郑州信息科技职业学院
校园网特色应用建设项目（包二）

招标编号：豫财磋商采购-2022-500

合
同
书

甲方：郑州信息科技职业学院

乙方：河南金明源信息技术有限公司

甲方：郑州信息科技职业学院

乙方：河南金明源信息技术有限公司

根据河南诚信工程管理有限公司对郑州信息科技职业学院校园网特色应用建设项目（包二）招标结果，甲乙双方认真友好协商，达成以下合同条款：

一、招标文件、乙方投标书作为合同的一部分，变动或强调部分按本合同执行。

二、货物名称、数量（详细附件一）；货物技术规格性能（详细附件二）。

三、合同总金额：捌拾万陆仟元整（¥806000.00）

四、货物质量要求及乙方对质量负责条件和期限：

1．乙方提供的货物须是正规原厂产品，符合该产品的出厂标准和国家检测标准，技术参数按照投标文件执行；

2．乙方对所供设备的售后服务按照投标承诺执行，质保期后只收维修配件成本费，不收工时费；

3．对于出现的故障，乙方接到电话后 1 小时答复，12 小时内解决问题，如 12 小时内不能及时解决问题要提供备机服务、直到原设备修复。

五、设备安装：乙方对设备进行免费安装、调试，使其投入正常使用。

六、项目技术培训：乙方在所有项目设备（系统）正常运行后，免费对甲方人员进行技术培训。

七、完成工期：自合同签订之日起 30 日历日内交货，安装调试于交货后 20 日内完毕，并在交货时向甲方交付设备使用说明书、合格证及相关资料。

八、验收：乙方在所有货物送达指定地点并按要求安装调试完毕后，向甲方提出验收申请，由甲乙双方共同验收并签定验收报告。

九、质保期：从项目正式验收之日开始计算，质保服务期限 3 年（质保期内每季度进行设备巡检和策略优化，每季度一次技术培训操作），硬件设备提供五年质保服务（质保期内提供免费的系统版本升级）。

十、货物或服务（系统）交货（完工）初步验收合格并正常运行后甲方向乙方支付合同额的 45%，试运行无问题经采购人组织的最终验收通过后甲方向乙方支付合同额的 55%。

十一、未尽事宜，甲乙方可签定补充协议作为本合同的有效组成部分。

十二、本合同发生争议产生的诉讼，由合同签订所在地人民法院管辖。

十三、合同生效及其它：本合同经双方代表签字并加盖公章后生效。

十四、本合同一式七份，甲方四份、乙方二份、招标方一份，具有同等法律效力。

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：2022.08.12

乙方名称：河南金明源信息技术有限公司（印章）

授权代表（签字）：

地址：郑州市金水区 139 号河南外包产业园 B4（A 期天元 I）号

邮政编码：450000

电　　话：0371-63661766

纳税人识别号：9141010579324483X0

开户银行：中国银行股份有限公司郑州高新技术开发区支行

帐　　户：252052415716

日期：2022.08.12

附件一、合同标的货物内容及数量

序号	名称	品牌	型号和规格	计量单位	数量	原产地和制造商名称	单价	总价	备注
1	48 口接入交换机	华为数通智选	S5735-L48T4X-A1	台	16	深圳市华为技术有限公司	7162	114592	无
2	24 口接入交换机	华为数通智选	S5735-L24T4X-A1	台	15	深圳市华为技术有限公司	4200	63000	无
3	万兆单模光模块	万兆通	AXS13-192-10	个	62	深圳市深圳市万兆通光电技术有限公司	205	12710	无
4	资源统一管理平台（含硬件设备）	木云	资源统一管理平台软件 V2.1	套	1	郑州市郑州木云电子科技有限公司	242428	242428	无
		木云	资源统一管理平台硬件 MYM-3600ENT	项	1	郑州市郑州木云电子科技有限公司	37570	37570	无
5	网络安全等级保护测评服务	金明源	技术服务	项	1	郑州市河南金明源信息技术有限公司	236700	236700	无
6	系统集成服务	金明源	技术服务	项	1	郑州市河南金明源信息技术有限公司	99000	99000	无
总计：人民币（捌拾万陆仟元整）								806000.00	

附件二、货物技术规格性能

序号	货物名称	主要规格	数量	交货地点
1	48 口接入交换机	1、整机吞吐量 432Gbps，包转发率 144Mpps， 2、实配：48 个 10/100/1000BASE-T 以太网端口,4 个万兆 SFP+,交流供电； 3、支持 ARP 规格 4096、MAC 地址表容量 32880、IPv4 路由规格 4096； 4、设备支持 STP/RSTP/MSTP 二层防环协议； 5、设备支持 RIP/ RIPng/ OSPF/OSPFv3 三层路由协议； 6、为防止设备终端仿冒攻击，设备支持 DHCPv6 Snooping、CPU 黑名单； 7、设备支持以太网环网保护交换 ERPS； 8、为保证设备安全，设备支持大包校验（软件数字签名）； 9、支持新交换机零配置部署； 10、GE（千兆）和 10GE（万兆）端口可以达到线速转发； 11、业务端口转发时延：GE 口小于 4us、10GE 端口小于 2us； 12、支持 EEE 能效以太网；	16 台	采购人指定地点
2	24 口接入交换机	1、交换容量 336Gbps，包转发率 108Mpps； 2、实配：24 个 10/100/1000BASE-T 以太网端口,4 个万兆 SFP+，交流供电； 3、支持 ARP 规格 4096、MAC 地址表容量 32880、IPv4 路由规格 4096； 4、设备支持 STP/RSTP/MSTP 二层防环协议； 5、设备支持 RIP/ RIPng/ OSPF/OSPFv3 三层路由协议； 6、为防止设备终端仿冒攻击，设备支持 DHCPv6 Snooping、CPU 黑名单； 7、设备支持以太网环网保护交换 ERPS； 8、为保证设备安全，设备支持大包校验（软件数字签名）； 9、支持新交换机零配置部署； 10、GE（千兆）和 10GE（万兆）端口可以达到线速转发； 11、业务端口转发时延：GE 口小于 4us、10GE 端口小于 2us； 12、支持 EEE 能效以太网；	15 台	采购人指定地点
3	万兆单模光模块	光模块-SFP+-10G-单模模块(1310nm,10km,LC)；	62 个	采购人指定地点
4	资源统一管理平台	1、采用软硬件一体式设计的设备，配置千兆电口 8 个，千兆光口 4 个，万兆接口 2 个，可管	1 套	采购人指定地点

	（含硬件设备）	理资源站点数量 400，WebVPN 并发用户数 10000 个。配置备案管理、资源发布、WebVPN、一键断网、HTTPS 证书管理、安全威胁管理、僵尸网站检测、资源导航、远程运维管理、日志审计等功能模块，配置一套单独的日志分析系统，除日志分析系统外其它功能模块均在单台设备上实现； 2、IPv6 资源发布：1)支持对校内网站及信息系统等 Web 资源进行集中统一管理，统一入口，隐藏服务器内部 IP；2)全面支持 IPv6，满足全校网站及业务系统进行 IPv4/IPv6 双栈规模化升级改造要求；3)支持站点自定义排序，对站点的查询支持按部门分类统计；4)产品满足 IPv6 相关检测要求； 3、备案管理：1）提供独立的备案工作台，支持以用户身份登录显示由其负责的备案站点，包括我的流程、我的待办、流程设计等，能够集中显示待办事项；2）支持备案审批流程的自定义，工作台支持备案流程设计，包含流程节点设计、表单字段设计，支持表单字段在不同节点上的权限设置，权限支持可读、可编辑、隐藏，以满足个性化信息修改与查看需求，流程节点类型支持审批人、办理人、抄送人和条件分支；支持包含节点、表单字段、表单字段在不同节点上的权限设置、多人依次审批和会签；3)支持二级部门自助备案网站或信息系统，备案成功后二级部门管理员可对本部门站点进行上、下线操作管理；4）备案审核之后自动发布站点，支持审核一键发布，支持仅审核、不发布；审核发布支持 HTTPS；5）支持备案年审，提供一键通知年审功能、备案移交功能以及备案变更功能，并提供备案输出功能，备案输出包括但不限于备案打印、导出为 CSV 和 Excel 格式，产品在显著位置显示详细的年审列表、整改列表以督促问题站点及时整改； 4、图书资源管理：支持图书资源的自定义集中管理发布，可按首字母、数据库类型、学科分类、语种分类自定义查询，查询结果以列表、中外文、图书详情分类展示；支持 PDF 和 Word 格式的报表，可指定报表统计时间区间，支持用户名称自定义，并可自动生成报表编号；支持电子图书资源的统计分析报表，提供 HTTPS 访问下的电子图书资源库名称、总访问量、入口访问量、全文下载量、及访问百分比的分析		

		报表； 5、一键关停：支持一键关停，支持安全中心移动手机端自定义绑定，支持 PC 端及微信一键关停功能；支持自定义一键关停二次验证功能，对网站及信息系统等 web 资源一键断网时支持短信通知相关部门负责人功能； 6、访问控制：支持网站、信息系统等 web 资源访问及上下线时间的自定义；支持 web 资源访问策略的自定义；支持基于地理位置、日期、时间等要素的策略定义，支持精确到目录的访问策略控制；完成与学校智慧校园统一身份证平台对接，支持对接用户不同权限分配，支持自定义权限管理，满足不同应用场景的安全认证需求，支持本地用户名口令、第三方认证组件(LDAP、CAS、RADIUS）、企业微信、钉钉、手机短信、用户名口令+短信双因素认证等认证方式；支持本地创建用户分组，不同用户可以分配不同权限，权限种类包括管理员权限、备案权限、整改权限、日志权限、访问协议权限； 7、WebVPN：配备 WebVPN 模块，无须在系统中通过域名或别名对资源进行预先定义或适配即可通过系统访问 HTTP、HTTPS、RDP、VNC、Telnet、SSH 协议的资源；无需配置通配符泛域名解析，即可实现用户通过门户中导航块直接访问资源，支持通过门户中的地址栏自定义其访问目标；且可以对 HTTPS/HTTP、SSH、RDP、telnet 等协议权限做控制； 8、CA 证书管理：支持证书集中管理，支持对网站批量进行证书加载或卸载；支持证书有效期的监控预警管理，在证书到期前 15 天通知客户；支持证书检测，可查看证书用户名、有效期、颁发机构、使用单位信息等，支持证书合成，可以自动补全中间证书； 9、僵尸网站管理：支持自定义创建僵尸网站策略，策略条件包括访问量、网站是更新、时间段。同时可以检测网站在 180 天内是否有更新； 10、支持 WAF 规则自定义，支持 WAF 防护、安全策略、IP 黑白名单限制，支持 SQL 注入、XSS 跨站、cc 攻击等攻击防护，支持例外设置； 11、支持网站防篡改策略，策略类型包括名称、策略对象、有效期、起止时间、周选择。同时可以对单个网站大小、文件数进行查看和管理，可以恢复至任意备份站点，支持防篡改功能的缓存管理；		

		12、支持防盗链管理，提供防盗链事件日志记录，包括时间、请求类型、请求网站、地理位置、防盗链规则等； 13、支持弱密码检测及防护功能，支持针对网络中存在弱密码系统的进行事件日志记录，包括时间、用户名、密码、详细信息等，可导出日志； 14、支持安全威胁管理，信息系统发生安全风险时可根据安全隐患名称、隐患类别通过短信及邮件及时通知相关责任人； 15、监控告警：提供雷达实时监控及监控列表两种方式，支持批量告警设置，支持在监控列表中一键通知相关负责人，支持实时监测与告警信息同屏显示，以便监控人员在发现问题时无需转到其它页面即可了解具体的告警信息；内置短信平台模块，支持通讯录定制开发，可满足组织架构创建与维护，自定义全局通讯录信息；可根据部门、职位、管理权限等信息自定义用户组下发漏洞整改报告； 16、API 接口：提供微信 API 接口，支持通过微信对接实现信息系统及站点一键关停操作及系统的告警信息推送；支持 DNS 联动，提供 API 联动接口文档； 17、业务负截均衡支持同一域名下的多个服务器进行负载均衡及健康状态检测，负载均衡算法包含轮询、权重、IP 哈希、URL 哈希、响应时间；健康状态检测包含主机服务状态、连接成功次数，失败次数； 18、网络及常工具：支持应用层 xforward_ip 字段来源模式转发设置。开启后可在日志系统中对 xforward_ip 字段进行查询；支持在多接口服务的环境下提供源进源出的路由功能，支持接口聚合，实时查看各网络接口上的流量；提供常用网管工具 PING、TRACEROUTE、网站访问、转码工具、端口探测、whois 等小工具以提高网络和配置问题定位和排查的效率； 19、支持以中国地图为背景的各省实时访问全景图展示，动态实时显示系统访问状态及排名。包括站点访问量排行、系统性能监测、实时访问、攻击数据滚动显示等； 20、提供系统操作日志、弱密码日志、超级终端日志、在线用户日志等。支持访问日志的自定义查询，支持访问日志详细查询可精确到具体 URL、具体路径及文件名；		

		21、提供各信息系统资源的访问日志,实时显示访问时间,访问源 IP,详细 URL、访问类型等日志的记录.支持访问 URL 排名,支持访问 IP 排名形成详细的网站流量统计分析报表,终端访问者的操作系统和浏览器统计; 22、支持各站点资源的攻击日志记录，实时显示攻击时间,攻击源 IP,URL、类型等日志的记录.支持攻击 URL 排名,支持攻击 IP 排名,支持图表显示; 23、提供独立的日志分析系统一套，支持 IPV4、IPV6 访问日志的集中管理，满足 180 天日志审计需求;		
5	网络安全等级保护测评服务	1、根据学校信息化建设现状，开展网络安全等级保护测评工作: 主要包括校务管理系统类、教学科研类、招生就业类、综合服务类、教育系统服务类等五类信息系统及子系统的二级测评。 2、项目总体管理和技术：总体与《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）、《教育行业信息系统安全等级保护定级工作指南（试行）》的通知》（教技厅函 [2014]74 号）等信息安全等级保护系列文件保持一致，开展信息安全等级测评工作。具体信息安全技术标准以文件相应部分提及的为准; 3、本项目按照信息安全等级保护 2.0 测评标准进行安全等级测评。具体项目测评内容如下: 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、安全计算环境和安全管理中心等五个方面的安全测评; 安全管理测评：安全管理机构、安全管理制度、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控制测评; 4、在安全等级测评过程中，每个工作阶段、流程、内容、及成果交付严格遵循《信息安全技术 网络安全等级保护测评要求》和《信息安全技术 网络安全等级保护测评过程指南》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，测评报告得到项目单位的确认，报送网安部门审核、批复。测评报告编制的内容及格式严格遵	1 项	采购人指定地点

		照《网络安全等级保护测评报告模版（2021 年版）》进行； 5、测评技术团队符合《网络安全等级保护测评机构管理办法》对测评机构和测评人员管理的要求，项目负责人由公安部培训考核认证通过的信息安全高级等级测评师承担，通过注册信息安全专业认证、具备良好的教育背景、受过专业的技术培训、拥有丰富的行业等级测评安全服务工作经验，对用户在信息系统安全等级测评过程中可能会面临的各类技术问题提供及时解决方案； 6、等级测评交付成果： 测评准备活动：项目计划书、被测系统基本情况分析报告； 方案编制活动：测评指导书、信息系统安全测评方案； 现场测评活动：测评结果记录、测评中发现的问题汇总； 分析与报告编制活动：单项测评结果汇总分析、整体测评结果汇总分析、风险分析和评估、等级测评结论、信息系统安全等级测评报告； 7、整改具体：依照《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)，严格遵循《信息安全等级保护安全建设整改工作指南》各项要求，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，提供安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和运维等安全工程类信息安全服务咨询，并制订信息安全等级保护安全建设整改方案，方案内容包含但不限于：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全建设整改技术方案设计、安全建设整改管理体系设计、信息系统安全产品选型及技术指标建议、安全建设整改项目实施计划、项目预算，整改后可能存在的其他问题； 8、整改交付成果： 等级化安全保障建议方案： 内容包括但不限于以下方面： （1）安全区域和等级划分； （2）安全体系框架设计； （3）等级化安全指标体系报告； 安全体系建设建议方案：		

		内容包括但不限于以下方面： （1）网络面临风险分析； （2）针对性措施建议； 相关网络安全管理制度： 内容包括但不限于以下方面： （1）机房安全管理制度； （2）网络故障应急预案及应急方案流程制度； （3）客户端管理制度； （4）数据备份及恢复制度； （5）灾难恢复策略及制度； 9、渗透测试： 对信息系统中的主机操作系统、数据库系统、应用系统等进行模拟攻击测试，在保证整个渗透测试过程都在可以控制和调整的范围之内，尽可能的获取目标信息系统的管理权限以及敏感信息，以查找和分析安全漏洞和隐患。每次渗透测试后出具正式的分析报告和解决方案。 服务：由具备注册渗透测试资质和专业能力认证的工程师现场部署渗透环境，通过真实模拟黑客使用的工具、分析方法来对网站进行模拟攻击，并结合智能工具扫描结果，进行深入的人工测试和分析，识别工具弱点扫描无法发现的问题，主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误等以及其他专项内容测试与分析； 渗透测试后出具正式的分析报告和解决方案，针对渗透测试出的问题、漏洞、缺陷等，完成整改及后续验证工作，每项渗透内容报告包括问题整改和验证的过程记录及详细的解决方案； 人员：渗透工程师具备专业资格认证、受过良好的技术培训、拥有丰富的信息安全渗透测试工作经验； 10、安全咨询： 安全服务机构建立专业团队对网络安全现状进行调研、梳理，按照国家等级保护三级要求、行业网络安全要求及信息安全规划，以ISO27000、ITIL 系列标准以及国际、国内最佳实践为指导，提供信息安全等级保护等相关安全咨询服务，保证本项目建设期内持续性、连续性安全需求。咨询服务内容包括：安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和运维等安全工程类信息安全服务咨询；系统定级、备案、测评、建设整改等		

		咨询；信息技术服务管理体系、信息安全管理体系认证等合规咨询； 服务：依据前期等保测评结果，结合监管部门要求、国家等级保护制度要求以及信息安全发展方向，为重要信息系统提供满足未来三至五年信息安全管理体系建设规划； 安全管理体系建设规划要求能够落地，明确信息安全管理的方针、目标和对象。在信息安全管理标准框架下，通过制订各项信息安全管理制度，规范信息安全日常管理工作，切实提高重要信息系统等安全基础管理水平，实现制度化、流程化、体系化的管理思想； 11、应急承诺： 建立安全应急预案，遇到重大安全事件如网络入侵、大规模病毒爆发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决时，我公司安排专业技术人员以 7*24 小时远程、电话、邮件及现场等方式提供应急响应支持，快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响，查明安全事件原因，确定安全事件的威胁和破坏的严重程度，并根据对事件的分析及原因提供相应的解决方案； 服务：在发现安全事件时，及时判断安全事件的级别。针对严重的安全事件，对安全事件进行紧急分析处理、灾难恢复和和入侵追踪和取证，出具应急响应报告（含加固建议）。 建立长期稳定的本地专业安全服务团队，并通过专业认证，在发生重大安全事件时，在半小时内提供现场应急响应；在发生一般安全事件时，一小时内提供现场应急响应； 12、安全培训： 面向全员的安全意识培训：结合行业信息安全保障的重点，着重提高所有人员的信息安全意识和技能，对人员理解信息安全对机构的意义，开展信息安全工作，在机构内逐步建立和融入信息安全文化，提高整体信息安全防护水平； 面向技术人员的安全技术培训：对信息化技术人员培训重点是熟悉网络安全技术、了解各种常用安全产品的原理，能正确使用解决方案中的各种安全产品，以达到最佳的安全保障效果。主要的培训内容包括安全域培训、入侵检测技术、漏洞发现技术，安全产品管理、用户管理策略、日志分析方法、故障诊断和维护等；		

		面向技术主管与管理层的管理体系培训：对技术主管和管理层的培训重点是信息安全知识体系和安全意识的，目的是使管理人员在了解了信息安全知识体系的基础之上，注意到使用信息系统的风险，并使他们关注降低风险的对策；网络攻防实训：针对常见的网络攻防技术手段，组织用户动手实践，使用户深刻理解网络攻防的基本理论，掌握常用的网络攻防技术手段和工具软件，具备能够科学合理地提升单位网络安全水平、独立处理日常信息系统运维过程中可能出现的安全事件的能力； 13、数据库巡检：服务期内，定期为单位数据库系统进行健康状况检查，及时发现目前软件产品和生产数据库已经存在的或潜在的问题，确保整套系统正常运行。 14、项目最终成果： （1）《网络安全等级测评报告》； （3）系统定级材料编制； （4）交付项目涉及的所有业务系统的安全等级测评整改技术方案对应的文档，及其对应的安全等级测评报告原件（附 Word 电子版文件），可根据整改和规划内容的重要性和复杂程度采用分册方式编写； （5）完成各个信息系统的等级测评工作并提交等级测评报告； （6）提交测评各个阶段的文档。		
6	系统集成服务	1.本次项目所提供产品的安装和调试； 2.本次项目产品与现有校方设备的安全平稳对接和联调，不能中断学校业务； 3.本次项目中涉及的软件系统与学校统一身份认证系统对接，与学校数据中台互通，统一使用学校数据标准，定时将本项目所产生的数据资产交换到学校数据中台。 4.提供本项目实施所需相关网线、跳线、模块等辅材。 5.质保期内每年提供 4 次设备、系统的安全检查，培训交流与版本升级服务。	1 项	采购人指定地点