2026-2027年度武汉市教育系统网络安全综合服务采购需求

第一章　供应商资格要求

1．满足《中华人民共和国政府采购法》第二十二条规定，即：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

2．未被列入失信被执行人、重大税收违法案件当事人名单，未被列入政府采购严重违法失信行为记录名单；

3．近两年内投标人为国内地市级及以上政府部门网络安全应急服务支撑单位或承担过地市级及以上政府部门合同金额达到80万元的网络安全运维服务类项目，**须提交有效佐证材料**；

4．不接受联合体投标，不允许服务转包或分包；

5．投标人参与电子商城报价时，需同步提交上述资格中要求提交的相关佐证材料，**必须满足“技术及商务要求”中“*”指标项**。否则即便竞价中标，采购方亦将取消其中标资格。

第二章 技术及商务要求

一、 项目背景

为及时发现并处置全市教育系统可能存在的网络安全漏洞及隐患，保障全市教育系统网络安全，武汉市教育科学研究院从2019年开始每年通过

购买服务方式开展全市教育系统网络安全监测。随着网络安全形势的不断变化和防护要求的持续提升，以监测为主的服务已难以全面满足实际工作需求，各类网络安全深度保障服务（如应急响应、安全加固、应急演练、培训指导等）的价值日益凸显。为此，2026~2027 年度拟将原有监测服务升级为涵盖更多保障服务的网络安全综合服务，项目名称相应调整为“2026~2027 年度武汉市教育系统网络安全综合服务项目”，以进一步提升全市教育系统网络安全保障与应急处置能力。

二、 项目时间及付款方式

服务时间 1 年；

合同签订且中标人提供的网络安全管理监测平台满足采购人招标需求及实际工作需要后 15 个工作日内支付 30%预付款，服务期满且通过验收后支付 70%尾款。

三、 服务内容要求

（一）提供安全漏洞检测及安全事件、内容监测服务

对全市教育系统近 300 个网站信息系统（实际数量可有 10%的上下浮动）开展 7×24 小时的安全检测及监测服务，及时发现系统存在的各类安全隐患及安全事件，具体要求如下：

1.服务内容

提供**安全漏洞检测服务**：通过大数据漏洞扫描技术，定期对目标网站进行全面的安全漏洞扫描，发现系统存在的各类安全隐患；

提供**安全事件监测服务**：对网站进行页面资源与指纹信息的分析，通过监测技术对各类安全事件进行全面分析感知，包括篡改、暗链、黑页、挂

马、后门等，并向采购人进行定向安全通报；

提供**内容监测服务**：能识别色情、涉政、暴恐、垃圾广告等敏感词汇，能按采购人要求及时进行安全通报；

提供**人工验证服务**：对发现的漏洞、事件等进行人工验证，以保证结果的准确性。对采购人及下属单位已整改的安全漏洞进行复核，保证整改的有效性；

提供**线上技术支持服务**：对采购人及下属单位漏洞整改提供线上技术支持服务；

* 提供**专项风险扫描及渗透测试服务**：按照采购人需要，针对特定风险隐患开展专项风险扫描及渗透测试服务；

* 提供**高危事件电话提醒服务**：对纳入监测范围站点首页及一级链接页面发生的严重网页篡改、挂马攻击等重大网络安全事件，能够做到事件发生后30分钟之内发现并电话通知采购人。

2.技术能力要求

(1)* 投标人自身具备丰富的网站安全监测资源，全国范围内具备3个（含）以上云监测节点。

(2)所有纳入监测范围内的网站单次遍历扫描监测周期不得超过7天，特殊时期可按照甲方要求缩短监测周期。

(3)网络安全事件及内容监测必须不间断实时监测。

(4)* 具备Web漏洞扫描能力，包括SQL注入漏洞、跨站脚本漏洞、网站第三方应用漏洞、隐藏字段、表单绕过、框架注入等。支持大规模网站漏洞扫描能力。

(5)* 具备安全事件监测能力，对能力范围内的Web资产提供包括暗链、挂马、黑页、webshell、坏链在内的安全事件监测。

(6)具备内容风险监测能力，对能力范围内的Web资产提供包括身份证信息、敏感内容、不良信息在内的内容风险监测。

(7)支持对安全事件进行扫描监测并自定义设置扫描层数。

(8)支持对风险弱点进行处置流程闭环，提供风险弱点的状态跟踪功能。

(9)支持扫描策略的在线自动升级。

(10) 具备7x24小时值守及应急响应能力，要求提供7x24小时应急值守电话并在合同中明确列出。

（二）提供成熟的网络安全管理监测平台

中标人负责平台的日常管理、运维及安全保障工作，负责做好采购人存量数据的迁移，负责按照管理部门要求做好平台的等保、密评等合规性工作，负责承担平台正常运行所需的相关费用。负责保障采购人可正常使用平台开展漏洞处置、通知发布、信息资产管理、信息集中展示及知识库、报平安、责任制考核等工作，其中通知发布、漏洞处置、报平安等功能需支持移动端。

平台需至少具备以下功能模块。

1．漏洞通报处置

（1） 支持将第三方发现的漏洞导入平台，实现多方风险数据的直观展示与通报；通报可下发给指定下级单位，下级单位能够签收及下载通报文件，采购人可了解通报签收情况。

（2） 支持下级单位接到通报提醒后，登录平台对通报进行处置，并按规定提交问题修复情况说明并上传相应的处置材料。

（3） 提供漏洞通报、处置、初审、终审流程管理，支持标注状态（待通报、待处置、待初审、待终审、已完结）及状态更新时短信及邮件提醒。

通报：支持自定义漏洞通报到下级单位，处置不完善的可再次通报；

处置：能选择转发至对应单位，对超期处置的进行催办；

审核：能查看漏洞处置情况，对处置情况进行初审和终审等审核流程。

（4）支持按时间范围、区域、漏洞类型、漏洞级别等条件检索、汇总统计漏洞通报信息。

2．通知公告

（1） 可依据采购人日常工作要求进行通知发布、通知查看状态标注、下级单位提交回执，对回执进行单个及批量下载等操作。

（2） 具备通知列表的展示与通知管理的功能。

（3） 支持使用回执功能自定义下级单位需要回执的信息，例如安全培训的报名表等。提供回执数据的汇总及下载功能，提供回执驳回及催办功能。

（4） 通知发布及催办支持通过短信及邮件进行提醒。

3． 资产管理与探测

（1） 资产信息管理：支持信息系统、网站、联网带屏设备等资产及相关联信息的批量录入、导入、展示及管理；支持自定义资产字段（如负责人、联系方式、物理位置等）；支持自动识别 URL 资产的指纹信息（中间件、Web 框架、CMS、OA、程序语言等）及属性（网站标题、ICP 备案编号、返回码、后台路径等），自动形成网站资产台账。

（2） 主动探测与状态监控：支持通过主域名解析、IP/IP 段扫描、Web 探测等方式发现存活资产（含子域名），可自定义探测周期及资产入库方式（人工确认后入库）；支持实时监控资产状态，展示资产存活信息、Web 访问状态码、主机在线情况。

（3） 资产上报与年审：支持下级单位主动上报资产信息、进行资产备案，由上级单位审核决定是否纳管；支持定期下发资产年审任务，完成资产信息确认与变动资产信息更新。

（4） 业务系统关联与拓扑展示：支持资产与业务系统的快捷关联（无需跳转模块），在业务系统详情中直接编辑资产明细并全局同步；支持直观

展示业务系统、域名、端口、主机、Web 资产及其在线/离线状态。

4. 网络安全报平安

重要时间节点，采购人可发布报平安任务，并通过短信、电子邮件提醒；下级单位按要求上报内部安全情况。支持汇总分析上报数据，以日历形式直观展示报平安记录，并提供查询统计与数据导出功能。

5. 网络安全责任制考核模块

（1） 指标与模板管理：根据采购人实际考核指标灵活设置指标库，自定义考核项及填报表单；可将不同考核项组合为考核模板，供后续任务复用。

（2） 考核任务全流程：支持创建、下发考核任务；下级单位在线填报、上传资料，可手动引用上一年已提交的考核材料；采购人可进行审核、答疑、人工分数修正，并支持根据平台数据自动赋分。

（3） 考核结果应用：支持日常考核与年度考核相结合，年度考核项可直接引用日常考核得分；可查看各单位考核分值、排名及任务状态，支持导出考核总分。

（4） 定制化扩展：能针对采购人后续网络安全责任制考核要求进行定制化开发。

6. 信息集中展示及知识库模块

（1） 提供信息集中展示页面，集中展示资产、监测、运营、通报等维度信息，支持大屏幕自适应展示，便于采购人集中了解安全监测总体情况。

（2） 知识库：提供网络安全应知应会知识库、法律法规及地方条例知识库（及时跟进并更新新出台的法规条例）、网络安全预警及安全资讯以及定期更新国内网络安全执法实例的执法案例知识库。

7. 组织机构管理

（1）支持市、区、校三级管理。市级管理员可管理区级及市直属单位，区级可管理本区所属单位。上级管理员可添加、修改、删除下级管理员账号，可协助市、区管理员批量导入下级单位名称和管理员账号信息。

（2）资产管理、通知公告、安全通报处置模块中区级管理员具备相应管理功能，包括管理区级账号及资产、向区属单位发送通知及接收回执、安全漏洞通报转发及处置等。

（3）密码重置后可提供短信提醒。

8.移动端支持

（1）支持移动端报平安：可通过手机查看报平安任务，支持在重点时期采用移动端界面进行平安上报功能。

（2）支持移动端漏洞处置功能：支持对漏洞通报的查看、下载、转发及整改报告上传等功能。移动端查看通报信息后系统能自动标记，查阅状态需同步到非移动端。

（3）支持移动端查看通知功能：支持对通知内容的查看、附件下载及回执上传等功能。移动端通知查看状态需同步到非移动端。

（三）提供网络安全深度保障服务

1.安全评估与检查服务

（1）网络安全检查：为采购人在其行业内开展网络安全检查提供技术、人员及装备支持等服务，检查内容包括互联网系统渗透测试、漏洞扫描、基线加固、弱口令排查、日志分析、威胁监测等。每年服务不少于 6 次。若服务期内服务次数不满 6 次，未履行部分可根据采购人需要调整为培训服务。

（2）“两高一弱”专项检查：对云上服务器进行安全探测，及时修复高危漏洞；对业务系统进行端口梳理，关闭不必要端口；利用 APT 等工具检测并整改弱口令。

（3）数据安全：协助采购人完成业务数据的分类分级梳理，形成数据资产清单，并针对不同类别和级别明确相应的安全保护要求。

（4）管理部门日常技术支撑：根据采购人需要，提供技术支撑服务，协助采购人完成网络安全管理部门交办的网络安全工作任务。

2. 安全加固与应急响应服务

（1）安全事件响应：提供安全事件响应与处置服务。

（2）现场保障：派遣技术人员到采购人指定现场协助安全事件处置，保障关键重要时期网站安全，每年度不少于6次。若服务期内次数不满6次，未履行部分可根据采购人需要替换为检查或培训服务。

（3）应急演练技术支撑：按照采购人需要提供应急演练支撑，包括制定演练方案、过程监督审计、突发事件应急支撑等。

3.定期制度更新与季度监测报告服务

（1）制度更新服务：根据国家相关法律法规及政策规范，协助采购人每年提供一次网络安全管理体系制度更新服务，覆盖安全管理制度体系、安全管理机构、人员安全管理、系统建设管理、运维安全管理体系等，确保满足现行规范要求。

（2）季度监测报告：每季度出具季度监测情况报告。

4.安全培训与宣传教育服务

（1）网络安全宣传周：提供宣传周主题宣传材料发放、员工有奖答题活动、网络安全视频宣传、海报张贴宣传。

（2）安全专家培训：每年度协助采购人组织安全专家对相关人员开展安全风险意识、安全管理知识、安全应急响应技能等培训，一年不少于6次。

（3）认证培训：提供1人次CISP认证培训或2人次ECSP认证培训。

（4）宣传教育活动：协助采购人开展各类网络安全宣传教育活动（含上述网络安全宣传周活动）。

5.学术研究技术及大型活动支撑服务

（1）根据采购人需要，协助采购人在网络安全、数据治理、人工智能赋能安全、网络安全教育等研究方向提供技术支撑，助力采购人形成相关工作

成果。

（2）大型活动专项支撑：每年支撑采购人完成一次100人以上的大型活动（如应急演练、比赛、展示等），提供活动策划、技术保障、现场执行等支持。

四、 项目预付款支付

中标人在服务合同签订后15个工作日内，须按照采购人要求完成：

1. 网络安全管理监测平台所有功能开发、配置、调试及大屏自适应展示等，经测试符合并满足采购人工作需要。

2. 将采购人存量数据迁移到平台。

中标人完成上述工作内容并经采购人测试并确认满足工作需要后，视为达到采购人支付项目预付款的条件。

在此期间，采购人有权对中标人提供的综合服务能力（尤其是监测服务能力）进行核实，并对管理监测平台的各项功能进行测试。若发生下列任何一种情况，采购人有权终止合同，并追究中标人的违约责任。

1. 中标人实际综合服务能力与投标文件不符；

2. 中标人未在规定时间内完成平台开发并上线运行；

3. 中标人未在规定时间内完成存量数据迁移。

五、 服务质量要求

中标人承诺按招标需求及合同履行服务内容。采购人同意如采购人因工作原因未安排中标人履行相关服务（含技术人员现场人工服务、培训服

务、CISP 认证培训）而导致中标人未完全按合同要求提供所有服务，视为中标人完全履行合同。

1.* 提供 7*24 小时安全专家值守服务，实时发现各类安全威胁，第一时间安全告警通知。需提供 7*24 小时值守电话。

2.* 中标人至少提供安全漏洞及安全事件通报联系人一人，协助采购人管理本项目涉及的网络安全管理监测平台，开展安全事件通报、复核安全漏洞及事件整改情况等。

3.* 中标人提供的涉及本合同范围内的安全漏洞通报、安全事件通报、安全漏洞复核、安全事件整改、现场技术支持、安全事件现场处置、应急演练技术支撑、宣传教育培训等人员均为本公司自有专业技术人员，且以上各工种技术人员总人数不低于 5 人，每人至少具备 CISP 专业资格证书。需提供上述人员证书复印件和加盖公司公章的近 3 个月在职社保证明。

4. 在重要节会时期、大规模 0day 漏洞爆发或其他重大安全事件爆发期间，中标人可提供临时的网站云防护服务，并配备提供 7×24 小时专家团队的监控防护服务。

5. 中标人承诺安全检测和实时监测扫描服务能够基本覆盖所有已知的网络安全风险及安全漏洞，对纳入监测范围内的网站能够及时发现风险及漏洞并通知采购人采取措施及时处置。

6. 中标人承诺经人工审核后发布的安全风险及漏洞是真实有效的，所发布的安全风险及漏洞的误报率不超过 3%。

7. 服务结束时，中标人须协助采购人将网络安全管理监测平台中所有相关数据以结构化数据的形式导出并交由采购人保存。

8. 若因中标人未切实履行网络安全保护义务，导致其提供的网络安全管理监测平台发生网络安全事件，并对采购人造成较大责任风险，采购人有权拒绝支付合同尾款，并可依据自身权益受损情况向中标人提出索赔。

六、 服务考核

为规范运维服务管理，保证服务质量，采购人每年度对中标人实行百分制考核，考核办法可参照《武汉市教育科学研究院网络安全综合服务考核细则》，考核情况作为衡量中标人服务质量的依据。在本项目合同签订时，采购人可根据实际情况与中标人协商对考核细则进行调整。

武汉市教育科学研究院网络安全综合服务考核细则

第一条 为了规范对网络安全综合服务中标人的管理，保证服务质量，结合采购人的实际情况，制定本考核办法。

第二条 以年度为单位对中标人实行百分制考核，评分结果作为衡量服务质量的依据。考核等级分为 “非常满意”、“满意”、“一般”、“不满意”四档，对应的分数为“100-95 分”、 “94-80 分”、“79-60 分”、“60 分以下”。如考核结果为“非常满意”或“满意”，不扣服务费；如考核为“一般”，不足 80 分的部分，按每分 3000 元的标准在剩余合同款项中扣除；如考核结果为“不满意”的，在扣除服务费 60,000 元的基础上，不足 60 分的部分，按每分 3000 元的标准在服务费中继续扣除。考核结果为不满意的，采购人将拒绝中标人今后参与本项目。

第三条 中标人接到采购人安排的合同范围内服务项目后，未在 1 个工作日内响应，或虽响应但未在约定时限内完成（不可抗力或经采购人书面同意的情况除外），视为一次履约延迟，每发生 1 次扣 10 分。

第四条 中标人安排的安全漏洞复核、安全事件整改、现场技术支持、安全事件现场处置、应急演练技术支撑、宣传教育培训等服务人员，若出现不具备合同约定的专业资质（如无资质证书或与合同要求不符等），或因专业能力不足导致现场无法提供有效服务且经采购人指出后 24 小时内仍不能解决问题或替换合格人员的情形，每发生一人次扣 5 分。

第五条 中标人安排的安全漏洞及安全事件通报联系人，在甲方联系 10 分钟之后仍不能及时响应的，每发生一次扣 2 分；拒绝合理服务要求或服务过程中态度恶劣，每发生一次扣 5 分。

第六条 中标人安排的现场技术服务人员不按照采购人合理要求提供服务、服务过程中态度恶劣、擅自从事与职责无关的其他事项而导致采购人声誉或利益受损，每发生一次扣 5 分。

第七条 纳入监测范围内网站因网站首页、一级页面被篡改、挂马等攻击

而发生重大网络安全事件后中标人未能在 30 分钟之内电话通知采购人，每发生一次扣 30 分。

第八条 纳入监测范围内网站出现高危漏洞后中标人未先于采购人上级单位发现而导致采购人被通报，每发生一次扣 2 分。

第九条 中标人提供的网络安全漏洞和事件通报每误报 1 次扣 1 分。

第十条 中标人提供的网络安全管理监测平台在未提前通知采购人的前提下无法打开或出现功能故障，每发生 1 次扣 1 分。

第十一条 中标人因自身原因导致采购人数据及信息泄露，每发生一次扣 10 分。

第十二条 中标人提供的网络安全管理监测平台因未做好网络安全合规或安全防护工作等原因导致采购人受到管理部门通报，对采购人合法权益造成损害的，每发生一次扣 20 分。

第十三条 本考核办法的解释权归采购人所有。