网络安全运维服务采购需求

武汉市肺科医院（武汉市结核病防治所）

2026 年 6 月

一、项目概况

1.1 项目背景

为落实《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》等法律法规要求，加强医院电子病历系统应用水平分级评价、医院信息互联互通标准化成熟度测评中相关网络安全工作要求，全面强化武汉市肺科医院网络与信息安全防护能力，确保医院核心业务系统稳定、安全运行，现开展武汉市肺科医院 2026 年度网络安全运维服务采购工作。

1.2 项目目标

- 建立常态化的网络安全运维机制，实现安全资产全生命周期管理和安全威胁实时监测；
- 通过安全工具部署、漏洞扫描加固、渗透测试等手段，全面识别并消除信息系统安全隐患；
- 完善安全事件应急响应体系，确保突发网络安全事件后快速响应、有效处置，最大限度降低安全事件影响；
- 建立重保时期多级联动保障机制，确保关键节点网络安全零事故；
- 通过安全知识培训，提升医院工作人员网络安全意识和防护能力；

- 协助采购人完成主管部门下达的网络安全绩效考核相关指标。

1.3 服务期限

自采购人书面通知开工之日起计算一年。

1.4 预算金额

预算金额：人民币肆拾万元整（¥400,000.00，含税全包价）。

二、运维服务范围

本项目运维服务范围涵盖武汉市肺科医院核心业务信息系统，包括但不限于：医院信息系统（HIS）、实验室信息管理系统（LIS）、医学影像存档与通信系统（PACS）、电子病历系统（EMR）、医院信息集成平台、互联网医院系统、数智化病理系统、办公 OA 系统、医院官方网站等。为上述系统提供网络安全防护、日常监控告警、漏洞扫描加固、安全事件处置、安全设备维护、重大节日保障等全周期安全运维保障，支撑采购人各项诊疗业务、公共卫生服务与信息化系统稳定安全运行。

本项目包含以下 13 项安全运维服务：

序号	服务项目	服务频率
1	驻场运维服务	1 年
2	资产识别梳理服务	持续更新
3	基线核查服务	2 次/年

4	威胁分析处置	持续
5	漏洞扫描服务	4 次/年
6	新应用上线测试	按需
7	渗透测试服务	2 次/年
8	重保服务	全年（含全部法定节假日）
9	应急响应服务	全年
10	一体化安服工具服务	全年
11	互联网出口防护服务	全年
12	安全设备配置操作手册编制服务	持续更新
13	安全意识培训服务	至少 1 次/年

三、技术要求

3.1 驻场运维与日常安全服务

1. 驻场运维服务

- 供应商须提供一名具备网络安全中级职称或 CISP 认证资质的人员进行 5×8 小时驻场服务；

- 驻场人员须建立安全资产动态清单，定期检查并记录安全设备健康状态、更新设备规则库、核查安全策略有效性；
- 驻场人员须开展日常安全巡检，出现安全问题及时通报采购人并联动二线安全专家进行处置；
- 驻场人员须提供日常安全咨询服务，包括网络安全相关项目立项论证、技术审查、问题解答等；
- 驻场人员须配合采购人开展上级单位网络安全考核、等级保护测评等相关工作事务；
- 完成采购人交办的其他网络安全相关工作事务。

2. 资产识别梳理服务

- 利用专业工具结合人工方式，对安全设备进行全面的资产统计；
- 收集 IP 信息、开放端口、业务系统名称等关键信息；
- 形成安全资产清单并持续动态更新。

3. 基线核查服务（2 次/年）

- 对核心业务系统的服务器、操作系统等基于信息安全风险的视角进行配置核查；
- 检测错误配置及弱策略等安全隐患，提出整改建议；
- 协助运维人员优化配置策略，达到相应的安全防护要求。

4. 运维手册编制服务

- 根据采购人网络安全工作需要，编制关键安全设备《安全设备配置操作手册》；

- 《安全设备配置操作手册》须持续更新，重大系统变更后 5 个工作日内完成更新。

3.2 威胁监测与安全分析服务

1. 威胁分析处置

- 供应商须配置不少于 2 人的安全专家团队，在服务期内持续对不同安全设备的安全日志、流量进行关联分析；
- 主动识别网络和主机中的安全威胁，协助采购人处置安全事件；
- 每次安全事件处置后须提供加固建议和处置报告。

2. 漏洞扫描服务（4 次/年）

- 使用专业漏洞扫描工具对核心业务系统、数据库、操作系统、中间件等进行漏洞、端口、弱口令的扫描检测；
- 扫描完成后由技术人员对漏洞进行确认测试；
- 提出整改建议，并持续跟踪督导系统运维人员落实整改工作。

3. 新应用上线测试

- 模拟黑客攻击测试目标系统，通过安全专家测试发现平台工具无法检测到的漏洞与威胁；
- 上线测试须覆盖：配置管理、身份认证、会话管理、授权测试、上传下载、信息泄露、数据存储等方面；
- 须覆盖 XSS 跨站脚本攻击漏洞、SQL 注入漏洞等 OWASP 十大漏洞；
- 测试完成后须提交安全检测报告。

4. 渗透测试服务（2 次/年）

- 通过搜索引擎侦测、专业化工具检测结合人工分析，确定信息资产的网络暴露面；
- 业务系统配置管理方面安全测试：包括敏感目录遍历、Robots 方式的敏感接口查找、HTTP 开启方法测试等；
- 业务系统认证方面安全测试：包括登录验证码、认证错误提示、锁定策略、认证绕过等测试；
- 业务系统会话管理方面安全测试：包括会话变量泄露、Cookie 属性测试、Cookie 存储方式测试等；
- 业务系统授权方面安全测试：包括绕过授权模式测试、横向提权测试、纵向越权测试等；
- 业务系统文件上传下载方面安全测试：包括 HTTP PUT/MOVE 上传文件测试、页面上传测试、文件下载测试等；
- 业务系统信息泄露方面安全测试：包括连接数据库的账号密码加密测试、客户端源代码敏感信息测试等。

5. 安全工作月报

- 组织月度例会，汇报本月采购人网络安全工作情况，包括资产识别更新情况、本月威胁监测情况、《安全设备配置操作手册》本月更新情况等。

3.3 应急响应与重保服务

1. 重保服务

- 供应商须提供多名专业安全服务工程师组成的重保团队，包括现场网络安全数据分析师、安全运营人员、安全值守人员等；
- 配备二线和三线远程后台支撑服务团队；
- 重保覆盖时间为全部法定节假日及上级单位临时通知时段（元旦 1 天、春节 8 天、清明节 3 天、劳动节 5 天、端午节 3 天、国庆节 7 天、中秋节 1 天等），全年不低于 28 天；
- 在上级单位攻防演练时期，提供网络安全技术人员团队 7×24 小时现场保障；
- 重保期间，实时监控网络流量、安全设备告警及日志审计信息，及时发现并处置潜在威胁；
- 配合攻防演练开展漏洞排查、应急响应和攻击溯源工作，确保业务系统持续稳定运行；
- 建立多级联动机制，强化与上级单位的协同配合，按要求报送安全态势和重大事件进展，严格落实值守记录和交接班制度，保障关键节点零事故。

2. 应急响应服务

- 当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，供应商须提供包括事件检测与分析、风险抑制、问题根除、协助业务恢复的全流程应急响应服务；
- 远程服务响应：15 分钟之内电话响应；

- 现场服务响应：突发网络安全事件 15 分钟之内电话响应，1 小时内到达采购人现场进行应急响应；
- 每次应急事件处置后须提交应急响应报告。

3.4 安全工具与培训服务

1. 一体化安服工具服务

- 提供一体化安全服务工具，具备脆弱性管理及漏洞无效化能力；
- 对于无法常规整改的漏洞，提供漏洞无效化技术手段，使扫描器可扫描到资产但扫描不到漏洞；
- 安服工具须提供资产管理、脆弱性管理、威胁监测、响应与处置等能力；
- 所有安全数据统一汇总在安服工具上，采购人可随时使用安服工具功能及查看安全数据。

2. 互联网出口防护服务

- 为采购人互联网出口提供防火墙防护服务，涵盖策略优化、实时阻断、恶意域名与 IP 地址动态封禁，确保出口流量可视、可管、可控。

3. 安全意识培训服务

- 邀请行业安全专家对医院工作人员进行至少 1 次安全意识培训；
- 培训须交付：培训计划、培训课件、签到表、培训评估报告等资料；
- 培训内容包括但不限于：网络安全法律法规、常见网络攻击类型及防范措施、日常安全操作规范、数据安全与隐私保护等。

3.5 SLA 服务级别要求

故障等级定义与响应要求：

故障级别	故障描述	响应时间	临时解决方案时限	彻底修复方案时限
一级故障 MTTR	网络安全相关原因引起的核心系统完全瘫痪（如全院系统宕机、数据库损坏），导致门急诊/住院/收费等全部中断，或造成患者安全严重威胁、医疗数据丢失。	15 分钟内	2 小时内	24 小时内
二级故障 MTTR	网络安全相关原因引起的核心业务主要模块不可用（如住院医嘱、电子病历系统失效），影响大面积用户但有部分替代流程，虽未完全瘫痪，但严重影响诊疗效率并存在患者安全隐患。	30 分钟内	4 小时内	72 小时内
三级故障 MTTR	网络安全相关原因引起的非核心功能受限或性能严重下降（如报表系统故障、部分科室打印异常），有可行的变通方法，不直接威胁患者安全，但对局部工作效率影响较大。	2 小时内	3 个工作日内	10 个工作日内
四级故障 MTTR	网络安全相关原因引起的单点问题或界面瑕疵（如某客户端显示错位、非关键数据查询失败），不影响正常医疗业务流程，用户可自行绕过或问题轻微。	8 小时内	10 个工作日内	30 个工作日内

四、商务要求

4.1 服务周期

- 服务周期：自采购人书面通知中标人开工之日起计算一年。

4.2 付款方式

付款方式：转账。供应商在每次收款前，均应当向采购人开具等额有效的正规发票。费用按如下方式支付：

第一阶段，即首期款阶段。在合同签订生效且项目前期准备工作（涵盖运维服务需求调研报告、运维服务方案等）完成，并经甲乙双方确认后的 30 个工作日内，甲方向乙方支付本合同总额的 15%。

第二阶段为进度款支付阶段。在合同执行满六个月后，以本合同总额的 35%作为进度款阶段计划支付金额，甲方依据前六个月内服务质量评价结果对照惩罚条款执行费用扣减，经甲乙双方确认后的 30 个工作日内，向乙方支付实际应付金额（实际应付金额=进度款支付金额 - 惩罚扣减金额）。

第三阶段为合同期满且终验完成阶段，在所有交付物均已完备，项目通过审计及终验合格，以本合同总额的 50%作为完成阶段计划支付金额，甲方依据年度服务评价结果对照惩罚条款执行费用扣减，经甲乙双方确认后的 30 个工作日内，向乙方支付实际应付金额（实际应付金额=计划支付金额 - 惩罚扣减金额 - 审计扣减金额）。

4.3 保密要求

- 供应商及服务团队成员须签署保密协议，对服务过程中接触到的所有信息严格保密；

- 严禁泄露医院业务数据、患者信息、系统架构、安全策略、网络拓扑等敏感信息；
- 供应商非经采购人书面同意，不得以任何方式向第三方披露、转让和许可本项目的技术资料和文件（依法律法规、规定、行政或者司法机关要求提供的除外）。除本项目工作需要之外，未得到采购人的书面许可，供应商不得以任何方式商业性地利用上述资料和技术。如供应商违反本条规定，除立即停止违约行为外，还应当赔偿采购人的全部损失；
- 供应商的保密义务不因本协议的终止、解除或履行完毕而失效，将持续有效，直至相关保密信息进入公共领域（非因供应商违约造成），或采购人书面通知解除该义务。

4.4 交付物要求

运维服务过程中，结合已开展的工作，分不同阶段提交相应的有形交付物。相应服务结束后 5 个工作日内提交，交付物包括但不限于：

- 《资产清单表》——资产识别梳理服务完成后提交；
- 《基线核查报告》——基线核查服务完成后每次提交；
- 《漏扫报告》——漏洞扫描服务完成后每次提交；
- 《新应用上线测试报告》——新应用上线测试完成后提交；
- 《渗透测试报告》——渗透测试服务完成后每次提交；
- 《漏洞跟踪函》——漏洞扫描及整改跟踪过程中持续提交；
- 《重保值守服务报告》——重保服务结束后提交；

- 《应急响应报告》——应急响应事件处置完成后提交；
- 《安全设备巡检报告》——驻场运维日常巡检按月提交；
- 《安全设备配置操作手册》——开工之日起一个月内提交；

4.5 人员要求

- 供应商须为本项目配备不少于 5 人的专业运维服务团队；
- 项目负责人须同时具备 PMP（项目管理专业人士）、CISP（注册信息安全专业人员）、通信类高级工程师资质；
- 运维服务团队成员（除项目负责人以外）须具有系统集成项目管理师、信息系统项目管理师、ITSS IT 服务工程师、网络工程师等资质（须提供人员证书复印件和劳动合同证明扫描件，一人多证只计一次）；
- 供应商近三年（合同签订时间：2023 年 9 月 1 日至今）须具有类似项目经验。

4.6 考核要求

4.6.1 服务质量评价

采购人每季按打分表进行服务质量评价和考核（总分 100 分，≥85 分为优秀，60≤分数<85 为合格，<60 为不合格）。年度服务质量评价得分 = 月/季度维度得分的算术平均值（保留一位小数），总分 100 分，≥85 分为优秀，60≤分数<85 为合格，<60 为不合格。评分结果作为进度款支付及惩罚依据，表样见附件一、附件二。

4.6.2 服务考核

若服务评价得分大于或等于 85 分，该期采购人将全额支付款项；若服务评价得分在 60 分（含）至 85 分（不含）之间，该期支付金额按照以下公式计算：支付金额 = 每期运维服务费总额 - 每期运维服务费总额 × (85 - 实际评分) × 0.5%；若评分低于 60 分，则视为出现严重服务质量违约情况，该期服务费不予支付。

4.6.3 服务严重不达标惩罚

重大故障、服务严重不达标情况
一级故障彻底修复时间＞24 小时
二级故障彻底修复时间＞72 小时
发生数据丢失情况，但后续完成恢复，未造成直接损失
发生网络安全事件，但及时采取弥补措施，未造成损失

发生以上任意情形之一的，当期服务质量评价和考核结果为不合格，视为出现服务质量违约，故障事件发生当期服务费按以下条款进行增加处罚：

（1）一级故障 MTTR 指标不达标，每次扣减合同总金额的 5%；

（2）二级故障 MTTR 指标不达标，每次扣减合同总金额的 3%；

（3）发生数据丢失但已恢复未造成直接损失的，每次扣减合同总金额的 3%；

（4）发生网络安全事件未造成直接损失的，每次扣减合同总金额的 2%；

4.6.4 严重违约情形

（1）发生以下情形之一的，采购人有权单方解除合同，供应商应退还全部已支付费用，并赔偿采购人因此造成的直接经济损失：

（2）因供应商原因导致采购人重要医疗数据丢失且无法恢复；

（3）因供应商原因致使采购人遭遇网络安全事件，且该事件被上级部门通报，并给医院造成损失（包括但不限于经济损失和声誉损失等）；

（4）供应商服务评价结果连续三个月不合格或全年累计不合格评价结果次数占比≥40%。

五、附件

附件一：

_____运维服务____月度评价表

评价维度	分值	评分标准	得分
需求调研与手册完备性	8	优秀（7-8 分）：完成需求调研，需求文档规范；系统操作/维护/常见故障手册完整，及时更新，版本管理清晰。 合格（5-6 分）：基本完成调研，手册内容覆盖主要模块，但存在多处更新滞后或小缺失。 不合格（0-4 分）：未开展必要调研；手册内容缺失严重或超过三个月未交付，影响运维交接。	
培训质量	10	优秀（9-10 分）：培训计划执行率 100%，资料完备。 合格（6-8 分）：计划执行率≥80%。 不合格（0-5 分）：培训延期未补、计划执行率＜80%，或因培训不足导致重要操作失误。	
会议及报告规范性	5	优秀（5 分）：按时召开例会；月报、季报、故障分析报告等零延迟提交，内容详实、数据准确、有改进分析。 合格（3-4 分）：未按时召开例会，报告迟交，内容基本完整无关键错误。 不合格（0-2 分）：无故不召开例会，或报告多次迟交、数据严重失实、质量低劣。	
巡检到位率	15	到位率 = （实际完成巡检数÷计划巡检数）×100% 到位率 100%且记录详实：15 分； 95%≤到位率＜100%：12-14 分； 90%≤到位率＜95%：9-11 分； 到位率＜90%：0-8 分。 发现巡检记录造假，本项计 0 分。	
应急预案	10	优秀（9-10 分）：预案覆盖所有核心系统，内容科学可执行； 合格（6-8 分）：预案基本完备，有演练文本。 不合格（0-5 分）：预案缺失、无演练文本。	
交付物提交质量	7	优秀（7 分）：所有约定交付物（报告、记录单等）按时提交，格式规范，无需退回修改。 合格（5-6 分）：基本按时，存在个别退回修改但不超过 3 次。 不合格（0-4 分）：频繁迟交，质量粗糙，驳回超过 3 次，影响服务或评价。	
故障响应及时性	25	考核三级故障和四级故障的故障响应与修复时限。 优秀（21-25 分）：周期类所有三级、四级故障均在合同约定的 SLA 时限内完成响应；偶有轻微超时，但未对业务运行及用户使用造成可感知影响；故障处理记录完整规范，无用户投诉或科室不满反馈。 合格（13-20 分）：周期类所有三级、四级故障存在少量超时；未引发用户书面投诉或科室正式催促；故障处理记录基本完整，存在个别疏漏但经提醒后能及时补正。 不合格（0-12 分）：周期类所有三级、四级故障存在多次严重超时；因响应修复严重延误导致业务受阻、引发用户正式投诉；故障处理记	

评价维度	分值	评分标准	得分
		录缺失、混乱或失真，影响服务质量评价和事件追溯。	
用户满意度	20	由主要使用科室代表按月打分（十分制），平均分×2 即为本项得分。 问卷关键项：响应速度、服务态度、技术能力、沟通协调。 平均分≥9：优秀； 6≤平均分＜9：合格； ＜6：不合格。	
总分			

评价结论：□优秀（评分≥85 分）□合格（60≤评分<85）□不合格（评分<60 分）

采购人代表签字：_____ 日期：_____ 供应商代表签字：_____ 日期：_____

附件二：

_____运维服务____月度满意度评价表

评价维度	分值	评分标准	得分
响应速度	10	10 分：报修后瞬间响应远优于 SLA，到场极快。 8-9 分：严格满足 SLA 时限，基本无等待感。 6-7 分：偶有略超时但未影响业务。 4-5 分：频繁轻微超时，需反复催促才响应。 1-3 分：经常联系不上或严重超时，对诊疗造成明显阻碍。	
服务态度	10	10 分：态度热忱、主动，能安抚用户急躁情绪，主动跟进结果。 8-9 分：礼貌、耐心，沟通顺畅，用户感受良好。 6-7 分：态度正常，完成本职沟通，无投诉但也无亮点。 4-5 分：偶有语气急躁、推诿或不够耐心。 1-3 分：态度恶劣、与用户争执，或被多次投诉态度问题。	
技术能力	10	10 分：无需转手，一次到场即精准确诊并解决复杂问题，能主动优化隐患。 8-9 分：能独立解决职责内的各类故障，偶需二线支持但效率较高。 6-7 分：常见问题能处理，疑难问题明显依赖后方，但最终能闭环。 4-5 分：基础技能不足，处理耗时过长，或相同故障反复出现。 1-3 分：技术严重欠缺，操作失误导致影响扩大或引发新故障。	
沟通协调	10	10 分：变更、升级、恢复等主动同步信息，跨厂商协调无需我方介入，过程透明。 8-9 分：关键节点主动告知，响应及时，多方配合顺畅。 6-7 分：被动式沟通，一问一答，但信息准确。 4-5 分：信息传递滞后或错漏，需我方反复确认协调。 1-3 分：隐瞒延误、推卸责任、协调完全失效导致故障扩大。	
问题解决效果	10	10 分：彻底根治，近期未复发，且提供有效的自查建议或改进方案。 8-9 分：故障完全恢复，功能正常，用户认可解决结果。 6-7 分：主要功能恢复，但遗留小问题，或临时方案不够便捷。 4-5 分：解决不彻底，短期内复发，或临时方案严重降低效率。	

评价维度	分值	评分标准	得分
		1-3 分：未解决核心问题，或修复过程中造成数据丢失等衍生事故。	
小计			
总分	服务满意度得分 = 五个维度得分的算术平均值（保留一位小数）。		

评价结论：□优秀（评分≥9 分）□合格（6≤评分<9）□不合格（评分<6 分）

采购人用户科室：

采购人用户代表签字：_____ 日期：_____ 供应商代表签字：_____ 日期：_____

武汉市肺科医院

（武汉市结核病防治所）

2026 年 6 月