河南对外经济贸易职业学院信息安全提升建设及信息服务项目合同

甲方： 河南对外经济贸易职业学院

乙方：河南小鹰网络科技有限公司

甲乙双方根据 2026 年 3 月 24 日项目编号为 豫财磋商采购-2026-83 的磋商文件和响应文件，并经协商一致，在平等互利的基础上，就河南对外经济贸易职业学院信息安全提升建设及信息服务项目达成以下条款：

一、 声明

磋商文件及磋商响应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。

二、 合同总价及设备清单

合同总金额： 壹佰万零玖仟陆佰 （大写）（￥： 1009600 元）。

清单见附件 1："河南对外经济贸易职业学院信息安全提升建设及信息服务项目设备清单"、

规格见附件 2："河南对外经济贸易职业学院信息安全提升建设及信息服务项目项目设备技术规格表"

。

三、 项目建设要求：

1. 签订合同之日起 30 历日内完成交货、安装调试完毕，并完成验收。

2. 交货地点：供方按需方指定地点 采购人指定地点 将货物免费送达。供方或最终用户(包括供方或最终用户的工作人员)填写收货确认单，或者在乙方的物流配送单据上予以签字或盖章，结合验收报告等作为双方结算的依据。

3. 乙方必须按合同提供原厂全新设备（包括零部件），并符合国家以及该产品的出厂标准（以合格证为准），并负责可能的缺陷弥补。乙方提供的产品与合同要求的品牌、型号、规格、产地必须一致，交货时出具原产地证明及合格出厂证明（合格证）。

4. 产品运输过程中由供方按国家有关设备供应的规定标准进行包装、供应，产生的相关费用由供方承担。

5. 供方应在交货时向需方提供设备使用说明书、合格证及相关的随机备品备件、配件、工具等资料。

6. 乙方承诺保证提供的货物均为符合专利权、商标权、著作权或其他知识产权的正规渠道产品，并免受第三方提出的侵犯其专利权、商标权、著作权或其他知识产权的起诉。如果受到第三方起诉，其一切法律后果应由乙方承担。

7. 乙方负责保修期内产品设备的正确安装保证及定期保养等正常运转保证，在产品使用寿命期内须具有符合质量要求和产品说明书提供的性能。在货物质量保证期之内，乙方须对由于设计、工艺或材料的缺陷等而发生的任何不足或故障负责。设备一年开机率保持在95%（含）以上。设备保修期内，设备维修占用日期每增加一天按维修时间往后顺延七天。

四、 货物验收

1. 货物到达指定地点后，甲方根据合同要求，确认货物产地、规格、型号和数量。安装调试后，乙方先自检，调试运行稳定后报甲方进行验收。

2. 乙方所交的货物安装、调试完毕及时向甲方提出验收申请，甲方在收到乙方验收申请后组织验收。甲方无正当理由拒验且无相关说明文件，应视为验收合格。

3. 验收合格后，甲方出具验收报告。

五、 付款方式

1. 乙方向甲方开具增值税普通发票。

2. 合同签订生效后，甲方验收合格并正常运行后，支付乙方合同价 100% ，合计人民币：壹佰万零玖仟陆佰元。

付款信息如下：

乙方银行开户名称：河南小鹰网络科技有限公司

乙方开户银行名称：中信银行郑州润华支行

乙方开户银行账号：8111101013000833368

统一社会信用代码：91410105MA45BEJ082

六、 售后服务

1. 项目整体质保期为 3 年，维护服务标准为故障响应不超过 1 小时，到达现场不超过 5 小时，保障故障排除时间不超过 1 小时；设备质保期内，如果在 4 小时内无法修复的应当提供同等型号备用设备；对设备的易损件拥有库存备件，保证用户的备件及时供应。设备质保 3 年（自验收通过之日起），使用过程中出现问题 1 小时内到现场服务；质保期外提供相关承诺。

2. 乙方售后服务违约情况达到或超过 3 次时，甲方可向乙方发出违约通知单，乙方应在 5 个工作日纠正所有违约行为，并提供有效售后服务方案，乙方未能按时响应并纠正违约行为的，甲方有权申请执行

全额履约保函，并保留采取法律措施追究乙方违约责任的权利。

七、 法律责任

1. 乙方所交的货物品种、品牌、型号、规格、质量等，若不符合本合同文件的规定，甲方有权拒收设备，乙方应在本合同规定的交货期内负责更换并承担因更换而支付的费用。因更换而造成的逾期交货，则按逾期交货处理。

2. 除受不可抗力事件(诸如战争、严重火灾、洪水、台风、地震等)的影响外，如果乙方没有按照合同规定的时间交货和提供服务，甲方可从合同价中扣除误期赔偿费。每延误一天的赔偿费按迟交货物交货价或未提供服务的服务费用的百分之一(1%)计收，直至交货或提供服务为止。一旦误期满 10 个日历天，甲方有权终止合同。

3. 甲方无正当理由拒收设备，每延误壹周应向乙方支付无正当理由拒收设备金额百分之零点五（0.5%）的违约金，违约金的最高限额为合同价格的百分之五(5%)。一旦达到违约金最高限额，乙方有权终止合同。

4. 因乙方原因造成逾期付款，甲方不承担责任。

5. 因设备质量问题发生的争议，以本合同条款为标准协商解决，若协商无果，任何一方均可向合同签订地的人民法院提起诉讼。

八、 合同生效及其它

本合同经双方法定代表人或委托代理人签字并加盖公章后生效。本合同壹式 伍 份，甲方 叁 份、乙方 贰 份。

九、 其他

1. 未尽事宜，由双方协商解决，签订补充协议，与本合同同样具有法律效力。

2. 本合同执行期间，如果发生纠纷，双方协商解决。如协商不成，双方可到合同签订地人民法院诉讼解决。

甲方：河南对外经济贸易职业学院

（盖章）

甲方委托代理人：

电话：

签约时间： 2026 年 4 月 16 日

签约地址：

乙方：河南小鹰网络科技有限公司

（盖章）

乙方委托代理人：

电话：

附件 1 河南对外经济贸易职业学院信息安全提升建设及信息服务项目设备清单

单位：元

序号	设备名称	品牌	型号	单位	数量	单价	总价
1	核心交换机	H3C	H3C S7510X	台	1	152900	152900
2	汇聚交换机	H3C	S6520X-30QC-EI	台	2	20500	41000
3	下一代防火墙（核心产品）	深信服	AF-2000-FH2350A-ID	台	1	168000	168000
4	安全托管服务	深信服	安全托管服务 MSS-10	套	1	74800	74800
5	安全探针系统	深信服	STA-100-B2100	台	1	81700	81700
6	超融合云平台升级	深信服	超融合云平台升级	年	1	74500	74500
7	终端安全接入授权扩容	深信服	统一端点安全管理系统 V6.0	套	1	102000	102000
8	4K 高清视频终端及高清图像编解码器	DVISION	DVISION FOCUS 4900	套	1	49000	49000
9	超高清解码器	海康威视	DS-6A10UD	台	1	19500	19500
10	会议系统安装实施以及线缆及辅材	定制	定制	项	1	4900	4900
11	教育网视频会议网元租金	定制	定制	年	1	24500	24500
12	信息化技术运维服务	定制	定制	项	1	205400	205400
13	云桌面管理软件	北京和信	和信下一代云桌面系统 V4.0	个	38	300	11400
总计		小写：1009600 元 大写：壹佰万零玖仟陆佰元整					

附件 2：河南对外经济贸易职业学院信息安全提升建设及信息服务项目设备技术规格表

编号	产品名称	技术参数
1	核心交换机	1、交换容量 200Tbps，包转发率 115000Mpps；采用全宽主控设计，配置双主控引擎。整机交换网板槽位数 2，业务板槽位数 10。主控引擎、风扇、电源等关键部件冗余。所有业务板、引擎、风扇、电源模块均支持热插拔；
		2、为保障后续可扩展性，支持 10GEPON 功能；MAC 地址表容量 1M，ARP 表项容量 256K；支持 VXLAN，能够实现基于 IPv4/IPv6 的 VXLAN 二层及三层网关功能（支持集中式与分布式网关模式）。支持 MPLS L2VPN（VPLS、VPWS）、MPLS L3VPN、MPLS-TE 及 MCE 功能；
		3、为提高网络健壮性，实现统一管理，设备支持 4 框虚拟化技术；支持将一台物理交换机划分为多台逻辑独立的虚拟交换机，并支持虚拟交换机的创建、删除、物理端口/板卡资源动态划分；
		4、支持融合 AC 功能，无需额外配置单独硬件，在交换机上实现对 AP 的接入控制和管理，有线无线用户的统一认证管理；为提升网络可靠性，设备支持 RRPP 和 ERPS 标准环网协议，实现毫秒级故障收敛，并支持双向故障检测与倒换。
		5、支持真实业务流的实时检测技术，能够对业务报文进行标记和统计，实现网络级与设备级的时延、丢包率等指标的精准测量；为保证产品满足未来 3 至 5 年可扩展性，设备单槽位支持端口密度 24 个 40G 接口的业务板卡，支持多业务融合板卡，能够实现对摄像头等物联终端统一识别、认证和管理；
		6、本实配千兆电接口 24 个、万兆光接口 28 个、40G 光接口 2 个、万兆单模光模块 12 个、40G 多模光模块 4 个、40G 堆叠线缆 2 根；为保证产品安全可靠，交换机具备网络关键设备检测证书。
		7、此次购买核心交换机是为提高智慧教室网络网络稳定性，解决单点故障问题，能与原有核心交换机 S7510X 堆叠互联。
2	汇聚交换机	1、交换容量 2.5Tbps，包转发率 720Mpps，以官网所列最低参数为准；设备采用模块化双电源、双风扇设计，支持风扇热插拔与电源冗余；风道设计支持前后或后前通风，符合标准散热风道；提供 10GE 光接口 24 个，40G 光接口 2 个，扩展插槽 2 个；配置同品牌原厂原装万兆多模光模块 4 个、万兆单模光模块 4 个。
		2、支持 IPv4 和 IPv6 环境下的策略路由，支持 IPv6 静态路由、RIPng、OSPFv3、ISISv6、BGP4+；可根据需要灵活扩展端口，能够支持防火墙插卡、端口扩展板卡等不同种类的业务插卡；
		3、支持安全启动，在系统启动过程中支持安全检测，防止对系统镜像进行修改和伪造数据；支持 VxLAN 二层网关、集中式网关及基于 EVPN 的分布式三层网关；
		4、支持堆叠技术，堆叠台数 4 台，具备堆叠分裂检测与自动修复机制，分裂后能自动完成 MAC/IP 地址收敛；支持基于第二层、第三层和第四层的 ACL，支持出入方

		向、端口及 VLAN 的 ACL 绑定，以便于灵活实现数据包过滤；
		5、支持智能网络质量分析技术，可快速测量网络性能的检测机制，直接对业务报文进行测量，测量数据可以真实反映网络质量状况，实时感知丢包时间、丢包位置、丢包数量；
3	下一代防火墙（核心产品）	1、性能要求：吞吐量：网络层吞吐量 40Gbps，应用层吞吐量 25Gbps，IPS 吞吐量 4Gbps；连接数：HTTP 新建连接数 19 万 CPS，并发连接数 420 万;硬件要求：规格 2U;内存 16GB;硬盘容量 128GSSD+480GSSD;接口 16 个千兆电口+6 个万兆光口 SFP+;冗余电源；提供 3 年维保服务。
		2、产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上。产品具备独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略。
		3、内置漏洞特征规则库 15,000 条，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则。
		4、产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 128 万种，可识别主机的异常外联行为；产品支持 Cookie 防篡改攻击防护，并能记录相关攻击日志。
		5、产品支持云威胁情报网关技术，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。
		6、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；产品支持基于网络区域、网络对象、MAC 地址、服务、应用等维度进行访问控制策略设置。
		7、产品支持与学校现有态势感知平台（SIP-1000-B400）联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。
		8、产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持 3 种的调度算法，包括带宽比例、加权流量、线路优先等。
		9、为实现更好的防护效果，产品支持与学校现有的统一端点安全管理系统（aES 6.0.2R4）联动管理，可在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理，支持检测到某主机有僵木蠕毒的 C2 通信时，手动或自动化将恶意域名信息下发到终端安全软件做 C2 通信的封锁遏制，支持管理员下发一键隔离指令，对终端恶意文件进行隔离。
		10、支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息。
4	安全托管服务	1、我方为招标方 10 项核心资产（包括但不限于 IP 地址、域名、云主机实例）提供为期 1 年的安全托管运营服务。通过“人机共智”模式，整合云端安全运营中心、招标方现有安全态势感知平台及专业安全专家团队，建立持续化、主动化、闭环化

		的安全运营体系。
		2、我方使用安全工具对招标方服务资产开展互联网暴露面探测，全面梳理资产互联网开放状况，及时发现违规暴露资产及关联风险，协助处置并确保暴露面资产可管可控；针对服务范围内资产扫描到的高危可利用漏洞，我方为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失。
		3、我方具备云端检测和分析平台，通过采集招标方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标方提供 7*24 小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；提供云端服务平台告警审核功能界面截图，举证一个告警聚合分析的例子和一个告警详情展示具备上述能力。
		4、为了保证安全监测的准确率和服务质量，我方支持为招标方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求；安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。提供一份完整威胁情报处置工单示例，工单内容包含威胁情报的基本信息、推送信息和跟进记录。
		5、我方安全专家每月对招标方的安全设备的防护策略进行检查，确保安全设备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。我方云端服务平台应当具备丰富的策略检查工具（40 种策略检查的工具），支持排查安全设备防护策略配置的合理性。
		6、我方为招标方提供在线安全值守服务，包括夜间、周末及法定节假日。节假日期间每日为招标方提供《节假日值守总结》。
		7、为了降低招标方因网络安全事件造成的损失和影响，我方按照以下服务指标和要求为招标方提供服务：（1）分析研判通知时效 MTTA：从安全日志上传分析研判到通告给招标方的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于 15 分钟，一般事件的通告时间少于 30 分钟。（2）我方承诺，服务范围内的所有安全事件的闭环处置比例达到 100%。（3）在具备我方的边界防护组件的情况下，要求招标方可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到 99%。（4）事件闭环时间 MTTR：经招标方授权后，我方服务人员协助进行安全事件的闭环，一般安全事件的闭环完成时间少于 8 小时，重大事件的闭环完成时间少于 24 小时。我方为招标方提供移动端服务过程展示门户（移动端 Portal），通过清晰可视化的风险消减图和漏洞消减图，让招标方清晰了解云端安全托管服务的风险消减机制，直观实时了解当前风险闭环情况。
		8、我方云端服务平台支持对接招标方网络中已部署的主要安全设备，支持实时接收安全设备检测到的安全事件信息、安全日志数据提供安全托管服务；提供云端服务平台支持对接的上述安全设备的能力证明，展示详细的对接步骤；为保护数据信息安全要求云端服务平台应当做好严格的安全防护，并严格按照《信息安全技术—网

		络安全等级保护基本要求》完成等级保护测评工作，服务平台至少通过等级保护三级测评；
5	安全探针系统	1、网络层吞吐 1Gbps，内存 8G，硬盘 128GminisataSSD，具备 8 千兆电口+2 万兆光口 ，提供 3 年质保服务。
		2、支持 IP，IP 组，服务，访问时间等定义违规访问策略，主动建立针对性的业务和应用访问逻辑规则，针对目标 IP（组）已开放的服务，白名单策略只允许白名单里的 IP（组）在指定的时间内访问，其他时间或其他 IP 的访问均被视为违规，黑名单策略禁止黑名单里的 IP（组）在指定的时间内访问，否则将被视为违规。
		3、支持包括命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测在内的多维度检测功能，支持自定义配置启用、高检出、低误报模式。
		4、支持检测出网络中的网络拓扑设备进行绘制，更直观可视化查看网络整体情况；支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。
		5、支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞、自定义 WAF 规则、WAF 云防护等网站攻击检测。
		6、支持 5 种场景的日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。
		支持将流量还原的文件发送至沙盒分析；可支持安天追影高级鉴定系统第三方沙盒对接；内置 IPS 漏洞特征识别库、应用识别库、WEB 应用防护库、僵尸网络识别库、实时漏洞分析识别库。
		7 可与学校现有的态势感知平台（SIP-1000-B400）对接，对接 SIP 时使用智能遥测模式，在不影响安全检测效果的情况下，削减 40%日志量，能够大幅削减直连时的探针设备数量，节省成本。
		8、支持僵尸网络行为检测功能，支持对 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等行为进行检测。
		9、支持上报型号信息，健康状态、安全策略信息，能够进一步提升服务效率，缩短客户选型和策略检测时间。
6	超融合云平台升级	1、超融合云平台升级服务 开封校区 8 台 aserver-R-2205 超融合一体机目前运行旧版管理软件（ID 号：20211027A0000763）升级至该产品系列官方发布的最新稳定版本超融合软件及管理平台，确保所有功能许可同步生效。全过程保证现有业务数据的安全性、完整性与一致性，最大限度减少或消除业务中断时间，制定完备的回退方案。对现有 8 节点超融合集群进行全面的健康状态检查、配置信息收集与拓扑分析。出具详细的《升

		级兼容性与风险评估报告》，明确升级路径、潜在风险及应对措施。制定详尽的《升级与数据迁移实施方案》，包括步骤、时间计划、回退预案、验证方案等，并经采购人确认。严格按照确认的方案执行升级操作，确保集群平台服务的高可用性。采用原厂认可或标准化的数据迁移技术，确保虚拟机、业务数据、网络配置、存储策略、用户权限等所有信息完整、准确地迁移至新版本平台。升级前后需对关键配置及数据进行备份，确保回退能力。处理升级过程中可能出现的任何兼容性、配置冲突等问题。完成升级后，进行全面的系统功能、性能及稳定性测试，确保所有业务负载正常运行。与采购人共同进行业务验证，签署《系统升级交付报告》。提供完整的《升级后系统架构文档》及《运维手册》。自项目最终验收合格之日起 1 年。在此期限内，对于因本次升级直接导致的系统软件缺陷或兼容性问题，服务商须提供免费、及时的修复服务。
		2、跨校区安全互联网络建设服务 在开封校区与郑州校区之间，通过双方现有及新增的防火墙设备，建立一条安全、稳定、可靠的 VPN 加密隧道，实现两校区网络可控互联。在此互通基础上，配置郑州校区探针，将其产生的全部日志、告警与流量数据，安全、实时地上报至开封校区的态势感知平台，实现郑州校区的网络安全探针（或传感器）接受开封校区态势感知平台的统一管理；在实施阶段提供《跨校区网络互联设计方案》，明确 VPN 隧道配置参数（如加密算法、存活检测）、路由策略及带宽保障机制。VPN 通道需具备高可用性设计，保障链路稳定性，其性能（带宽、延迟）满足管理流量实时传输及未来业务扩展需求。实现在开封总部统一监控、分析两校区的整体安全态势。制定详细的《安全互联与集中管控集成实施方案》，并获采购人确认。完成集成后，须进行端到端的功能与性能验证，包括 VPN 连通性测试、态势感知平台告警接收测试、EDR 管理平台跨校区终端管控测试等，并出具《集成验证报告》。本部分建设内容自验收合格之日起，提供为期 1 年的技术支持保固服务。确保 VPN 链路稳定，并保障集中管理平台对分支节点设备的持续有效管控。
7	终端安全接入授权扩容	终端安全接入授权扩容： 对现有终端安全管理系统（aES 6.0.2R4）进行扩容 500 套 PC 端全量版端点安全软件授权及 20 套服务器端全量版端点授权用于郑州校区终端使用，扩容后的授权需与现有 EDR 管理平台兼容，支持跨校区统一管理，我方提供兼容性证明材料；将此次授权安全地扩容实现从开封总部对两地终端进行统一的策略下发、威胁查杀、漏洞修复、合规检查及运营响应。同时将终端安全 EDR 平台统一升级至官网最新稳定版本，以实现全量终端的主机安全防护，并完成与现有态势感知平台的策略联动，达成防护策略统一管控、安全告警同步上报、威胁数据互通分析的闭环防护能力。 全过程保障现有终端安全平台的稳定运行，确保原有终端的防护策略不中断、安全数据不丢失，最大限度降低对两校区现有终端业务使用的影响，制定完备的扩容及升级回退方案。前期对开封校区现有统一端点安全管理系统（aES 6.0.2R4）的运行

		状态、授权信息、策略配置、与态势感知平台的联动情况进行全面核查，同时对郑州校区待接入终端的数量、型号、操作系统版本等信息进行详细收集与兼容性分析。出具详细的《授权扩容与平台升级兼容性及风险评估报告》，明确授权扩容流程、平台升级路径、潜在兼容性风险（如终端系统与新版本 EDR 平台适配性、新旧授权融合冲突等）及针对性应对措施。制定详尽的《终端安全接入授权扩容与 EDR 平台升级实施方案》，包括授权激活步骤、平台升级操作流程、郑州校区终端批量接入配置规范、策略联动参数设置、时间计划、回退预案、验证方案等，并经采购人确认。 与采购人共同进行两校区终端安全防护及策略联动业务验证，签署《终端安全接入授权扩容与 EDR 平台升级交付报告》。提供完整的《终端安全授权扩容后系统架构文档》《EDR 平台新版本运维手册》《郑州校区终端接入操作指南》及《策略联动配置说明》。
8	4K 高清视频终端及高清图像编解码器	**1、支持与河南省教育厅视频解码终端工作系统互联互通。**
		2、4K 高清视频终端参数要求
		1）支持 H.323 和 SIP 双协议栈，工作速率支持 64Kbps－8Mbps。
		2）支持 720P,1080P，4K 等图像格式，支持最高双路 4K 30 帧/秒编解码。
		3）支持 G.711,G.711U,G.722,G.722.1C,G.728,G.729A,G.719,AAC-LD 等音频协议，支持 20KHz 以上宽频语音，支持双声道立体声。
		4）支持 H.264,H.264HP,H.265 等视频协议。
		5）在不扩展的情况下，具备 2 路 HDMI，2 路 HDbaseT 数字高清输入接口， 1 路 VGA 标清输入接口，接口为标准通用规格，不得采用私有的协议和私有的接口类型。
		6）在不扩展的情况下，具备 2 路 HDMI 数字高清输出接口，接口为标准通用规格，不得采用私有的协议和私有的接口类型。
		7）在不扩展的情况下，音频支持 1 路麦克阵列输入、1 路 XLR 输入（支持 48V 幻象供电）、2 路线性输入接口；在不扩展的情况下，音频支持 1 路 HDMI 输出、2 路线性输出接口。
		8）支持国际标准 H.460.18 和 H.460.19 安全防火墙穿越标准；支持媒体端口范围可配置；支持 SNMP 协议，支持被集中管理软件管理，支持基于 USB 以及 WEB 方式进行远程升级。
		3、高清图像编解码器参数要求
		1）图像传感器：1 英寸 CMOS，1200 万像素。
		2）支持 30 倍光学自动变焦，12 倍数字变焦。
		3）视场角：H:63° -2.5°
		4）视频输出接口：1 路 HDMI 2.0，1 路 RJ-45（支持 POE 供电）,2 路 12G-SDI，1 路 USB 3.0。

		5）音频接口：1 路 LINE IN ，支持 3.5mm 音频接口
		6）支持 4kp60/p50/p30,1080P60/P50/P30/P25，1080I60/I50，720P60/P50 分辨率。
		7）水平、俯仰转动角度：-173 度到+173 度，-30 度到+90 度。
		8）水平、俯仰控制速度：0.1 ～120°/秒，0.1～90°/秒。
		9）控制接口：1 路 RS-232 IN，1 路 RS-232 OUT（支持 RS485）；支持网络控制，红外遥控；控制协议：PELCO,VISCA
		10）可记忆设置 256 个预置位。
		11）支持图像翻转功能（桌面正装/吊装）。
		12）带三脚架套装，优质铝合金超轻三角架黑色
9	超高清解码器	1、支持 10 路 HDMI 输出。采用嵌入式架构，专用 Linux 系统，使用 DSP 解码；为了设备稳定可靠运行，不得采用工控机或者 PC 机的 X86 架构。可通过控制面板进行监控场景切换，最大可支持切换场景数为 4 个，场景切换时间 2s，过程中无黑屏、闪屏现象。
		2、支持 5 路 3200W、或 5 路 2400W、或 10 路 1200W、或 20 路 800W、或 25 路分辨率为 600W、或 40 路 400W、或 80 路 200W、或 160 路 100W 像素的视频图像同时解码上墙，支持对主/子码流区分取流和解码显示。（提供封面具有 CNAS 认证标识的公安部报告证明）支持接入 MPEG4、MPEG2、H.264、MJPEG、H.265、SVAC 等编码格式视频，并解码输出。
		3、支持客户端软件将电脑投屏后，通过设备对电脑进行远程操作。
		4、支持全部输出口同时输出 3840×2160 分辨率的图像。每个输出口支持任意开窗、漫游；任意 1 路信号显示画面可进行任意漫游、缩放；可在单屏或多屏的任意位置上叠加显示，图层最大不少于 64 层。
		5、支持不通过 IP 网络，通过红外遥控器实现解码图像切换、场景切换、屏幕亮度调节。
		6、显控系统支持自动检测输入源的信号类型，根据信号源类型和显示位置，自动配置信号源所在屏幕的显示场景模式；支持将视频图像进行轮巡输出显示，并可在客户端软件设置轮巡计划。
		7、区域入侵场景：支持接入具有区域入侵功能的前端摄像机，支持区域入侵侦测、越界侦测、进入区域侦测、离开区域侦测，可对前端码流里面的智能信息进行解码并显示，并触发报警弹窗、联动报警输出。
		8、智能抓拍场景：持接入具有智能抓拍功能的前端摄像机，支持同时对行人、非机动车、机动车进行检测、跟踪，可对前端码流里面的智能信息进行解码并显示，并触发报警弹窗、联动报警输出。
		9、支持通过键盘控制画面上墙、点位切换、画面分割、场景切换的功能。
10	会议系统	安装实施服务费，网络机柜及网络配件材料（含替换现开封校区终端移机到郑州校

	安装实施以及线缆及辅材	区）
11	教育网视频会议网元租金	郑州市教育网网元，保证与教育厅视频会议网络一致。
12	信息化技术运维服务	面向郑州、开封两校区提供驻场信息化技术运维服务，服务范围涵盖驻场行政办公维修保障、公共机房信息化运维及网络安全驻场保障，所有服务均需专业人员现场提供。服务期限1年，自合同签订生效之日起计算。服务期满后，根据服务质量及服务水平评估结果，可续签服务合同，最多续签两次，每次续签期限为1年，续签条件及具体事宜另行约定。
		一、网络安全保障、运维服务具体要求：
		组建专属安全服务小组：小组核心成员3名网络安全专家，其中1名全职安全专家驻场服务，负责日常网络安全监控、风险研判、基础安全保障、网络机房巡检及教学楼、实训楼、食堂、宿舍等楼层弱电井的巡查工作；其余2名安全专家具备专业资质（如CISAW、CISA等），作为应急支援力量，实行24小时待命应急响应机制，确保突发安全事件时可快速到场处置。
		日常安全监控与漏洞检测：驻场安全专家需实时监控两校区网络安全态势，包括网络流量异常监测、入侵行为拦截、病毒木马查杀等；每月开展1次全校区范围内的网络安全漏洞扫描，覆盖核心服务器、网络设备、终端主机及应用系统，扫描范围包含系统漏洞、配置缺陷、弱口令等风险点，对扫描发现的漏洞进行分级（高、中、低）评估，并形成详细漏洞清单及整改建议。
		应急响应处置：建立网络安全应急响应流程，接到安全事件告警或采购人通知后，驻场安全专家需立即启动应急处置，其余应急支援人员需根据事件严重程度在2小时内到场（重大安全事件1小时内）；针对病毒爆发、网络攻击、数据泄露等不同类型安全事件，制定标准化处置方案，明确处置步骤、责任分工及止损措施，事件处置完成后24小时内提交应急处置报告，说明事件原因、处置过程、损失评估及防范建议。
		安全报告提交：定期提交多维度安全报告，包括每月漏洞扫描报告（含漏洞详情、整改跟踪情况）、每季度网络安全态势分析报告（含周期内安全事件统计、风险趋势研判、优化建议）、年度网络安全综合评估报告（含全年安全工作总结、体系建设情况、下一年度安全规划）；所有报告需数据真实、分析深入，经安全小组审核签字后提交采购人。
		安全制度与体系完善：协助采购人梳理现有网络安全管理制度，结合国家网络安全相关法律法规（如《网络安全法》《数据安全法》《个人信息保护法》等）及教育行业安全规范，修订完善网络安全责任制、应急预案、数据分级分类管理、访问控

	制等制度；每年开展 1 次网络安全体系合规性评估，形成评估报告并提出制度优化建议。
	培训与演练组织：每半年组织 1 次两校区相关人员网络安全培训，培训内容涵盖网络安全基础知识、常见风险防范、应急处置流程、制度规范等，培训形式可采用线上线下结合，确保参训人员掌握核心安全技能；每年组织 1 次网络安全应急演练，演练场景可选取病毒入侵、数据泄露、网络瘫痪等典型场景，制定详细演练方案、评估标准，演练结束后提交演练总结报告，分析演练效果并优化应急预案。
	二、提供郑州、开封两校区驻场行政办公维修保障服务及公共机房信息化运维服务，具体服务内容包含：
	1、开封校区行政办公信息设备、网络故障处理，维修、维护驻场服务。公共机房信息化运维驻场服务
	（1）一名专项技术人员负责对开封校区行政办公信息设备（含台式电脑、笔记本电脑、打印机、传真机、复印机、扫描仪、投影仪等）、基础网络设备进行维护；对故障进行处理。提供驻场服务。
	（2）保证办公室内教师办公计算机运行正常，定期更新操作系统补丁，安装教师授课需求的教学软件，严禁出现严重的程序漏洞，以确保系统的稳定高效安全运行。
	（3）信息化设备的线路整理、老化线路更换、线路故障的排查。线路标线标，排序规整，检查漏电以及老化线路，控制端口检测，输入/输出线路检测，断点接焊，控制信号检测，防止线路干扰；强电线路接头以及裸露电线绝缘胶带包固，强弱电分离，无安全隐患。
	（4）对开封校区 10 间公共机房，提供相应的运维服务，每周巡检、每季度提交运维报告，保障正常教学及实训，提供驻场服务。
	2、郑州校区办公信息设备及网络维护驻场服务
	（1）一名专项技术人员负责对郑州校区行政办公信息设备（含台式电脑、笔记本电脑、打印机、传真机、复印机、扫描仪、投影仪等）、基础网络设备进行维护；对故障进行处理。行政办公维修保障需实现驻场服务。
	（2）保证办公室内教师办公计算机运行正常，定期更新操作系统补丁，安装教师授课需求的教学软件，严禁出现严重的程序漏洞，以确保系统的稳定高效安全运行。
	（3）信息化设备的线路整理、老化线路更换、线路故障的排查。线路标线标，排序规整，检查漏电以及老化线路，控制端口检测，输入/输出线路检测，断点接焊，控制信号检测，防止线路干扰；强电线路接头以及裸露电线绝缘胶带包固，强弱电分离，无安全隐患。
	三、以上服务由专业人员现场持续提供服务。一年期满后根据服务质量及服务水平，可续签该服务项，最多续签两次。
	四、以上服务供应商为所有驻场人员购买足额的工伤保险、人身意外伤害保险等相

		关保险，如驻场人员在服务期间发生人身伤害或财产损失，由供应商承担全部责任和费用。若供应商提供服务、服务质量不合格、未按时提交相关报告、违反保密义务或人员更换不符合要求的，采购人有权要求供应商限期整改，并可根据违约情况扣除相应服务费用。
		五、服务期满或合同终止时，向采购人移交完整的服务记录、巡检报告、安全报告、资产台账、设备维修记录等所有相关资料，确保资料的完整性和准确性。
13	云桌面管理软件	windows 系统教学主机用云桌面管理软件： 1、支持离线超管功能，可以直接在客户机终端上开启镜像模版并进行修改，并支持在广域网线路上将修改的镜像模版文件自动上传到服务器或者指定目录上； 2、为保障教学环境的业务连续性，系统必须支持网络和硬盘双启动方式：当终端电脑出现硬盘故障或者无硬盘时，终端自动通过网络启动；当网络中断时，终端可正常运行无需重启。终端自动更新时可以通过管理端的更新进度条查看更新状态； 3、支持自动还原和更新，客户机只需要重启便能够恢复到初始的可靠状态；在无 DHCP 情况下，也能够实现所有客户机的更新并支持对客户机进行统一远程开机、重启等操作。系统支持创建单镜像和多节点镜像； 4、支持使用 PC、笔记本、云终端、手机、平板等作为虚拟桌面终端，支持 Android、IOS 等手机、平板访问虚拟桌面； 5、满足终端无分区无系统情况下的自动部署功能，在终端系统初始化启动的时候，无需人工干预，系统可自动根据终端硬盘大小的不同实现终端硬盘不同的分区策略。可在管理平台预创建自动部署策略，自动部署策略中可指定自动分区个数、镜像数据缓存所在分区，并可按百分比配置各个分区大小； 6、支持数据快照与恢复功能，可以随时在客户机终端上进入快照状态安装应用或驱动，保存为快照节点，保存快照数量不受限制，当系统文件发生损坏或需要退回某个桌面环境，可随时恢复到指定节点快照。快照操作支持快照开启、保存、重置、删除和撤销等多种类型； 7、支持对终端本地的硬盘保护，可对本地硬盘中 10 个的分区进行不保护、还原和不还原三种模式设定； 8、客户端具有个人云盘功能，用户存储的数据在服务器端以加密单文件形式保存。用户在任何一台虚拟终端上都可以基于独立的用户密码系统打开磁盘空间； 9、可无缝接入原有多媒体教学网管理系统，支持原有平台统一管理；