标参数要求	无
		8.★渗透测试服务：	8.渗透测试服务：	无偏离	满足招标	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件		参数要求	
		（1）要求服务商应保证信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，根据采购人提供的账户信息对系统所有页面进行安全风险入侵测试，查找针对应用程序的各种漏洞，发现系统脆弱路径并针对安全隐患提出解决办法，切实保证信息系统安全；	（1）我公司保证信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，根据采购人提供的账户信息对系统所有页面进行安全风险入侵测试，查找针对应用程序的各种漏洞，发现系统脆弱路径并针对安全隐患提出解决办法，切实保证信息系统安全；	无偏离	满足招标参数要求	无
		（2）要求服务商应在投标文件技术部分详细说明渗透测试的实施流程、渗透测试方法、实施过程中用到的工具、提供渗透测试所面临的主要风险及相应的风险规避措施；	（2）我公司在响应文件技术部分已详细说明渗透测试的实施流程、渗透测试方法、实施过程中用到的工具、提供渗透测试所面临的主要风险及相应的风险规避措施；	无偏离	满足招标参数要求	无
		（3）要求渗透测试应至少包含如下项目：WEB应用系统渗透、主机操作系统渗透、数据库系统渗透；渗透测试内容包括但不限于：身份验证类、会话管理类、访问控制类、输入处理类、信息泄露类、第三方应用类；	（3）渗透测试包含如下项目：WEB应用系统渗透、主机操作系统渗透、数据库系统渗透；渗透测试内容包括但不限于：身份验证类、会话管理类、访问控制类、输入处理类、信息泄露类、第三方应用类；	无偏离	满足招标参数要求	无
		（4）要求服务商应编写渗透测试报告并提交给学校，报告应该阐明学校业务系统中存在的安全隐患以及专业、切合实际、可执行的漏洞风险处置建议；输出《渗透测试报告》、《渗透测试复测报告》等服务交付物；	（4）我公司负责编写渗透测试报告并提交给学校，报告阐明学校业务系统中存在的安全隐患以及专业、切合实际、可执行的漏洞风险处置建议；输出《渗透测试报告》、《渗透测试复测报告》等服务交付物；	无偏离	满足招标参数要求	无
		（5）要求服务频次：不低于20个应用系统；	（5）服务频次：20个应用系统；	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		（6）要求服务商至少 2 名工程师具备中国信息安全测评中心认证的注册渗透测试工程师（CISP-PTE）证书，提供工程师证书和所在供应商连续半年的社保证明材料；	（6）我公司具有并提供 2 名工程师具备中国信息安全测评中心认证的注册渗透测试工程师（CISP-PTE）证书，响应文件中后附工程师证书和连续半年的社保证明材料；	无偏离	满足招标参数要求	无
		9.★重保支持服务：	9.重保支持服务：	无偏离	满足招标参数要求	无
		（1）要求服务商在国家或行业重要会议、活动期间，网络安全保障技术支持，包含重保前的摸底加固、重保中的监测响应、重保后的总结改进；	（1）我公司在国家或行业重要会议、活动期间，网络安全保障技术支持，包含重保前的摸底加固、重保中的监测响应、重保后的总结改进；	无偏离	满足招标参数要求	无
		（2）要求服务商提供 20 天的 7*24 小时技术支持，含漏洞发现、安全加固、威胁发现、应急处置等；	（2）我公司提供 20 天的 7*24 小时技术支持，含漏洞发现、安全加固、威胁发现、应急处置等；	无偏离	满足招标参数要求	无
		（3）要求服务商至少 3 名工程师具备中国信息安全测评中心认证的注册信息安全专业人员（CISP）证书，提供工程师证书和所在供应商连续半年的社保证明材料；	（3）我公司具有并提供 3 名工程师具备中国信息安全测评中心认证的注册信息安全专业人员（CISP）证书，响应文件中后附工程师证书和连续半年的社保证明材料；	无偏离	满足招标参数要求	无
		10.备份容灾数据恢复演练服务：要求服务商提供业务数据备份策略优化；对要备份的数据进行分类，提供数据备份的流程和数据安全管理的制度，最大程度保证在真正数据灾难发生时，能顺畅的进行应对，最大化减少损失；容灾演练次数：1 次/年；演练和验证完毕后，出具《备份数据恢复演练报告》；	10.备份容灾数据恢复演练服务：我公司提供业务数据备份策略优化；对要备份的数据进行分类，提供数据备份的流程和数据安全管理的制度，最大程度保证在真正数据灾难发生时，能顺畅的进行应对，最大化减少损失；容灾演练次数：1 次/年；演练和验证完毕后，并出具《备份数据恢复演练报告》；	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		11. 网站探测和梳理服务：提供校园网运行网站发现和资产梳理，识别双非资产和僵尸资产，提升校园网资产运营能力。频率：2 次/年，出具《网站资产报告》；	11. 网站探测和梳理服务：提供校园网运行网站发现和资产梳理，识别双非资产和僵尸资产，提升校园网资产运营能力。频率：2 次/年，出具《网站资产报告》；	无偏离	满足招标参数要求	无
3	安全运营监测服务	1. 提供数据中心资产（IP）数量≥60 个的安全托管服务。设备管理和维护：为保障设备正常运转，服务人员每日巡检流量采集状况、存储情况、授权、规则和情报更新状态等，避免故障和异常影响设备威胁检测能力。为保障设备安全监测能力，服务人员定期对设备进行威胁情报、规则库进行更新，对系统进行版本升级。为保障云端运营平台及服务工具正常运转，日常巡检发现设备故障后，服务人员协调跟踪产品售后人员对设备进行故障修复；	1. 提供数据中心资产（IP）数量 60 个的安全托管服务。设备管理和维护：为保障设备正常运转，服务人员每日巡检流量采集状况、存储情况、授权、规则和情报更新状态等，避免故障和异常影响设备威胁检测能力。为保障设备安全监测能力，服务人员定期对设备进行威胁情报、规则库进行更新，对系统进行版本升级。为保障云端运营平台及服务工具正常运转，日常巡检发现设备故障后，服务人员协调跟踪产品售后人员对设备进行故障修复；	无偏离	满足招标参数要求	无
		2. 服务资产管理：每季度协助客户更新监测资产的台账，提供告警、资产关联分析能力；	2. 服务资产管理：每季度协助客户更新监测资产的台账，提供告警、资产关联分析能力；	无偏离	满足招标参数要求	无
		3. 持续漏洞利用情况监测：利用云端安全运营平台持续监测客户处漏洞利用情况，对监测发现的安全漏洞进行验证分析和跟踪整改情况；	3. 持续漏洞利用情况监测：利用云端安全运营平台持续监测客户处漏洞利用情况，对监测发现的安全漏洞进行验证分析和跟踪整改情况；	无偏离	满足招标参数要求	无
		4. 资产漏洞预警：结合厂商漏洞监测平台信息，通过沟通群对客户资产漏洞进行预警；	4. 资产漏洞预警：结合厂商漏洞监测平台信息，通过沟通群对客户资产漏洞进行预警；	无偏离	满足招标参数要求	无
		5. 漏洞修复指导：对监测发现的客户处漏洞进行分析，提供可落地专业漏洞修复指导；	5. 漏洞修复指导：对监测发现的客户处漏洞进行分析，提供可落地专业漏洞修复指导；	无偏离	满足招标参数要求	无
		6. 漏洞确认：对用户服务内资产，监测发现的	6. 漏洞确认：对用户服务内资产，监测发现的	无偏离	满足招标	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		漏洞远程进行研判确认；	漏洞远程进行研判确认；		参数要求	
		7.流量威胁检测：提供威胁检测响应工具，对网络内流量进行检测，包括网页漏洞利用情况检测、网络攻击检测、webshell 检测、威胁情报检测（APT、恶意软件）等；	7.流量威胁检测：提供威胁检测响应工具，对网络内流量进行检测，包括网页漏洞利用情况检测、网络攻击检测、webshell 检测、威胁情报检测（APT、恶意软件）等；	无偏离	满足招标参数要求	无
		8.提供 7*24 安全威胁监测：服务人员通过云端托管运营平台提供7*24安全威胁监测服务，持续监测网络内的安全隐患情况并进行分析，包括对外部网络攻击网络漏洞利用情况、恶意软件活动情况、以及内网安全情况；	8.提供 7*24 安全威胁监测：服务人员通过云端托管运营平台提供 7*24 安全威胁监测服务，持续监测网络内的安全隐患情况并进行分析，包括对外部网络攻击网络漏洞利用情况、恶意软件活动情况、以及内网安全情况；	无偏离	满足招标参数要求	无
		9.主动响应分析：服务人员综合所发现的安全事件、攻击情况，评价客户侧整体网络安全态势，包括但不限于告警趋势分析、威胁类型分布分析、安全事件分析等；	9.主动响应分析：服务人员综合所发现的安全事件、攻击情况，评价客户侧整体网络安全态势，包括但不限于告警趋势分析、威胁类型分布分析、安全事件分析等；	无偏离	满足招标参数要求	无
		10.安全事件通告：服务人员对安全监测发现的安全隐患及事件在服务规定时间内进行通告，同时根据客户需求每日同步安全情况；	10.安全事件通告：服务人员对安全监测发现的安全隐患及事件在服务规定时间内进行通告，同时根据客户需求每日同步安全情况；	无偏离	满足招标参数要求	无
		11.威胁抑制/阻断：建立工作群，实时推送封禁信息，包括高频攻击源、恶意软件 IOC、内外交互的恶意链接等，协助客户进行封禁，阻止进一步攻击；	11.威胁抑制/阻断：建立工作群，实时推送封禁信息，包括高频攻击源、恶意软件 IOC、内外交互的恶意链接等，协助客户进行封禁，阻止进一步攻击；	无偏离	满足招标参数要求	无
		12.入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务；	12.入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务；	无偏离	满足招标参数要求	无
		13.事件跟踪管理：对事件处置过程进行跟踪	13.事件跟踪管理：对事件处置过程进行跟踪形	无偏离	满足招标	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		形成闭环，在实战中不断加固，协助推动用户建立可行的事件处置流程；	成闭环，在实战中不断加固，协助推动用户建立可行的事件处置流程；		参数要求	
		14. 运营汇报及解读：安排资深专家在线进行运营情况汇报，进行威胁分析情况解读，并进行疑难解答；	14. 运营汇报及解读：安排资深专家在线进行运营情况汇报，进行威胁分析情况解读，并进行疑难解答；	无偏离	满足招标参数要求	无
		15. 安全运营问题解答：通过沟通群等方式对安全运营中的产品问题、安全分析问题进行解答，协助进行问题解决；	15. 安全运营问题解答：通过沟通群等方式对安全运营中的产品问题、安全分析问题进行解答，协助进行问题解决；	无偏离	满足招标参数要求	无
		16. 服务交付物要求： 交付物名称：《安全运营周报》，报告频率：每周一次； 交付物名称：《首次威胁分析报告》，报告频率：一次； 交付物名称：《安全事件报告》，报告频率：按需触发，不限次数； 交付物名称：《安全通告》，报告频率：按需触发，不限次数； 交付物名称：《安全运营月报》，报告频率：每月一次； 交付物名称：《年度汇报 PPT》，报告频率：每年一次；	16. 服务交付物： 交付物名称：《安全运营周报》，报告频率：每周一次； 交付物名称：《首次威胁分析报告》，报告频率：一次； 交付物名称：《安全事件报告》，报告频率：按需触发，不限次数； 交付物名称：《安全通告》，报告频率：按需触发，不限次数； 交付物名称：《安全运营月报》，报告频率：每月一次； 交付物名称：《年度汇报 PPT》，报告频率：每年一次；	无偏离	满足招标参数要求	无
		17. 数据保密要求：要求本服务工具支持将收集的安全日志以加密通道上传到安全服务云平台上，并支持在该平台上对服务工具进行管	17. 数据保密：本服务工具支持将收集的安全日志以加密通道上传到安全服务云平台上，并支持在该平台上对服务工具进行管理；	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		理；				
4	网络安全能力服务	1. 要求提供面向全省开放大学师生定制化的网络安全培训，培训频率：按需服务；	1. 提供面向全省开放大学师生定制化的网络安全培训，培训频率：按需服务；	无偏离	满足招标参数要求	无
		2. 要求提供专为学校 IT 管理人员设计的技术培训，包括最新网络安全技术和解决方案；培训与考试频率：按需提供，满足不同专业人员的学习进度和需求；	2. 提供专为学校 IT 管理人员设计的技术培训，包括最新网络安全技术和解决方案；培训与考试频率：按需提供，满足不同专业人员的学习进度和需求；	无偏离	满足招标参数要求	无
		3. 要求提供网络安全能力认证的培训课程，以确保学校专业人员掌握最前沿的网络安全知识；培训方式：面授课程或在线学习，并提供模拟考试平台；频率：按需服务；	3. 提供网络安全能力认证的培训课程，以确保学校专业人员掌握最前沿的网络安全知识；培训方式：面授课程或在线学习，并提供模拟考试平台；频率：按需服务；	无偏离	满足招标参数要求	无
		4. 要求根据学校需求，提供网络安全态势分析报告，便于学校管理层了解当前网络安全形势。组织网络安全专家座谈会，分享最新的网络安全趋势、案例分析和应对策略。座谈频率：按需提供，确保学校管理层及时获取网络安全动态；	4. 根据学校需求，提供网络安全态势分析报告，便于学校管理层了解当前网络安全形势。组织网络安全专家座谈会，分享最新的网络安全趋势、案例分析和应对策略。座谈频率：按需提供，确保学校管理层及时获取网络安全动态；	无偏离	满足招标参数要求	无
		5. 要求提供网络安全宣传周的网络安全宣传支持：网络安全周期间使用的文字、音视频材料、展板等相关支持；	5. 提供网络安全宣传周的网络安全宣传支持：网络安全周期间使用的文字、音视频材料、展板等相关支持；	无偏离	满足招标参数要求	无
		6. ★为保障学校网络安全能力的有效提升和加强，要求服务商至少具备 1 名网络安全能力认证（CCSC）培训讲师，提供讲师证书和所在供应商连续半年的社保证明材料。	6. 为保障学校网络安全能力的有效提升和加强，我公司具备并提供 1 名网络安全能力认证（CCSC）培训讲师，响应文件中后附讲师证书和连续半年的社保证明材料。	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
5	等级保护测评服务	1.等级保护备案工作：完成《信息系统安全等级保护备案表》的整理和公安部门的报备；	1.等级保护备案工作：完成《信息系统安全等级保护备案表》的整理和公安部门的报备；	无偏离	满足招标参数要求	无
		2.完成学校不少于50个子系统7个系统的二级等级保护测评工作，及时发现系统存在的安全风险，并对存在的安全风险进行加固整改，同时取得公安部门系统备案证明；	2.完成学校50个子系统7个系统的二级等级保护测评工作，及时发现系统存在的安全风险，并对存在的安全风险进行加固整改，同时取得公安部门系统备案证明；	无偏离	满足招标参数要求	无
		3.投标人必须遵循但不限于以下等级保护国家标准政策法规：要求与《信息安全等级保护管理办法》（公通字[2007]43号）、《信息系统安全等级保护实施指南》（信安字[2007]10号）和《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号）（含附件）等公安部信息安全等级保护系列文件要求保持一致。符合以下要求：《信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术 网络安全等级保护定级指南》（GB/T22240-2020）、《信息安全技术 网络安全保护等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全保护等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全保护等级保护安全设计技术要求》（GB/T25070-2019）、《信息安全技术 网络安全等级保护测评过程指南》	3.我公司遵循但不限于以下等级保护国家标准政策法规：与《信息安全等级保护管理办法》（公通字[2007]43号）、《信息系统安全等级保护实施指南》（信安字[2007]10号）和《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号）（含附件）等公安部信息安全等级保护系列文件要求保持一致。符合以下要求：《信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术 网络安全等级保护定级指南》（GB/T22240-2020）、《信息安全技术 网络安全保护等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全保护等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全保护等级保护安全设计技术要求》（GB/T25070-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）、《信息安全技术 网络安全等级保护测试评估	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		（GB/T28449-2018）、《信息安全技术 网络安全等级保护测试评估技术指南》(GB/T36627-2018）、《信息系统安全等级测评报告模板》（公安部 2019 版）、《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]429 号）、《信息安全等级保护管理办法》（公通字[2007]43 号）、《信息安全技术 网络基础安全基础要求》（GB/T20270-2006）、《信息安全技术 信息系统通用安全技术要求》(GB/T20271-2006)、《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）、《信息安全风险评估规范》（GB/T 20984-2007）、《信息技术安全性评估准则》（GB/T 18336-2001）、《教育行业信息系统安全等级保护定级工作指南》等。	技术指南》(GB/T36627-2018）、《信息系统安全等级测评报告模板》(公安部 2019 版)、《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]429 号）、《信息安全等级保护管理办法》（公通字[2007]43 号）、《信息安全技术 网络基础安全基础要求》（GB/T20270-2006）、《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）、《信息安全风险评估规范》(GB/T 20984-2007)、《信息技术安全性评估准则》（GB/T 18336-2001）、《教育行业信息系统安全等级保护定级工作指南》等。			
		4.安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；	4.安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；	无偏离	满足招标参数要求	无
		5.安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评；	5.安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评；	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		6.系统整体测评：安全控制点间、层面间、区域间、系统结构安全等四个方面的安全测评；	6.系统整体测评：安全控制点间、层面间、区域间、系统结构安全等四个方面的安全测评；	无偏离	满足招标参数要求	无
		7.在安全等级测评过程中，每个工作阶段、流程、内容、及成果交付要严格遵循《信息安全技术网络安全保护等级保护测评要求》（GB/T28448-2019）和《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告，测评报告需得到学校的确认，测评报告编制的内容及格式严格遵照《信息系统安全等级测评报告模版》（公安部2019版）进行；	7.在安全等级测评过程中，每个工作阶段、流程、内容、及成果交付要严格遵循《信息安全技术网络安全保护等级保护测评要求》（GB/T28448-2019）和《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告，测评报告要得到学校的确认，测评报告编制的内容及格式严格遵照《信息系统安全等级测评报告模版》（公安部2019版）进行；	无偏离	满足招标参数要求	无
		8.安全整改：依照《信息安全技术 网络安全等级保护安全设计技术要求》的要求，在系统测评工作的基础上，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全建设整改建议方案，并协助指导完成整改工作。	8.安全整改：依照《信息安全技术 网络安全等级保护安全设计技术要求》的要求，在系统测评工作的基础上，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全建设整改建议方案，并协助指导完成整改工作。	无偏离	满足招标参数要求	无
6	堡垒机授权服务	1.由于堡垒机（安恒DAS-USM1800）设备授权数量已经到达上限，管理不能再添加新设备，现需要扩充300点授权；	1.由于堡垒机（安恒DAS-USM1800）设备授权数量已经到达上限，管理不能再添加新设备，现扩充300点授权；	无偏离	满足招标参数要求	无
		2.要求提供售后服务承诺函。	2.响应文件中后附售后服务承诺函。	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
7	上网行为管理系统续保服务	1.提供三年工程师上门服务，三年 7*24 小时远程技术支持服务（含现场升级服务），400 电话支持服务；	1.提供三年工程师上门服务，三年 7*24 小时远程技术支持服务（含现场升级服务），400 电话支持服务；	无偏离	满足招标参数要求	无
		2.提供三年软件升级和 URL&应用识别规则库升级，提供硬件设备同等功能软件版本更新、升级，以及该软件版本配套的文档资料、用户手册。升级后用户将享有新版本软件的使用权利。	2.提供三年软件升级和 URL&应用识别规则库升级，提供硬件设备同等功能软件版本更新、升级，以及该软件版本配套的文档资料、用户手册。升级后用户将享有新版本软件的使用权利。	无偏离	满足招标参数要求	无
		3.要求提供售后服务承诺函。	3.响应文件中后附售后服务承诺函。	无偏离	满足招标参数要求	无
8	数据中心防火墙续保服务	1.提供三年工程师上门服务，三年 7*24 小时远程技术支持服务（含现场升级服务），400 电话支持服务；	1.提供三年工程师上门服务，三年 7*24 小时远程技术支持服务（含现场升级服务），400 电话支持服务；	无偏离	满足招标参数要求	无
		2.提供三年软件升级，提供硬件设备同等功能软件版本更新、升级，以及该软件版本配套的文档资料、用户手册。升级后用户将享有新版本软件的使用权利；	2.提供三年软件升级，提供硬件设备同等功能软件版本更新、升级，以及该软件版本配套的文档资料、用户手册。升级后用户将享有新版本软件的使用权利；	无偏离	满足招标参数要求	无
		3.提供三年规则库升级，包括 WEB 应用防护识别库、IPS 特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和 URL&应用识别库升级，保持设备具备检测防御最新威胁的能力；	3.提供三年规则库升级，包括 WEB 应用防护识别库、IPS 特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和 URL&应用识别库升级，保持设备具备检测防御最新威胁的能力；	无偏离	满足招标参数要求	无
		4.要求提供售后服务承诺函。	4.响应文件中后附售后服务承诺函。	无偏离	满足招标参数要求	无
9	动力环	1.机房动环监控管理系统对机房的基础环境	1.机房动环监控管理系统对机房的基础环境各	无偏离	满足招标	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
	境监控系统	各个子系统监控接入统一管理平台，实现7*24H*365天的全面集中监控和管理，保障中心机房内各设备及子系统的安全运行。监控内容包括机房动力、环境、安防、集成第三方设备等基础设施的集中监控。集中管理平台通过手机短信等方式告警，及时通知机房管理人员机房基础运维环境的运行状态或报警情况；	个子系统监控接入统一管理平台，实现7*24H*365天的全面集中监控和管理，保障中心机房内各设备及子系统的安全运行。监控内容包括机房动力、环境、安防、集成第三方设备等基础设施的集中监控。集中管理平台通过手机短信等方式告警，及时通知机房管理人员机房基础运维环境的运行状态或报警情况；		参数要求	
		2.监控内容要求：配置1套机房动力环境监控系统（1台工业级监控服务器、1台数据采集服务器、12个温湿度传感器、4套漏水控制器及配套感应线缆、2套供配电软件接口、2套列头柜软接口、1套UPS软件接口、4套精密空调软件接口、1套漏水软件接口、1套温湿度软件接口、1套消防软件接口、1套远程浏览软件接口、1套短信告警系统）；	2.监控内容：配置1套机房动力环境监控系统（1台工业级监控服务器、1台数据采集服务器、12个温湿度传感器、4套漏水控制器及配套感应线缆、2套供配电软件接口、2套列头柜软接口、1套UPS软件接口、4套精密空调软件接口、1套漏水软件接口、1套温湿度软件接口、1套消防软件接口、1套远程浏览软件接口、1套短信告警系统）；	无偏离	满足招标参数要求	无
		3.软件要求：软件采用B/S+C/S架构，模块化设计，采用3D技术构建数据中心整个区域效果展示，可对整个数据中心的各设备的运行状态进行依次巡检，循环执行，实现可视化管理；以图形化的方式实现对设备实时数据和状态的监控，并进行远程设置，系统主界面包含所有子系统内监控设备的视图，可直接点击子系统内的任意监控设备进入其运行状态界面。通过软件界面应可直观展示机房整体视图，包括	3.软件：软件采用B/S+C/S架构，模块化设计，采用3D技术构建数据中心整个区域效果展示，可对整个数据中心的各设备的运行状态进行依次巡检，循环执行，实现可视化管理；以图形化的方式实现对设备实时数据和状态的监控，并进行远程设置，系统主界面包含所有子系统内监控设备的视图，可直接点击子系统内的任意监控设备进入其运行状态界面。通过软件界面应可直观展示机房整体视图，包括机房分区、	无偏离	满足招标参数要求	无

序号	名称或条款号	技术规格或系统功能要求		对磋商文件偏离	描述	备注
		磋商文件	响应文件			
		机房分区、设备布局等。系统具有强大的报警级别管理功能，可区分5级报警，当系统出现报警时，可根据不同监控对象报警事件而划分不同的报警方式，包括划分报警等级、时间优先、次数频率等，在监控中心可以以不同颜色和声音对报警事件进行区分。支持关键设备集中展示功能，可以在一个页面上组合若干重要设备的参数；同时监控软件还可通过曲线、指针、仪表等多种方式展示监控数据。同时软件平台可自定义展示窗口数量和随意拉动窗口大小；	设备布局等。系统具有强大的报警级别管理功能，可区分5级报警，当系统出现报警时，可根据不同监控对象报警事件而划分不同的报警方式，包括划分报警等级、时间优先、次数频率等，在监控中心可以以不同颜色和声音对报警事件进行区分。支持关键设备集中展示功能，可以在一个页面上组合若干重要设备的参数；同时监控软件还可通过曲线、指针、仪表等多种方式展示监控数据。同时软件平台可自定义展示窗口数量和随意拉动窗口大小；			
		4.提供权威机构出具的“集中监控平台”软件产品登记测试报告及著作权证明扫描件；	4.响应文件中后附权威机构出具的“集中监控平台”软件产品登记测试报告及著作权证明扫描件；	无偏离	满足招标参数要求	无
		5.★为确保动环厂商对UPS进行协议开发的兼容性，“UPS监测子系统软件”须通过中国软件评测中心出具的软件产品登记测试报告扫描件；	5.为确保动环厂商对UPS进行协议开发的兼容性，“UPS监测子系统软件”已通过中国软件评测中心出具的软件产品登记测试报告，响应文件中后附扫描件；	无偏离	满足招标参数要求	无
		6.要求提供三年售后服务承诺函扫描件。	6.响应文件中后附三年售后服务承诺函扫描件。	无偏离	满足招标参数要求	无

附件 3、中标通知书

成 交 通 知 书

采购编号：豫财磋商采购-2024-164

成交人		河南合众信泰科技有限公司
项目名称		郑州信息科技职业学院网络安全建设及设备续保服务项目
成交范围		详见磋商文件
采购人		郑州信息科技职业学院
采购方式		竞争性磋商
成交内容	成交金额（元）	大写：人民币贰佰叁拾柒万陆仟元整
		小写： 2376000.00 元
	服务期限	一次性建设内容在合同签订后 30 日历天内完成交付；服务类内容在合同签订后 30 日历天内完成服务前准备，并从正式服务日期起计算
	质量保证期	驻场服务、风险评估及保障服务、安全运营监测服务、网络安全能力服务、等级保护测评服务运维周期为 2 年，上网行为管理系统续保服务和数据中心防火墙续保服务软件续保服务为 3 年，动力环境监控系统质保期为 3 年。
	服务要求	符合国家或行业规定的合格标准，满足采购人提出的技术标准及要求

根据 郑州信息科技职业学院网络安全建设及设备续保服务项目 采购文件和你公司于 2024 年 04 月 22 日提交的响应文件，经磋商小组按照磋商文件确定的评审标准和方法，已完成评审和成交公告，确定你公司成交。请收到本通知书后 15 日内，与采购人签订合同。

代理机构：（盖章）

2024 年 04 月 22 日