

# 广东医科大学顺德妇女儿童医院

(佛山市顺德区妇幼保健院)

## 项目需求书

项目名称: 2025—2027 年度网络安全服务项目

2025 年 7 月

一、采购项目情况概述

随着我院“互联网+医疗”的业务不断深化，信息系统的集中管理以及业务扩展带来了更大的安全风险，信息系统的安全性要求大大提高，对信息安全工作提出了新的挑战。为进一步落实国家及监管部门对于信息系统等级保护建设的要求，不断完善医院信息安全保障体系，我院通过公开采购网络安全服务加强院内系统及设备安全管理，不断完善安全防护能力，确保医院各大信息系统安全稳定地运行。

二、项目采购内容

1. 项目清单

序号	项目名称	数量	单价 (人民币元)	预算总金额 (人民币元)	服务期
1	2025-2027 年度网络安全服务项目	1	390000	390000	两年：2025 年 10 月 8 日至 2027 年 10 月 7 日
合计：（单位人民币元）				390000	
备注：					

三、项目实施地点：

广东医科大学顺德妇女儿童医院（佛山市顺德区妇幼保健院）指定任何服务地点。

四、项目预算金额：

合计不超过 390000 元人民币。预算中包括但不限于服务费用、人力费用、税费以及完成本项目内容所需的一切费用等。

五、项目要求

1. 资质要求

- (1) 具备《中华人民共和国政府采购法》第二十二条规定的条件。
- (2) 必须是在中华人民共和国境内注册的具有独立承担民事责任能力的法人或其它组织。

(3) 营业执照经营范围：本项目相关的内容。具有项目服务的能力，保证能及时对服务项目提供实施服务与建议。

(4) 在近三年的商业活动中无违法、违规、违纪、违约行为；

(5) 本项目不接受联合体参与，不接受转包、分包；

(6) 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一项目报价，一经发现按废标处理并标记为不诚信供应商。

## 2. 服务要求：

➤ 本项目将计划在我院开展相关安全服务，具体服务内容如下：

序号	项目名称	具体内容
1	网络安全运维服务	<b>定期安全检查：</b> 每季度一次，分析现网的安全风险，发现潜在的系统漏洞，排查网络中潜伏的未知风险和威胁。
2		<b>安全设备配置备份：</b> 不定期备份，一个季度至少一次，建立安全设备台账。通过配置备份，保障设备运行健康，以防出现变更导致的错误，提高应急处置能力。
3		<b>安全设备配置适应性调整：</b> 一年内不限次数，在安全相关设备配置需要调整时，如：安全策略调整、新链路配置、产品参数调整等；乙方必须派遣工程师进行配置风险评估、提出调整方案并实施。
4		<b>安全事件紧急响应：</b> 一年内不限次数，在出现安全事故、数据泄密、网络入侵等安全事件的时候，紧急响应，快速定位和查找问题，制定出解决方案，第一时间把安全问题消灭在萌芽状态。
5		<b>安全建设配合响应：</b> 一年内不限次数，在医院相关或上级部门提出安全建设、安全整改、安全加固等任务时，派遣专业安全专家指导配合进行安全相关工作。
6		<b>漏洞扫描：</b> 每季度一次，使用系统漏洞扫描工具对 数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，

		扫描完成后由技术人员对漏洞进行确认，提出整改建议。
7		<b>系统加固服务：</b> 一年约 10 个服务器 IP，根据专业安全检测结果，制定相应的系统加固方案，针对不同目标系统，通过安装补丁、修改安全配置、增加安全机制等方法，合理地进行安全性加固。
8		<b>安全培训：</b> 一年内两次，安全攻防技术培训，全单位信息安全意识培训，单位网络安全意识宣传等。
9		<b>主机基线核查：</b> 一年核心服务器 IP 配置，保障系统最基本的安全要求。
10		<b>安全管理制度梳理：</b> 根据客户的各类管理内容建立安全管理制度，形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。
11		<b>资产梳理：</b> 终端科室检查准入控制信息的登记情况，对所有合法进入网络的计算机在入网前将进行必要的安全检查，确保每台计算机都符合既定的安全规范
12		<b>渗透测试：</b> 一年不超五次，每次不超过 5 个系统。渗透测试通过模拟黑客思维及行动模式，使用主流的攻击技术对目标网络、系统、数据库进行模拟攻击测试, 提前发现系统潜在的各种高危漏洞。
13		<b>应急演练：</b> 每年一次，根据突发网络安全事件的性质，深度切合医院所面临的实际网络安全问题。为医院提供分门别类的演练方案；突发网络安全事件演练解决方案应急演练场景可分为：有害程序事件演练，网络攻击事件演练，信息破坏事件演练，设备实施故障演练和灾害性事件演练。
14		<b>重保值守：</b> 安全监控：WAF、防火墙、态势感知、杀毒软件；攻击 IP 封禁、威胁主机断网隔离、日志溯源

➤ 详细服务要求如下：

## 1. 定期安全检查

服务频次：每季度一次

服务内容：对医院的现网整体安全提供全面的巡检服务，巡检的内容包括但不限于：

（1）安全设备品牌、设备型号、设备放置、设备性能参数、设备内存大小、设备槽位、设备序列号、设备购买年限、设备保修状态、设备备件状况、设备标签完善程度；

（2）安全设备软件版本信息、当前 IOS 版本信息、最新 IOS 版本信息、设备持续运行时间、设备 IOS 备份情况、设备 CPU 利用率、设备内存利用率、设备模块运行状态、设备风扇及电源状况、设备端口数量、设备端口类别、设备端口类型、设备运行机箱温度；

（3）安全设备连通性、冗余协议运行状态、VLAN 信息、以太通道信息、路由协议、邻居关系、交换协议、生成树 STP 协议、NAT 连接数状态、FLASH 信息、设备配置信息分析、多余配置信息分析、配置精简建议、IOS 安全建议、防火墙信息、防火墙策略、防火墙 DMZ 区检查、防火墙 Xlate 状态、应用业务、IP 地址使用状况；

（4）对设备性能、告警信息、被攻击和入侵情况（如入侵事件、入侵源、前十位攻击对象等）、安全威胁进行动态评估；

（5）对安全系统瓶颈和资源竞争情况进行分析，找出潜在问题。

（6）对服务器、终端做周期检查，主要内容是检查是否存在高危漏洞，杀毒软件病毒库是否最新。如果发现问题需要及时提供人工现场处理修复或者升级服务。

## 2. 安全配置备份

服务频次：不定期备份，一个季度至少一次

服务要求：为了保证安全设备的健康运行情况，使得设备在失效或配置丢失时，能依靠备份尽快地恢复系统与配置，保护关键策略，保证配置不丢失，需根据实际情况对院方网内重要网络安全设备配置进行不定期的配置备份。整体备份要求如下：

（1）在重要节假日和特殊时期（含粤盾、粤网安、国护、中秋、国庆、两会、春节、五一等）对院内关键网络设备配置进行全量配置备份；

(2) 在院方业主重大改动前期，如新业务上线、网络架构调整、新设备上  
线等情况，对改动范围内重要网络设备配置进行全量备份。

(3) 每季度对服务范围内网络安全设备进行一次全量备份。

(4) 备份工作实施时需按以下标准执行：

备份前期应熟悉院内所有范围内设备的配置文件所在位置，文件导入导出方  
式；

对关键的网络安全设备的策略配置进行备份，防止策略的丢失与错误变更配  
置；涉及备份和恢复的事由专人负责备份工作，并认真填写备份日志。

备份数据应该严格管理，妥善保存。

一旦发生配置丢失或数据破坏等情况，要由负责人员进行备份数据的恢复，  
以免造成不必要的麻烦或更大的损失。

备份数据恢复后，应验证恢复配置后的设备联通性情况、配置或策略有效性  
情况。

### **3. 安全设备配置适应性调整**

服务频次：一年内不限次数

服务内容：在安全相关设备配置需要调整时，如：安全策略调整、新链路配  
置、产品参数调整等；派遣工程师进行配置风险评估、提出调整方案并实施。安  
全相关设备配置包括但不限于以下情况：

(1) 网络出口新增加，评估新网络出口的风险和安全防护措施；

(2) 防火墙、UTM 等边界类设备的配置变更，详细记录变更内容，包括 IP  
策略、端口策略、放通/禁止策略等；

(3) 网闸等隔离类设备的配置变更，详细记录变更内容，包括 IP 策略、端  
口策略、应用通道、转发模式等；

(4) 入侵防御、网络行为分析等旁路安全设备配置变更，包括协议监控、端  
口监控、联动策略等；

(5) 杀毒软件、准入控制等终端管理类软件的配置变更，包括扫描策略、准  
入方式、控制范围等；

(6) 协助医院进行安全设备或软件的配置变更时，要充分考虑到配置变更  
过程中和变更后带来的安全风险，采取一定的预防措施，将风险降低到最小，最  
小化对医院正常业务开展的带来的影响。

#### 4. 安全事件应急响应

服务频次：一年内不限次数

服务内容：在接到医院的安全事件紧急救援服务请求后，安全工程师立即响应，通过预先确认的远程连接方式登录到相应的系统上，对安全事件进行排查，在发现远程登录无法解决的安全事件后，立即采用最快方式赶赴甲方现场，2小时内可到达医院的现场。如信息系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改，或已经发现的有可能造成上述现象的安全隐患，如非授权访问、信息泄密、系统性能严重下降、黑客攻击、蠕虫或大面积爆发病毒等，安全团队需在2小时之内赶赴现场协助解决问题，必要时应提供入侵调查分析、安全审计预警与黑客追踪服务。

应急响应服务包括远程应急响应服务和本地应急响应服务，其主要内容如下：

(1) 消除潜在安全隐患：通过日志信息和其他必要信息，检查后门程序和网络系统漏洞，消除其再次受到攻击的可能性，即消除今后的安全隐患，对系统的安全进行重新评估。

(2) 检查安全日志：通过检查系统、防火墙、路由器等系统安全日志，为确认攻击来源和攻击手段以及调查取证提供必要的条件。

(3) 入侵者追踪：通过所能得到的信息追踪入侵者，并记录其尽可能多的信息，为调查取证提供条件。

(4) 主机恢复：在甲方信息系统网络或主机受到攻击并且出现网页遭替换或系统丢失等恶性事件后，确认已经消除安全隐患，在系统网络管理人员的协助下，对应用系统或操作系统进行恢复，保证系统资源在第一时间内的可使用性。

(5) 网络恢复：医院信息系统的核心交换机、路由设备等网络设备出现问题，在确定是受到攻击所造成的情况下，确认已消除安全隐患，在经过医院授权后，对网络设备进行恢复，保证医院信息系统网络资源在第一时间内的可使用性。

#### 5. 安全建设配合响应

服务频次：一年内不限次数

服务内容：在医院相关或上级部门提出安全建设、安全整改、安全加固等任务时，派遣专业安全技术人员指导配合进行安全相关工作，需配合建设响应的情况包括但不限于：医院网站漏洞排查、公安部门递送的安全检查或安全漏洞通知、

上级部门递送的安全检查或安全漏洞通知、国家重大事件的安全保障检查、突发性事件的检查通知或现场检查、医院业务改动等场景。

整体服务要求如下：

对于上级单位下发的政策通知或整改要求向院方进行专业性解读，解释相关政策或整改要求条款、合规性标准、建设指引、依据等内容。

根据场景要求对院方信息化现状进行调研，按照政策要求或整改要求或实际业务改动需求角度分析用户现状合规差距。

根据实际分析出来的差距，从合规性、经济学、安全性等方面进行考虑，设计并输出相关建设解决方案。并在方案落实过程中给予实施指导。

## 6. 系统漏洞扫描与分析

服务频次：每季度一次

服务内容：定期利用专业的漏扫工具对系统进行漏洞扫描，发现网络设备、主机操作系统、web 应用等安全漏洞情况。扫描要求如下：

针对用户 IT 设备进行安全漏洞扫描工作，并输出扫描报告与加固建议；

针对相关 Web 服务业务系统，进行网页安全漏洞扫描，并输出扫描报告与加固建议；

针对新上线系统进行漏扫和检查，并输出新上线系统检查加固报告。

可扫描识别出的漏洞范围包括但不限于：

### ➤ 网络层漏洞识别

1. 版本漏洞，涉及包括所有在线网络设备及安全设备。
2. 开放服务，包括但不限于路由器开放的 Web 管理界面、其他管理方式等。
3. 空弱口令，例如空/弱 telnet 口令、snmp 口令等；
4. 网络资源的访问控制：检测到无线访问点等；
5. 域名系统：拒绝服务攻击漏洞， DNS 拒绝服务攻击等；
6. 路由器：配置接口安全认证可被绕过，交换机/路由器缺省口令漏洞，网络设备没有设置口令等。

### ➤ 操作系统层漏洞识别

1. 操作系统（包括 Windows、AIX 和 Linux、VMware 等）的系统补丁、漏洞、病毒等各类异常缺陷等。
2. 空/弱口令系统账户检测等。

3. 例如：身份认证：通过 telnet 进行口令猜测等。
4. 访问控制：注册表普通用户可写，远程主机允许匿名 FTP 登录，ftp 服务器存在匿名可写目录等
5. 系统漏洞：远程缓冲区溢出漏洞，服务远程缓冲区溢出漏洞等
6. 安全配置问题：部分 SMB 用户存在薄弱口令，试图使用 rsh 登录进入远程系统等

#### ➤ 应用层漏洞识别

1. 应用程序（包括但不限于数据库 Oracle、DB2、MS SQL，Web 服务，如 Apache、Tomcat、IIS 等，其他 SSH、FTP 等）缺失补丁或版本漏洞检测等
2. 空弱口令应用账户检测。
3. 数据库软件：没有设置口令等
4. Web 服务器：远程缓冲区溢出漏洞，远程缓冲区溢出，服务程序分块编码传输漏洞等
5. 电子邮件系统：处理远程溢出漏洞，SMTP 服务认证错误漏洞等
6. 防火墙及应用网管系统：防火墙拒绝服务漏洞等

服务完成后，服务人员需对每次扫描服务范围内的安全状况进行概述，对主机系统，网络设备，开放服务和漏洞情况进行统计。包括弱口令，主机安全扫描报告。根据漏洞扫描的结果针对每个漏洞进行详细描述，描述内容包括了漏洞厂商、威胁目标、危险级别、危害描述以及详细解决方案等。

### 7. 系统加固服务

服务频次：一年约 10 个服务器 IP

服务内容：根据专业安全检测结果，制定相应的系统加固方案，针对不同目标系统，通过安装补丁、修改安全配置、增加安全机制等方法，合理地进行安全性加固。

### 8. 安全培训服务

服务频次：一年两次

服务内容：配合医院开展安全建设和运维的工作，定期对医院信息科相关人员提供信息安全技术培训，培训结束后定期进行技术考核，提升医院信息安全意识和技术知识水平。

培训对象：医院系统管理员、网络管理员、数据库管理员、安全审计员等专业技术人员。

培训内容包括但不限于以下内容：

- (1) 国家等级保护流程与相关内容
- (2) 医疗行业等级保护建设案例分享
- (3) 医疗行业内外网互联安全建设风险
- (4) 医疗行业网站建设和漏洞防范介绍
- (5) 医疗行业数据库安全和漏洞防范介绍等。

### **9. 主机基线检查**

服务频次：一年约 10 个核心业务服务器 IP

服务内容：根据相关法律法规、行业标准制定用户安全基线基准。

安全配置检查内容：系统管理和维护的正常配置，合理配置，及优化配置。配置检查主要针对操作系统、网络设备、安全设备、数据库等，检查项包括系统目录权限，账号管理策略，文件系统配置，进程通信管理等方面，例如日志及审计、备份与恢复，加密与通信，特殊授权及访问控制等安全特性。

### **10. 安全管理制度梳理**

服务内容：依据网络安全法及网络安全等级保护相关管理要求，结合医院实际业务情况、部门情况及已有制度情况，为院方进行安全制度建设，查漏补缺，包括协助院方制定单位安全方针，建立信息安全策略框架制度；明确院内信息安全管理制制度，落实各项安全管理标准文档，以及各项管理相关表单。

### **11. 资产梳理**

服务内容：安全服务团队结合资产梳理工具成果进行梳理，识别出网站资产、服务器资产、终端资产，并形成资产清单。

第一次资产梳理：安全服务团队使用安全运营平台进行资产发现，并导入已知资产信息，形成初步资产表。

日常资产梳理：安全服务团队对运营平台自动发现的未知资产进行确认，指定资产责任人并为其分配用户。

### **12. 渗透测试**

服务频次：一年不超五次，每次不超过 5 个业务系统。

服务内容：渗透测试主要是模拟黑客的攻击方法，检测网站、网络协议、网

络服务、网络设备、应用系统等各种信息资产所存在的安全隐患和漏洞。

渗透测试主要分为扫描和人工两部分，依靠带有安全漏洞知识库的网络安全扫描工具以及安全专家对漏洞的深入了解，其特点是能对被评估目标进行覆盖面广泛而且更深度的安全漏洞查找，并且评估环境与被评估对象在线运行的环境完全一致，较真实地反映网站及服务器系统、网络设备、应用系统所存在的安全问题和面临的安全威胁。

### **13. 应急演练**

服务频次：一年 1 次。

服务内容：根据应急演练规划和应急预案要求，在对事先设定事件场景风险和应急预案认真分析的基础上，结合年度内发生网络安全事件的情况，发现存在的问题和薄弱环节，确定需调整的演练人员、需锻炼的技能、需检验的设备、需完善的应急处置流程、指挥调度程序以及需进一步明确职责等，分析完成举办应急演练的要求。

### **14. 重保值守**

服务内容：在攻防演习实战期间，安全监控小组将对外部安全威胁情报、安全漏洞情报及外部披露情报等安全情报进行实时监控，通过对医院内部安全设备进行监控预警，日志分析，实时从设备告警日志中捕获异常攻击行为或操作行为，通过策略调优、误拦分析，及时封堵异常攻击行为，对安全风险进行闭环等。

## **六、付款方式：**

签订合同后，从服务期限起始之日开始按半年度结算（每次给付合同款 25% 金额），乙方在每半年开始的 10 个自然日内向甲方提交上半年度服务明细报告等材料，经甲方验收确认后，乙方出具等额发票，甲方在 60 个自然日内支付合同款 25% 金额。因乙方原因逾期交发票的，甲方付款天数相应顺延。

因甲方使用的为财政资金，甲方在前款规定的付款时间为向上级主管部门提出办理财政支付申请手续的时间（不含政府财政支付部门审核的时间），在规定时间内提出支付申请手续后即视为甲方已经按期支付。

## **七、验收标准：**

验收标准：每项服务完成后，应在用户规定的时间内（3-5 个工作日）出具

相应服务报告，服务报告将作为项目最终验收主要依据。

同时，甲方根据乙方服务情况对乙方进行评分，并根据评分结果对本项目最终采购价进行调整：

评分结果大于 90 分时，全额支付合同款，最终采购价为合同全款；

评分结果  $80 \leq \text{评分} < 90$  时，本项目最终采购价为合同款 90%；

评分结果  $70 \leq \text{评分} < 80$  时，本项目最终采购价为合同款 80%；

评分结果  $60 \leq \text{评分} < 70$  时，本项目最终采购价为合同款 70%；

评分结果小于 60 分时，本项目最终采购价为合同款 60%；

### 八、其他

出现下列情形之一的，本项目合同终止：

- (1) 本项目顺利完成。
  - (2) 在本合同服务期内，因不可抗力情形导致本合同无法继续履行的，而由此导致毁损并造成的损失双方互不承担责任。
  - (3) 经双方协商一致解除本项目合同的。
  - (4) 因甲方需要搬迁医院时，甲方有权终止或变更合同。
- 其他未尽事项另行商谈确定。

### 九、评选参考标准

评分内容	技术部分	商务部分	价格部分
权重	40%	30%	30%

序号	评审项目	评分细则及标准	分值
技术部分（总计 40 分）			
1	投标人的项目经理资质要求	1、具有信息系统项目管理师认证证书； 2、具有项目管理专业人员资格认证（PMP 认证）； 3、具有容灾实施专家认证； 4、具有信息安全保障人员认证证书； 项目经理具备以上有效期内的资质证书，每个证书得 2 分，共 8 分。 注：投标人须提供上述人员有效期内的证书，以及在本公司任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月内《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无	8

		效。	
2	投标人技术服务团队能力	1、服务团队中有 OCP 数据库工程师认证； 2、服务团队中有人社局颁发的网络工程师中级认证； 3、服务团队有 RHCE 认证证书； 4、服务团队有 VMware 认证（VCAP）； 5、服务团队有注册信息安全专业人员。 投标人技术服务团队具备以上有效期内的资质证书，每个证书得 2 分，共 10 分。 注：一人有多证，只算一种认证得分；投标人须提供上述人员有效期内的证书，以及在本公司任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月内的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无效。	10
3	项目管理方案及质量保障措施	根据投标人针对本项目的服务方案、保障措施是否完整，详细、可行、有效，具有可操作性及技术性能指标的成熟性、稳定性、先进性以及关键重要部位控制措施是否明确、详尽、合理作为评审依据。 优：投标人的服务方案具有完整的保障措施，并且详细、可行、有效，具有可操作性的得 10-12 分； 良：投标人的服务方案具有一定的保障措施，并且具有一定的可行性、有效性、操作性的得 7-9 分； 中：投标人的服务方案具有不完善的保障措施，具有一些可行性、有效性、操作性的得 5-7 分； 差：投标人的服务方案具有不完善的保障措施，不具有可行性、有效性、操作性的得 0-4 分； 无服务方案：不得分	12
4	培训方案	投标人针对医疗行业提供网络安全技术培训方案完善、科学和可行性等方面进行对比评价，综合评价优得 6-8 分，综合评价良得 3-5 分，综合评价差得 0-2 分，不提供方案不得分。	8
商务部分（总计 30 分）			
1	投标人管理体系	1、具有 ISO9001 质量管理体系认证； 2、具有 ISO27001 信息安全管理体系统认证； 3、具有 ISO20000 IT 服务管理体系认证； 投标人具有上述 3 项认证，一个认证得 4 分，满分得 12 分； 注：1. 提供与投标人名称一致的有效的相关质量认证证明文件复印件，并加盖投标人公章；2. 上述证书的发证机构须为境内机构；否则不得分。	12
2	投标人服务能力	1、具有 ITSS 数据中心服务能力成熟度标准符合性证书二级满足得 4 分，不满足不得分； 2、具有信息系统建设和服务能力等级证书满足得 2 分，不满足不得分； 3、具有中国网络安全审查技术与认证中心 CCRC 颁发的信息安全服务资质-认证方向为信息系统安全集成、安全运维服务、信息安全风险评估证书。每个得 2 分，满分 6 分；	12
3	类似项目经验	投标人自 2022 年以来三甲医院安全服务实施经验，每个 2 分，投标人自 2022 年以来有二甲医院安全服务实施经验，每个 1 分，本项最高得 6 分。 （提供合同复印件和发票作为评审依据，否则有可能影响评审结果）	6

价格部分（总计 30 分）			
1	评选标准	经评选小组审核，满足采购文件要求，以折扣率最低者定为评选基准价，其对应报价得分为满分。	30
2	计算公式	报价得分 = (评选基准价 ÷ 评选最后报价) × 价格分值	