

郑州信息科技职业学院网络安全与数据安全运营服务项目采购合同

合同编号：豫财磋商采购-2026-771

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

本合同于 2026 年 8 月 29 日由甲方和乙方根据《中华人民共和国政府采购法》《中华人民共和国民法典》及郑州信息科技职业学院网络安全与数据安全运营服务项目（项目编号：豫财磋商采购-2026-771）竞争性磋商文件、响应文件、成交结果相关要求，并经双方协商一致，同意按下述条款签署。

一、本合同基础声明如下：

1、本合同总金额为：1597760.00 元；大写：壹佰伍拾玖万柒仟柒佰陆拾元整。本合同总价为包干总价，包含全部软硬件部署、授权、驻场人工、测评、网络安全险、重保、培训、应急处置、漏洞修复、软硬件维保、税费、检测认证、保密、人工差旅、报告编制、售后等全部费用，甲方无需额外支付任何款项。

2、本合同中的词语、术语释义，与本项目采购需求书、竞争性磋商文件、乙方响应文件保持一致；如文件约定冲突时，以对甲方有利条款优先适用。

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：服务分项价格表

附件 2：成交通知书

附件 3：主要技术参数或功能

4、服务的技术标准：按照竞争性磋商文件中的技术要求和甲乙双方在合同中商定的技术条件、质量标准或补充的技术要求执行。乙方提供的项目服务应达到竞争性磋商文件和乙方响应文件中的技术标准，安装运转后发现内在质量缺陷的产品，乙方无条件更换。

5、乙方承诺提供的全部产品及服务（含软硬件设备、系统、工具等）均为

合法正版、来源合规，不存在任何版权、知识产权纠纷或权利瑕疵。因乙方提供的产品或服务侵犯第三方合法权益而引发的任何索赔、诉讼或争议，由乙方承担全部法律责任和费用，并赔偿甲方因此遭受的全部损失。

二、合同履行的地点及工程进度

1、履行地点：甲方指定地点。

2、项目建设进度

合同生效后，一次性建设内容（包含软件成分分析系统、等级保护测评服务），在合同签订后 60 日历天内完成全部部署、调试、测评、初验，交付全套纸质+电子成果报告；

年服务建设内容（包含数据安全管理与监测运营服务、网络安全险服务、终端安全管理系统、资产梳理与暴露面检测服务、网站监测服务、重保支持服务、数据安全分类分级服务、驻场服务），在合同签订后 30 日历天内达到服务条件（包含但不限于完成工具上线、驻场人员全部进场、安全策略配置、保险保单交付），经甲方书面确认达标之日起，正式启动 1 年完整服务周期。

三、验收与付款方式：

1、合同签订完成后 30 日内，甲方向乙方支付合同总金额的 30%，即大写人民币肆拾柒万玖仟叁佰贰拾捌元整（¥479328.00 元）；服务期每满 6 个月由甲方组织一次验收，乙方技术人员参加，每次验收通过后，甲方向乙方支付合同总金额的 35%，即大写人民币伍拾伍万玖仟贰佰壹拾陆元整（¥559216.00 元）。

2、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）由甲方签字盖章的验收合格报告；（3）提供增值税专用发票；（4）各阶段交付物清单及对应的服务成果文件，包括但不限于资产台账、漏洞扫描月报、数据安全风险报告、风险评估报告、渗透测试报告、驻场运维日志等。

3、验收：服务期满 6 个月由甲方邀请专家组织第一次（中期）验收，乙方技术人员参加；服务期满 12 个月后，甲方邀请专家组织第二次（终期）验收，乙方技术参加，过程中所有文档存档。

4、若阶段性验收、终验不合格，甲方出具书面整改通知书，乙方须在 7 日内完成全部整改，整改所有费用由乙方自行承担；逾期未完成整改，甲方有权暂

停付款、扣除当期款项、计收违约金，直至单方解除合同。

四、人员培训及售后服务

1、乙方免费为甲方信息技术与数据管理中心教职工提供不少于 3 次专项安全培训，培训内容包含数据分类分级、漏洞处置、等保合规、工具操作、网络安全应急响应、师生个人信息防护；每次培训提供 PPT 操作手册、培训签到表、培训考核记录，单次培训时长不少于 2 课时。

2、售后服务：

(1) 远程支持：全年 7×24 小时不间断远程线上技术支持；

(2) 线上响应时效：甲方报修后 10 分钟内远程响应，1 小时内完成故障等级、影响范围、处置方案初步判定；

(3) 现场服务：甲方要求工程师到场时，乙方人员 2 小时内抵达校内现场；24 小时内解决故障或问题；

(4) 重大安全事件（如数据泄露、网页篡改、勒索攻击、高危漏洞爆发、重大活动重保期间等），乙方在收到甲方通知后立即线上线下联动处理解决，同时乙方增派专家团队 7×24 小时驻场值守，免费提供应急处置、攻击溯源、系统加固、事件复盘全流程服务。

3、质保周期：本项目配套运维、测评、驻场整体质保运维期 1 年；软件成分分析系统原厂质保 5 年，质保期内免费版本升级、漏洞库实时更新、功能迭代优化。

4、乙方未按上述约定提供售后服务或未在约定时间内提交成果文件或解决故障的，每发生一次，按合同总额的 1 %向甲方支付违约金并赔偿给甲方造成的全部损失，同时，甲方有权另行委托第三方处理，全部费用由乙方承担。

五、保密及数据安全要求

1、乙方在履行本合同过程中知悉的甲方的所有信息（包括但不限于业务数据、系统信息、管理信息、技术资料、用户信息等）均属于保密信息，乙方应承担严格的保密义务，不得向任何第三方泄露，不得用于本合同以外的任何目的。

2、乙方应确保其人员及所有接触甲方信息的相关方均遵守本条保密义务，并对其行为承担连带责任。

3、保密期限为永久，除甲方书面同意或保密信息被依法公开外，乙方不得

泄露甲方任何非公开信息。

4、乙方在处理甲方数据时应遵守《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规，采取必要的技术措施和管理措施保障数据安全。

5、乙方违反保密义务和数据安全要求的，乙方应立即采取甲方认可的有效措施予以解决和消除影响，且需赔偿甲方全部损失。如乙方不能及时解决和消除影响，甲方有权解除本合同，乙方应退还甲方全部款项并向甲方支付合同总金额20%的违约金；造成甲方损失的，乙方应全额赔偿。

六、知识产权

1、乙方利用甲方提供的业务需求、数据、资料等形成的针对甲方特定业务场景的定制化服务成果、报告、配置方案等知识产权归甲方所有。乙方不得超出本项目范围外使用、复制、商用或提供给第三方。

2、乙方为履行本合同所提供的通用软件、工具、平台等的知识产权归乙方所有，但甲方享有在合同约定范围内的永久免费使用权。

3、乙方提供的第三方软件、组件等，乙方保证已取得合法授权，并保证甲方使用该等软件、组件不侵犯任何第三方合法权益。如发生任何侵权纠纷，由乙方承担全部责任并赔偿甲方全部损失，同时乙方按本合同总额的10%向甲方支付违约金。情节严重的，甲方有权解除合同，乙方除支付违约金外，仍需退还甲方支付的全部费用。

七、服务团队及人员变更

1、乙方须按照响应文件及合同约定组建服务团队，项目经理及核心服务人员须与响应文件一致。

2、服务期内，未经甲方书面同意，乙方不得更换项目经理及驻场工程师。确有不可抗力等正当理由需要更换的，乙方应提前15个工作日向甲方提出书面申请，并提供具有同等或更高资质和经验的替代人员，经甲方书面同意后方可更换。

3、乙方擅自更换项目经理或驻场工程师的，每更换一人次，向甲方支付合同总额5%的违约金，如造成甲方损失的，乙方予以赔偿。

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、乙方所供的产品及服务内容、品牌、型号、规格、运行等不符合招标文件规定或合同规定的，甲方有权拒收，乙方应负责更换并承担因更换而支付的一切费用，同时甲方有权追究乙方责任。因更换而造成逾期交付，则按逾期交付处理。

3、若乙方未能按合同约定的时间完成交付或提供服务，除不可抗力事件外，每逾期一日，乙方应按合同总金额的 0.1%向甲方支付违约金；逾期超过 15 日的，甲方有权单方解除合同，乙方按本合同总金额的 20%支付违约金、赔偿退还甲方已支付的全部费用并赔偿甲方因此遭受的全部损失。

4、乙方交付的服务成果经甲方验收不合格的，乙方应在甲方要求期限内完成整改并重新提交验收。整改后仍不合格的，甲方有权解除合同，并要求乙方退还已支付的全部款项，同时乙方应向甲方支付合同总金额 20%的违约金并赔偿甲方全部损失。

5、因乙方运维疏漏、工具失效、应急处置不当引发甲方网页篡改、数据泄露、勒索病毒、高危入侵、等保测评不通过等安全事件，乙方免费提供全部应急处置、系统加固、复测整改服务，并赔偿甲方全部经济损失；同时甲方扣除合同总金额 10%作为处罚，情节严重直接解除合同，乙方仍需退还甲方支付的全部费用。

6、甲方无故逾期支付合同款项的，自逾期之日起，以逾期未付金额为基数，按同期全国银行间同业拆借中心公布的一年期贷款市场报价利率（LPR）计算违约金。

九、争议解决

本合同签订和履行适用中华人民共和国法律，甲乙双方因服务质量问题发生争议，由合同签订地质量技术鉴定单位进行服务质量鉴定；因履行合同发生的争议，由甲乙双方协商解决，如协商不成可向甲方所在地人民法院诉讼。

十、合同生效及其他

1、本合同经甲乙双方代表签字、加盖公章后生效。

2、本合同一式八份，甲方执六份，乙方执两份，具有同等法律效力。

(签署页，以下无正文)

甲方名称：郑州信息科技职业学院（印章）

乙方名称：河南合众信泰科技有限公司（印章）

法定代表人或其委托代理人：（签字）：

法定代表人或其委托代理人（签字）：

地址：郑州市郑东新区龙子湖高校区龙子湖北路 36 号

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

邮政编码：450000

电 话：0371-65927612

电 话：0371-65616616

纳税人识别号：12410000572452504K

纳税人识别号：914101056871236046

开户银行：建行郑州龙子湖支行

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：41050167281709666668

帐 户：16048201040004028

日期：2026.8.24

日期：2026.8.24

附件 1：服务分项价格表

序号	货物或服务名称	品牌	规格型号	单位	数量	单价	小计	产地	合计
1	数据安全管理与监测运营服务	合众信泰	技术服务	年	1	238800.00	238800.00	河南郑州	238800.00
2	网络安全险服务	合众信泰	技术服务	年	1	50000.00	50000.00	河南郑州	50000.00
3	终端安全管理系统	三六零	360 终端安全管理 系统 V12.0	年	1	50000.00	50000.00	北京	50000.00
4	资产梳理与暴露面 检测服务	合众信泰	技术服务	年	1	146600.00	146600.00	河南郑州	146600.00
5	网站监测服务	合众信泰	技术服务	年	1	127360.00	127360.00	河南郑州	127360.00
6	软件成分分析系统	安恒信息	DAS-SCA-130H3	套	1	198000.00	198000.00	浙江杭州	198000.00
7	重保支持服务	合众信泰	技术服务	年	1	50000.00	50000.00	河南郑州	50000.00
8	等级保护测评服务	合众信泰	技术服务	项	1	150000.00	150000.00	河南郑州	150000.00
9	数据安全分类分级 服务	合众信泰	技术服务	年	1	227000.00	227000.00	河南郑州	227000.00
10	驻场服务	合众信泰	技术服务	年	1	360000.00	360000.00	河南郑州	360000.00
合计：¥1597760.00 元（人民币壹佰伍拾玖万柒仟柒佰陆拾元整）									

附件 2：成交通知书

72671

成交通知书

项目编号：豫财磋商采购-2026-771

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与数据安全运营服务项目
成交范围	详见竞争性磋商文件
采购方式	竞争性磋商
成交金额（元）	大写：人民币壹佰伍拾玖万柒仟柒佰陆拾元整
	小写：¥1597760.00 元
质量要求	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
服务期	1 年
质保期	软件成分分析系统 5 年
根据 <u>郑州信息科技职业学院网络安全与数据安全运营服务项目</u> 竞争性磋商文件和你公司 2026 年 08 月 03 日 09 时 00 分提交的响应文件，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） 2026 年 08 月 04 日	

附件 3：主要技术参数或功能

名称	主要技术参数或功能
数据安全 管理与监 测运营服 务	1. 提供本地化部署包含数据安全风险监测工具(以下简称监测工具)的软硬件一体化设备,满足学校 7×24 小时持续监测服务,范围覆盖数据中台及核心业务系统(含教学、教务、学生、科研等)的数据流转、API 接口调用及数据访问行为。 2. 基于自动化的数据安全风险监测工具,结合数据分类分级、人工运营研判,提供常态化数据安全监测与运营服务。通过策略同步、风险监测、告警分析、API 监测、数据流转分析及态势感知可视化等手段,实现数据安全风险“可追溯”、态势“可感知”、效果“可量化”的运营目标,并定期输出风险分析报告与运营总结报告,为数据安全策略优化与风险处置提供决策支撑; 3. 项目实施期间,提供定期现场服务+远程专家支持服务。服务人员具备丰富的数据安全风险监测、研判与运营经验,熟悉数据全生命周期风险场景,并能熟练使用相关监测分析工具; 4. 策略配置与同步:支持依据开已有的数据分类分级结果(包括但不限于数据敏感等级、数据类别标签),将分类分级结果同步至数据安全平台; 5. 监测工具支持对监测发现的数据安全风险进行深入研判分析,结合业务系统信息、数据流向、数据类别、数据级别、取证文件,确认风险性质与影响范围; 6. 监测工具支持对数据安全告警进行多维度统计分析,包括告警类型、告警级别、数据类别、数据级别、处置状态等; 7. 监测工具具备对 API 接口调用行为的监测与分析能力,能够对接口传输内容进行解析与识别,监测异常调用行为,支持识别主流的接口脆弱性风险,支持 OWASP TOP10 风险识别,包括支持身份认证失败 / 缺陷、资源消耗无限制、敏感业务访问无限制、服务端请求伪造(SSRF)、错误的安全配置、存量资产管理不当。并结合 API 脆弱性检测,全面评估 API 接口的数据安全风险; 8. 技术工具支持对数据在内部系统间、内外网间的流转路径进行可视化追踪与分析,识别异常流转行为及数据出境风险,形成数据流转拓扑视图,辅助

	数据合规与风险研判； 9. 每月输出一份《数据安全风险分析报告》，报告内容应至少包括本期风险监测概况、重点风险事件详析、取证文件以及针对性的处置建议； 10. 监测工具通过评测机构的第三方测试； 11. 结合日常运营情况，每半年对数据安全运营工作进行系统性总结与分析，并输出《数据安全运营分析报告》。
网络安全险服务	1. 服务提供由保险公司提供最高 100 万保额的网络安全险保障； 2. 服务范围内的资产在服务期内如若遭受网络攻击或网络安全事故，可依据实际情况对应急响应费用、网络勒索处置费用、数据及硬件恢复费用进行定量理赔； 3. 合同签署后交付由保险公司出具的保单凭证以及保险理赔条款。
终端安全管理系统	1. 终端安全管理系统包含不少于 5000 台计算机终端授权； 2. 支持防病毒、漏洞补丁、防弹窗、软件分发、隐私防护、应用感知、系统优化等功能。支持 Windows、麒麟、统信等主流操作系统 PC 客户端；
资产梳理与暴露面检测服务	1. 暴露面监测服务：通过单位全称、关键字、出口 IP 等信息，收集单位/企业信息、邮箱信息、敏感代码、敏感文档、app 程序、微信小程序、微信公众号等外部/互联网攻击面信息； 2. 二级域名扫描：支持二级域名扫描功能，输入一级域名进行一键扫描，通过搜索互联网数据，自动获取到该域名的二级域名、网站标题、解析 IP 地址； 3. IP 反查域名监测：输入 IP 或者网段，通过搜索互联网数据，自动获取到 IP 对应的域名、url 链接、网站标题、返回状态码； 4. 网站资产相关度分析：通过爬取单位已知的网站页面，分析网页中是否包含单位相关的网站链接，从而发现未知网站；可配置“网段、域名”等命中规则，自动判断是否属于单位的网址； 5. 支持自动识别网站资产信息，包括：“中间件信息、web 框架信息、CMS&OA、程序语言”等指纹信息，支持爬取网站后台、ICP 备案编号、网站标题、网站返回码等属性，形成网站资产台账； 6. 支持通过导入现有资产信息，或在线编辑方式，录入网站资产的管理信息，

	比如网站所属部门、负责人、联系方式、资产价值、物理位置等； 7. 支持对状态码、IP、资产组、部门、责任人、URL、子域名、易危组件、中间件、ICP 备案号、公安备案号、归属地等进行精准搜索或模糊搜索； 8. 支持对已知 url 资产进行深度扫描，进一步发现登录后台和 API 接口，并识别是否暴露外网； 9. 支持以组织架构视角、自定义分组视角、网络空间视角根据 Web 资产、主机资产、域名资产、端口资产和组件资产进行分类，展示资产具体信息，包括但不限于资产名称、资产类型、资产重要等级、资产等级、资产互联网暴露情况、检出时间等信息； 10. 支持管理资产归属信息，通过将资产与单位、人员、地域、业务系统进行关联，明确资产归属和管理责任； 11. 针对可能泄露在外的涉及重要系统的邮件配置信息、数据库配置信息、FTP 配置信息、SVN 配置信息等等系统敏感数据进行识别发现，以及对百度网盘、百度文库、csdn 等互联网侧重点区域进行敏感数据发现及暴露面识别； 12. 主动探测并梳理与学校相关的泄露信息、敏感文件、失陷资产、威胁情报、黑产等内容，协助用户掌握数据资产情况； 13. 服务支持通过互联网接入的方式进行暴露面探测，可发现互联网业务系统高危指纹组件、开放端口、域名资产等； 14. 资产梳理服务工具支持但不限于以下能力： （1）能对目标设备的其他信息进行探测，包括但不限于网络设备类型识别、嵌入式设备类型识别、智能终端类型识别、虚拟化组件类型识别、安全防护设备识别等； （2）支持以组织架构视角、自定义分组视角、网络空间视角根据 Web 资产、主机资产、域名资产、端口资产和组件资产进行分类，展示资产具体信息，包括但不限于资产名称、资产类型、资产重要等级、资产等级、资产互联网暴露情况、检出时间等信息； （3）支持以业务系统的维度进行资产管理，支持录入或批量导入系统基础信息、系统关联资产信息（IP、域名、访问地址）、系统架构信息（开发语言、版本、服务组件等）、业务系统联系人，支持上传系统业务拓扑图，直观展示
--	--

	业务系统整体状态； 15. 提供资产漏洞评估工具，机架式设备，默认配置 4 个千兆电口，2 个万兆光口，64G 内存，2T 硬盘存储空间，冗余电源，无限 IP 授权，具备系统漏洞扫描、弱口令扫描评估、WEB 漏洞扫描、配置基线核查、蜜罐威胁诱捕、主机 Agent 威胁监测、主机漏洞屏蔽、黑链监测、DNS 域名监测功能； 16. 交付物：可使用的系统访问服务；按月定期总结向学校提供《资产台账》、《资产风险处置报告》。
网站监测服务	1. 为学校至少 100 个二级域名对应的网站（站群系统中在用网站）提供网站监测服务。本地化提供对网站的“漏洞、篡改、黑链、敏感文件、敏感词、网马监测、可用性、域名劫持”等 8 个维度开展实时监测，监测频率 5 分钟/次； 2. 网页敏感词监测：持续对网站主要页面进行监测，精准匹配敏感信息，发现网页敏感词事件第一时间通过微信通知学校，同时监测内容自动记录在报告中； 3. 敏感文件事件泄露监测：可监测发布到网上的 pdf、word、excel 文件中是否包含“身份证号、邮箱、手机号码、用户名/密码”等敏感信息，可在系统上查看泄露的信息以及敏感文件下载链接； 4. 敏感内容审查工具：可上传文件(pdf\word\excel)、或者粘贴内容进行敏感词审查，内置敏感词库 10 万+，支持人工再确认审查结果； 5. 网站挂马和黑链监测：对网站的挂马、暗链篡改进行监控，自动发现并人工验证，第一时间通知学校； 6. 网站页面篡改监测：对目标站点页面进行实时篡改监测，包含赌博、色情、涉政、营销类黑产（包括假证、卖药、代孕、医疗、武器等）、游戏外挂等，一旦发现被篡改第一时间对学校进行告警，同时电话主动通知学校； 7. 互联网漏洞监测：在学校授权之后，进行一次扫描，模拟攻击视角从互联网对网站的漏洞进行检测，对检测发现的高危漏洞进行专家验证，并实时向学校通告； 8. 网站可用性监测：多节点对网站的可用性进行探测，实时监测网站运行状况，及时发现断网故障，主动告警通知。支持网站故障原因定位，不限于：

	响应连接被重置、连接超时、HTTP 状态码、连接被拒绝等； 9. 定期总结报告：定期总结网站安全问题，向学校提供《安全运营周报》《每月安全运营报告》《季度安全运营报告》。
软件成分分析系统	1. 提供软件成分分析服务工具全模块系统 1 套，满足本地化安装部署运行，质保服务期 5 年；系统内容包含开发框架、应用程序、云端程序、接口及第三方组件和应用配置等方面进行深入的安全分析，从而发现系统源代码存在的安全问题，并采用安全测试等技术手段进行验证； 2. 支持对学校校园网应用系统的源代码及相关版本信息进行开源组件成分分析，识别出学校当前使用的全量开源组件资产和清单。开源组件资产包括每个组件的名称、版本、法律协议、组件影响的项目等信息。漏洞清单包括漏洞的基本信息、漏洞影响的组件版本、影响的项目以及解决方案等； 3. 基于软件开发安全生命周期管理的开源组件检测系统。支持对源代码、二进制文件、镜像及特征文件中的开源组件进行静态解析； 4. 软件开发或测试过程中，对软件源代码、特征文件、二进制文件进行安全检验，通过对相应文件中开源组件进行全面检测和分析，发现并同步缺陷管理平台其中存在的安全缺陷； 5. 支持解析语言包含但不限于 JAVA/JavaScript/Python/Golang/PHP/C/C++/.Net/Ruby/Scala/Perl/Erlang/Clojure/R；支持代码仓库包含但不限于 Gitlab、Gerrit、SVN、FTP 等；支持镜像仓库包含但不限于 Dockerhub、Harbor、Nexus、Artifactory；支持与 Jenkins、IDEA、VScode 等集成，并提供相关组件修复建议和漏洞修复建议，助力开发人员及时修复风险； 6. 第三方组件审计：审计软件中使用的第三方组件和开源库，检查其安全性和可靠性，防止因第三方组件漏洞而导致的安全风险； 7. 合规性审计：审计代码是否符合相关的法律法规和行业标准，包括隐私保护、数据安全、网络安全等方面的合规性要求； 8. 应严格按照应用代码审计流程开展审计工作，在审计前期应做好应审计范围、审计对象、审计要求的确认工作；在审计中期使用自研的代码审计工具开展审计工作并做好人工审核；在审计后期应输出审计结果并汇报；

	9. 提供 Ai 大数据管理与分析服务工具（无限资产数）、安全编排与协同响应服务工具（支持实现与校园网任何第三方安全设备或业务系统联动对接，实现剧本搭建及事件处置）；支持与学校全网日志数据分析系统对接，实现翻墙监测及预警展示；
重保支持服务	1. 重保支持服务： （1）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； （2）攻防演练及重保期间根据学校的实际需要，增派驻场人员，执行 7*24 小时值守（每年不少于 60 天），含漏洞发现、安全加固、威胁发现、应急处置等； （3）输出《重保值守服务方案》《安全事件分析报告》《重保值守总结报告》； （4）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投标商连续半年的社保证明材料。
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； 2. 完成学校不少于 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； 3. 必须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）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技术指南》（GB/T36627-2018）、《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)、《信息安全风险评估规范》(GB/T 20984-2007)、《教育行业信息系统安全等级保护定级工作指南》等。 4. 按照信息安全等级的测评标准进行安全等级测评; 5. 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; 6. 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; 7. 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; 8. 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; 9. 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。
数据安全分类分级服务	1. 提供本地化部署的结合人工智能技术应用的数据安全分类分级工具; 2. 提供学校指定系统数据库, 10 万字段以上的数据分类分级服务; 3. 服务以“大模型工具+人工”相结合的模式, 开展数据分类分级工作。参照教育行业数据分类分级相关标准与规范, 结合实际业务情况, 对学校核心数据库中包含的教学、教务、学生、科研等数据进行分类管理, 并根据数据敏感程度划分敏感等级, 生成数据分类分级目录清单; 通过该服务, 全面、清晰地盘点数据资产, 明确数据重要性及敏感程度, 实现对数据资产的规范化、精细化管理, 为后续数据安全策略制定与分级管控提供基础支撑;

	4. 项目实施期间，配置 2 名实施人员。实施人员熟悉数据安全、数据分类分级等相关法律法规及文件要求，具备一定的数据资产盘点、数据分类分级及数据资产风险评估实践经验，并能熟练使用相关工具； 5. 分类分级工具支持基于大模型的语义分析及 RAG 知识库检索增强技术，对系统中的敏感数据和重要业务进行自动识别，对重要数据及核心数据进行统计，建立重要数据目录； 6. 分类分级工具支持对于缺少字段中文注释和表注释的字段内容，利用大模型的核心推理能力，进行字段内容推测和分类分级打标。支持按照业务系统批量生成数据库注释，并且能够查看业务系统表数量、表注释数量、表注释去重数量、表注释填充率、字段适量、字段注释数量、字段注释去重数量、字段注释填充率、注释生成进度； 7. 支持文件嵌入识别；支持打入压缩包、多层嵌套识别；支持文档内容伪装识别：能够识别隐藏在文档中各个位置，如页眉、页脚、文本框、表格、批注、备注等；支持文件格式伪装识别：能够识别更改文件后缀、更改压缩包后缀等情况；支持文件分卷伪装识别；支持支持文件加密识别； 8. 分类分级工具支持知识库配置、分类任务下发、数据库聚类分析、数据库分类结果核验、模型调优报告等能力，为数据分类分级的准确性提供支撑； 9. 分类分级工具通过第三方机构的 AI+数据分类分级产品检验； 10. 分类分级工具支持分类分级任务动态展示及多元统计分析能力，能够展示分类分级任务运行开始时间、预计结束时间、运行结束时间、调度类型、进度、状态，并支持对分类分级任务全部、未启动、执行中、已完成、处理异常、手动终止、暂停等不同状态的数量统计分析及展现。
驻场服务	一、驻场运维服务范围 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； 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； 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； 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； 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； 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； 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； 8. 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； 9. 在校园网管理部门的安排下对学校网络运行的各种工作进行劳务支持。 二、驻场运维服务内容 10. 提供数据中心资产的安全运维服务，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. 结合安全工具发现的资产信息，按照学校格式要求，结合实际情况，对服务范围内资产的进行全面梳理。梳理的信息至少包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑等，并将信息同步交付给校方进行存档管理；当资产发生变更时，运维工程师对变更信息持续跟踪、信息确认与记录更新； 12. 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. 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. 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，发起变更流程，更新安全配置基线，持续优化和维护资产的静态安全性；
--	--

	15. 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. 协助建立规范的安全事件响应规范，根据规范，结合网络安全场景，制定行之有效的安全事件响应流程和操作脚本手册。基于威胁监测和态势感知平台对各类安全数据及日志数据进行关联分析与深入挖掘，及时发现各类安全事件并通知客户，同时协助客户开展通报、处置等响应动作，协助快速恢复业务，消除或减轻影响； 17. 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持续跟踪和处置； 18. 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，或在巡检当中发现问题时开始计算，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，必须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：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； 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； 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； 22. 根据用户系统的运行使用情况，及时向用户提出系统安全及系统优化的合理建议，确保用户系统安全正常运行。当用户的各项系统或设备出现与其它系统或设备或第三方厂家系统或产品需要协调的问题时，根据网络管理部门要求派工程师到现场协助协调、解决问题或提出合理化建议。根据网络管理部门的应用要求，重新配置、优化系统资源，包括网络、服务器、存储、安全设备等设备设施的资源调配和调整，操作系统的安装、配置和升级，基础数据库软件的升级等； 23. 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。建立专门的系统维护档案及日志，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。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； 三、风险评估服务 24. 风险评估：2 次/年 （1）通过安全专家+工具的形式识别数据中心现有核心资产的脆弱性，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。可能面临的威胁，并充分调研已有的安全控制措施，以综合判断存在的风险。对不同安全设备的安全日志、流量进行关联分析，识别网络和主机中的安全威胁，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；
--	---

	(2) 运维管理评估：对核心资产的密码、日志、版本信息、安全策略等进行检测，发现风险点并给出解决建议； (3) 威胁监测和分析：通过流量镜像对海量流量进行采集，基于 80000+威胁特征库，对于捕获的流量进行存储、分析，内置多重检测引擎，包含入侵检测、web 检测、威胁情报等，结合攻击源、风险等级、地理位置、攻击目标、命中规则数、告警次数等因素综合分析，精准识别攻击源头，发现不同场景下的已知威胁和未知威胁； (4) 实时翻墙上网监测：1. 支持流量加密及非加密场景的翻墙上网行为监测，无需加载证书，可识别主流翻墙工具（如 V2Ray、Surfshark、naiun、clash verge 等）。可关联威胁情报，识别命中非法代理、加密代理节点、订阅链接域名、IP、C2 服务器等违规外联行为。提供翻墙行为专属可视化看板，展示翻墙主机 IP，翻墙主机是否暴露在外网、命中规则类型、目标域名或 IP、翻墙工具、首次发现时间、最近活动时间等关键信息； (5) 主机安全管理服务：主动威胁监测：在用户的服务器、业务系统上安装安全监控软件，主动监测 webshell、暴力破解、异常登录成功、反弹 shell、挖矿检测等，发现可疑的入侵事件，并实时将告警同步到服务平台；Web 日志分析：可输入最新的 web 日志文件以及对应 web 端口号，后续会自动跟踪相同目录下的 web 日志，发现各类 web 入侵攻击，包括但不限于目录穿越、SQL 注入、XSS 跨站脚本攻击、web 路径遍历漏洞攻击，高亮显示攻击特征。文件篡改检测：可检测文件的篡改行为，包括：“创建、写入、修改权限、重命名、删除”等篡改行为；漏洞攻击屏蔽：精准检测恶意攻击源、扫描源，并可基于告警风险值、或者定向源进行屏蔽，即使扫描源接入同一网段扫描，也能实现扫描源可以探测到资产存活但扫不到漏洞的效果，同时支持流量阻断和主机屏蔽 2 种模式； (6) AI 研判和人工验证：联动本地 DeepSeek AI 模型，联动分析“流量、蜜罐、主机”三者告警结论，关联“资产+漏洞”信息，辅助输出综合研判结果：1. 给攻击源 IP 定性并打上攻击者标签，如：非法外联、外网恶意攻击、内网恶意攻击、漏洞利用成功等。2. 输出攻击源资产画像，包括网络区域、主机名称、MAC 地址等。接入 DeepSeek 大模型的云端 AI 智能体，支持深度
--	---

	思考模式：1. 支持对流量、蜜罐、主机等告警事件研判，输出研判过程与研判结论。2. 告警传输前可自动过滤“身份证号”、“手机号”、“邮箱”信息，避免客户数据泄露。3. 研判结果包括但不限于：分析 payload 中明显攻击特征，分析响应报文并判断是否攻击成功，关联威胁情报输出病毒外联事件关键点； （7）网络安全加固服务：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；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；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； （8）旁路阻断服务：不需要设备串联、不需要配置策略路由，就能通过监测中心流量监测告警处，对单个 ip 进行手工阻断。也可自动关联流量告警，根据智能研判标签，就会自动触发旁路阻断，包括但不限于非法外联-拦截域名解析的 IP（高风险）、外网恶意攻击（高风险）、利用成功（高风险）、暴力破解（高风险）、外网可疑访问（中风险）等标签，可灵活针对国内/国外 ip 进行灵活封禁，可灵活指定封禁时间间隔； （9）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。 25. 漏洞扫描与漏洞管理服务 （1）漏洞生命周期管理：漏洞库漏洞信息大于 340000+条，集成 4500+POC 对内网资产进行自动漏洞验证与渗透，提供详细的漏洞描述和对应的解决方案描述。通过 POC 验证过的漏洞，扫描结果包含漏洞利用证明，包括但不限于攻击 Payload、目标响应结果、漏洞利用点、关键参数等内容。支持漏洞跟踪管理，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注； （2）弱口令扫描研判：支持用户针对指定的目标 IP 与应用，通过在 web 界面上手工输入“用户名、密码”，系统将返回口令登录后的校验结果，确认弱口令是否真实存在； （3）基线配置核查：要求操作系统支持 Windows 2003/2008/2012/2016/2019/7/8/10/11；支持 linux（Centos、Redhat、suse
--	--

	等);应用服务支持 Linux、Windows 下的 Apache、Weblogic、TOMCAT、Nginx, 以及 windows 2003/2008/2012/下 IIS 6/7/8; 数据库支持 Linux、Windows 下 Oracle8i/9i/10/11g、Mysql。大数据应用支持 Flume、HBase、Hadoop、Spark、Storm、Hadoop、ZooKeeper; (4) 服务频次: 1 次/月 (5) 服务完毕后, 出具《网络安全漏洞扫描报告》, 报告内容包含以上所有项目; 四、渗透测试服务 26. 网络安全专业团队对学校重要信息系统进行攻击渗透测试。服务内容如下: (1) 服务工程师在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; (2) 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; (3) 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; (4) 提供渗透测试台账: 以 excel 报表格式导入渗透测试报告, 形成渗透测试台账。可在系统查看渗透测试结果, 以图表形式可视化展现漏洞风险级别比例、风险应用比例, 可对渗透报告中的漏洞进行跟踪确认, 处置漏洞状态: 未整改、已整改、忽略、未整改; (5) 服务完成后编写渗透测试报告, 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《渗透测试服务报告》、《渗透测试复测报告》等服务交付物; (5) 服务频次: 2 次/年 (6) 1 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投标商连续半年的社保证明材料; 27. 在学校数据中心部署攻击者诱捕系统, 对学校重要信息系统进行仿真模
--	--

	拟。服务内容如下： (1) 默认仿真蜜罐：支持至少 10 种可自定义 logo 和公司名称的仿真蜜罐，仿真蜜罐类型包括但不限于：“齐治堡垒机、启明堡垒机、深信服 VPN、泛微 OA、通达 OA、u8crm、wiki、mailcow、bbs 论坛、订单管理系统”； (2) 完全仿真蜜罐：支持通过反向代理的方式，接入用户自身搭建的应用系统，从而实现完全仿真真实业务系统，生成完全仿真蜜罐； (3) 引流防御：可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统； (4) 服务频次：不限次数，不限 IP 数； 五、应急演练服务： 28. 根据学校行业特点和信息安全发展所处阶段，针对不同场景制定相应安全应急预案，通过提供全方位、多形式网络安全应急演练服务，进一步加强网络安全应急响应能力建设，提高应对网络与信息安全事件的响应处置能力，减少网络与信息安全事件造成的危害和损失。服务频次：4 次/年。 六、人员能力要求 29. 项目经理资质：项目经理具有项目经理证书（具备中华人民共和国人力资源和社会保障部、工业和信息化部批准颁发的信息系统项目管理师（高级）证书），提供相关证书和所在投标商连续半年的社保证明材料； 30. 提供驻场工程师 2 名，资质：驻场工程师具有计算机或网络相关专业本科毕业，有两年及以上工作经验，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主流厂商认证的数通方向（IP 级别）认证证书，另一名工程师具备 CISP-PTE 认证证书，且不得是同一人；提供工程师证书和所在投标商连续半年的社保证明材料； 31. 为保证学校网络、数据中心、业务系统的稳定不间断运行，工程师具备专业资格认证、受过良好的技术培训、拥有丰富的工作经验； 32. 二线服务项目的人员 (1) 1 名工程师通过主流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投标商连续半年的社保证明材料；
--	---

	(2) 1 名工程师通过主流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投标商连续半年的社保证明材料； (3) 1 名工程师通过主流厂商认证的云计算方向（IE 级别）的认证，提供工程师证书和所在投标商连续半年的社保证明材料； (4) 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 1 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投标商连续半年的社保证明材料； (5) 1 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投标商连续半年的社保证明材料； 四、保密要求： 33. 服务期内，必须签订保密协议，承诺严格保护用户系统、数据、信息的安全，在服务期满后永久不得泄露用户所有信息。由于服务商违反保密协议而导致的泄密或破坏，由服务商负全责，并由服务商赔偿用户所有损失。提供服务期内保护用户系统、数据、信息的安全，以及服务期满后永久保守用户信息秘密的承诺书。
--	---