

河南建筑职业技术学院

政府采购合同书

甲方（全称）：河南建筑职业技术学院

乙方（全称）：河南领晟信息科技有限公司

根据《中华人民共和国民法典》及有关法律、法规规定，遵循平等、自愿、公平和诚实信用的原则，双方就河南建筑职业技术学院校园网络运维与管理升级改造项目及有关事宜协商一致，共同达成如下协议：

第一条 合同文件

下列与本次采购活动有关的文件及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. (豫财磋商采购-2025-668) 竞争性磋商文件
2. 响应文件

第二条 合同总价款

1. 本合同服务总价款：¥1228600 元（含税）。

大写：壹佰贰拾贰万捌仟陆佰元。

2. 本合同总价款包括服务期间必须的日常物料、易耗品、工具、调试费、培训费等相关费用。

第三条 合同服务内容

序号	项目名称	单位	数量	单价	总价
1	网络出口带宽租赁	项	1	650000	650000
2	校园设备维护和改造升级服务	项	1	490000	490000
3	百度信誉认证技术服务	年	1	6600	6600
4	OA 办公系统维护服务	年	1	12000	12000
5	服务器版杀毒软件特征库服务	年	1	50000	50000
6	系统等保测评服务	项	1	20000	20000
7	总计				1228600

第四条 合同期限

1、合同履行期限：2025年06月25日至2026年06月24日。

2、服务地点：河南建筑职业技术学院。

3、合同生效后，乙方应于5日内按甲方要求在河南建筑职业技术学院派驻专业人员执行本项目。

第五条 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。

第六条 付款方式

付款方式：乙方派驻人员进场后，乙方开具合同金额100%的发票送交甲方；甲方收到发票后支付合同金额100%货款。

第七条 争议的解决方式

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监督单位进行质量鉴定；因履行合同发生的争议，由甲乙双方直接协商解决，如协商不成可向甲方所在地人民法院诉讼。

第八条、违约责任

1、除如因战争、严重火灾、水灾、台风、地震、雷电和人为故意破坏等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、若乙方所供的服务、货物品牌、型号、规格、运行质量不符合招标文件和投标文件规定或合同规定的，乙方应负责改正更换并承担因变更而支付的一切费用，甲方有权追究乙方责任，给甲方造成损失的（包括但不限于直接和间接损失），乙方应全额承担。

3、若逾期超过30天仍不能履行合同，则甲方有权解除合同，乙方应在解除合同之日起2日内退还甲方已支付的合同款并支付违约金50000元，同时追究乙方责任。

4、乙方在维护过程中，如存在泄露甲方商业机密等情况的，甲方有权终止本合同并要求乙方支付违约金50000元并赔偿给甲方造成的一切损失，同时退还甲方已支付的全部合同款。

5、乙方应按附件运维服务方案提供服务，如有不符合附件方案的，乙方应在甲方提出异议后2日内整改。期限内整改不到位的，每次支付违约金1000元。若乙方仍拒绝整改，甲方可寻求第三方服务，由此产生的费用由乙方承担。

第九条 其他

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。本合同一式陆份，甲

方四份、乙方两份。

附件：运维服务方案

甲方代表签字：



甲方名称：

河南建筑职业技术学院

地 址：

河南省郑州市二七区马寨镇工业路51号

乙方代表签字：



乙方名称：

河南领晟信息科技有限公司

地 址：

河南省郑州市金水区郑花路59号21世纪广场4号楼5层516号

电 话：

电 话：

0371-61220020

开户银行：

中国农业银行股份有限公司郑州马寨支行

开户银行：

中国民生银行股份有限公司郑州心怡路支行

账 号：

16058701040002432

账 号：

170009572

签约时间：

2025年8月26日

附件：运维服务方案

1. 网络出口带宽租赁

- (1) 中国移动 1Gbps ；
- (2) 中国联通 1Gbps ；
- (3) 中国电信 500Mbps。

2. 校园设备维护和改造升级服务

(1) 驻场网络运维服务

覆盖校园网核心设备（如路由器、交换机、无线 AP）、出口链路（运营商专线）及网络安全体系（防火墙、入侵检测系统），具体包括：

服务模块	关键动作	目标效果
7×24 小时监控	部署网络管理平台，实时监测流量、设备状态、 链路质量	故障预警率 ≥90%，提前 发现隐患
故障快速 响应	分级处理：一级故障（全校断网）15 分钟到场， 二级（局部断网）1 小时内修复	故障修复及 时率≥98%
设备深度 巡检	周级硬件检查、月度性能评估	设备生命周 期延长 20%
网络优化 升级	基于教学场景（如在线课堂、考试系统）动态调 整 QoS 策略	关键业务带 宽保障率 100%

(2) 学生机房运维服务

聚焦教学场景，覆盖计算机、投影仪、多媒体设备及机房环境，保障“课前准备-课中运行-课后维护”全流程稳定：

A. 硬件全生命周期管理

日常维护：定期（每季度或每月）检查设备通电、显示、外设（键盘鼠标）状态；课后、登记故障（如电脑无法进入系统、无网络、屏幕花屏等）。

应急维修: 课中设备故障 10 分钟内到达现场进行维修, 如果硬件故障课后 48 小时内更换部件或 7 个工作日内修复。

B. 软件标准化管理

系统与软件: 统一部署教学专用系统 (如 Windows 11), 预装常用教学软件 (WPS、浏览器、钉钉、教学软件等), 支持教师自定义软件包需求。

数据保护: 启用硬盘还原卡 (或云桌面), 防止学生误操作导致系统崩溃。

病毒防护: 安装杀毒软件, 定期更新病毒库, 开启主动防御功能。

(3) 办公区网络与设备服务内容

A. 办公网络

基础网络维护:

局域网 (LAN) 管理: 交换机、路由器、光纤收发器等设备配置与调试

无线网络 (Wi-Fi) 维护: AP 点位优化、信号强度检测

IP 地址分配与 DHCP 服务管理

VLAN 划分及网络隔离策略实施

网络故障处理:

断网/延迟问题排查 (ping 测试、tracert 路由追踪)

物理层故障: 网线/光纤断裂、接口松动修复

逻辑层故障: DNS 解析错误、ARP 欺骗防护

网络安全服务:

防火墙策略配置与日志分析

网络设备漏洞扫描及固件升级

异常流量监控 (如 DDOS 攻击识别)

用户终端支持:

电脑/手机联网故障 (IP 冲突、认证失败等)

VPN 接入配置 (远程办公支持)

网络共享权限管理 (文件夹/打印机共享)

B. 打印机运维

硬件维护:

机械故障处理: 卡纸清除、进纸轮清洁

软件配置:

驱动安装与更新（本地/网络打印机）

共享打印机配置

网络扫描仪安装配置

故障诊断：

打印异常：乱码、空白页、颜色失真

连接问题：无法识别 USB 设备、网络打印脱机

队列清除：卡滞任务删除与服务重启

C. 有线电话运维

线路与设备维护：

电话线路检测：排查短路、杂音、无拨号音问题

座机硬件安装：听筒、按键故障更换

线路标签规范化管理

D. 维修费用

针对办公设备维修，我司承担维修费用不超过 1000 元的维修服务项目（含硬件）

3. 驻场团队与响应机制

(1) 驻场团队配置

A. 人员架构

网络工程师（1 名）：负责交换机、防火墙、VPN 等核心设备

桌面运维（1 名）：处理电脑终端、打印机、电话、服务器、有线电话等问题

备岗人员（1 名）：应对突发状况提供的人员支持

B. 技能要求

持证上岗：须具备中级网络工程师厂商认证（网络）、硬件维修工程师认证

工具熟练：掌握 ping（网络诊断）、PRTG（流量监控）、打印机管理工具

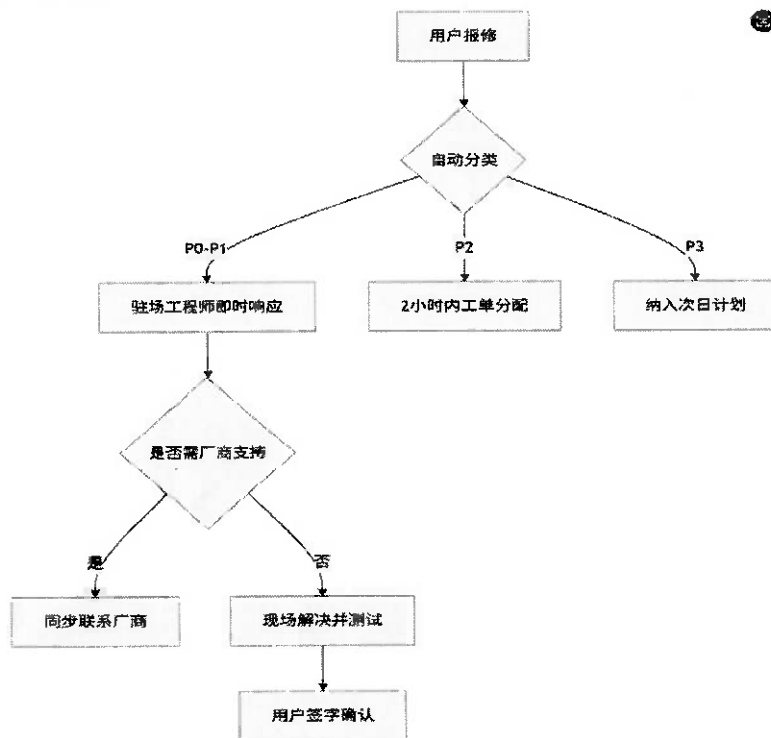
(2) 分级响应标准

A. 事件分级标准

等级	判定标准	响应时效	升级路径
P0（紧急）	全员断网、核心打印机瘫痪	≤15 分钟到场	驻场团队→甲方 IT 负责人→厂商支持

等级	判定标准	响应时效	升级路径
P1 (高)	部门级网络中断/领导专线故障	≤30 分钟	驻场直接处理
P2 (中)	单台设备故障(如 1 部电话不通)	≤2 小时	桌面运维处理
P3 (低)	非紧急需求(如备件补充)	≤4 小时	走采购流程

B. 处理流程



(3) 驻场工作管理规范

A. 日常巡检制度

网络设备：每日早 9 点检查核心交换机端口状态

学生机房：每季度进行一次统一巡检

B. 工具与备件

随身工具包：

网络：测线仪、光纤笔、Console 线

打印机：镊子（取卡纸）、酒精棉片

电话：电话机测试仪、备用话机

备件库存：

最低储备：5 箱六类网线、3 个电脑硬盘、3 个电脑内存、2 个投影仪、2 个 6U 机柜、2 个 PDU 等；

（4）服务质量指标

网络可用率：≥99.9%（年中断时间≤8.76 小时）；

机房设备课中故障率：≤1%（每 100 节课≤1 次设备故障）；

客户满意度：≥95%。

（5）持续改进机制

月度复盘会：与学校信息中心同步服务数据（故障统计、优化建议），调整下月重点；

知识库建设：汇总常见问题（如 WiFi 连接失败、软件激活异常），编制《校园网络运维手册》《机房操作指南》；

3. 百度信誉认证技术服务

（1）由百度官方授权服务商为学校开通百度信誉 V 认证账号，账号类型为公益组织/事业单位（免费通道）。

（2）百度搜索学校名称或官网域名时，显示蓝色“V”标，点击可查看学校信誉档案（含机构名片、口碑评价等）。增强公众信任度，防范仿冒网站。

（3）服务期：1 年（自认证通过之日起算）。

（4）运维支持：7×24 小时咨询：提供专属客服（电话/企业微信），解决认证状态查询、材料更新等问题。

（5）定期巡检：每季度检查认证标识展示状态，确保无异常。

4. OA 办公系统维护服务

针对校园泛微 OA 系统维护服务需求，提供以下服务内容，确保系统稳定运行。

服务内容	服务范围	服务次数	服务时间
电话支持	客户服务人员向校方提供热线电话技术服务解答泛微软件的使用维护问题。	不限	不限
在线远程登陆维护	用 QQ 或其他远程控制系统对校方使用的服务范围内规定软件进行维护调试。	不限	不限
邮件服务	向校方提供技术服务电子邮件地址，服务方在接收到校方服务支持请求邮件后在正常工作日 8 小时内处理。	不限	不限

客户交流会	提供参加泛微在上海或者在其他地区举办的客户交流会，培训免费(交通和食宿自理)。	不限	/
泛微客服期刊	每周发送泛微客服期刊，内容会包括：客户调查、使用小窍门、新功能介绍、培训邀请、应用解决方案。	每周	/
系统管理员培训	免费提供参加泛微举办的管理员培训，培训免费(交通和食宿自理)。	不限	/
上门回访服务	提供上门回访服务，以了解校方使用情况，提供更好的建议。	至少 1 次	/
系统重装和恢复支持	针对 Windows 操作系统提供技术人员通过远程辅助客户进行系统重新和恢复支持。	3 次	/
升级服务支持	提供技术人员通过远程辅助客户进行软件的升级和检查工作。	不限	/
技术支持服务	校方在系统使用过程中如出现的例如查询表结构、查询某数据、调整系统内的一些数据、校方开发需要的一些其他协助等非开发式的请求，提供协调及技术支持服务。	不限	/
登陆界面制作支持	提供客服人员辅助校方完成系统使用中的登陆界面制作。	1 次	/
金牌用户评选服务	在服务期间，校方享有泛微举办的金牌用户的评选权利。	3 次	/
优秀项目推广人和管理员评选服务	服务期间，校方享有泛微举办的优秀项目推广和管理员的评选权利。	3 次	/

5. 服务器版杀毒软件特征库服务

(1) 方案概述

本方案针对学校国产化终端及服务器的安全防护需求，提供统一端点安全管理平台，实现病毒查杀、威胁狩猎、资产管理、策略管控、攻击溯源等核心功能，满足招标文件全部技术要求，并适配国产化操作系统环境。

(2) 系统架构设计

A. 整体架构

采用“1+N”管理模式：

1 套安全管理控制中心：负责策略下发、日志收集、威胁分析、可视化展示。

N 个终端/服务器 Agent：轻量级代理，负责行为监控、病毒查杀、资产上报。

B. 网络部署

管理控制中心：部署于校内数据中心，支持 B/S 架构访问。

终端 Agent：静默安装，支持国产化操作系统（麒麟、统信等）及 Windows/Linux 服务

器。

(3) 核心功能实现

A. 国产化终端统一管理

适配国产 OS：支持中标麒麟、银河麒麟、统信 UOS 等，提供系统级安全防护。

策略统一下发：通过控制台批量配置查杀策略、监控规则、白名单等。

B. 高级威胁狩猎（ATT&CK 框架）

行为数据采集：监控文件变更、进程树、网络连接、DNS 查询等，存储 90 天日志。

全网威胁检索：支持条件组合查询（如进程名=powershell AND 目标 IP=外网）。

攻击链可视化：自动生成攻击路径图，标注初始入侵点、横向移动、持久化行为。

C. 资产管理

资产登记：支持录入责任人、联系方式、资产编号、位置等字段，支持必填项校验。

自动发现：通过 ARP 扫描识别未注册终端，减少人工维护成本。

D. 安全策略一体化

单策略多管控：

病毒查杀：全盘/快速扫描、信任目录排除。

WebShell 检测：支持 PHP/ASP/JSP 等脚本监控。

暴力破解防护：自动阻断高频登录尝试 IP。

E. 攻击溯源与可视化

进程树分析：展示恶意进程的父进程、子进程关系。

攻击故事线：时间轴形式呈现攻击阶段（初始访问→执行→持久化→数据渗出）。

F. 主机运行监控

实时状态检测：

进程与服务：监控异常进程（如挖矿程序）。

网络连接：识别可疑外联（如 C2 服务器通信）。

计划任务：防止恶意任务持久化。

G. 权限管理与审计

三权分立：

角色	权限	安全措施
超级管理员	策略配置、终端分组	USBKey+IP 白名单绑定

普通管理员	日常运维（扫描、补丁）	动态短信验证码
审计员	日志查看、报告导出	操作记录留存 6 个月

H. 无特征检测（AI 引擎）

沙箱行为分析：检测未知恶意软件（如勒索病毒变种）。

零误报保障：基于机器学习模型，提供第三方检测报告。

I. 勒索病毒防护看板

7 天防护统计：展示已阻断加密行为、隔离可疑文件、拦截暴力破解次数。

(4) 服务内容

A. 系统部署

环境适配测试：验证国产化 OS 兼容性。

策略初始化：配置基线安全策略（如病毒扫描计划、实时监控规则）。

B. 运维支持

特征库升级：每日更新病毒库，季度升级检测引擎。

应急响应：针对勒索病毒、挖矿木马等提供快速处置。

管理员培训：涵盖策略配置、告警分析、报告导出。

(5) 方案优势

全栈国产化适配：从 OS 到安全引擎均符合信创要求。

实战化威胁检测：基于行为分析，而非依赖特征库。

易用性：可视化管控，降低运维复杂度。

6. 系统等保测评服务

(1) 服务内容：为学校提供专业化的等保测评协助服务，完成指定业务系统的二级等保测评工作。服务内容涵盖测评前准备、测评过程协调、问题整改跟进及报告备案全流程支持，确保测评工作高效推进并顺利通过网安部门审核。

(2) 系统数量：1 个。

