佛山市第一人民医院

信息系统安全服务项目

用户需求书

2025年4月

# 项目背景

为加强网络与信息安全保障，提升信息系统安全防护水平，一系列政策法规相继出台。2017年6月1日，《中华人民共和国网络安全法》正式施行，明确提出国家实行网络安全等级保护制度，为信息安全等级保护工作提供了坚实的法律基础。2019年，国家市场监督管理总局、国家标准化管理委员会发布了GB/T 22239-2019《信息安全技术-网络安全等级保护基本要求》等一系列等级保护相关国家标准，进一步细化和规范了等级保护工作的各项标准和要求。

在当今信息化快速发展的背景下，佛山市第一人民医院网络安全面临着越来越复杂的安全挑战。医院的信息系统存储着大量患者的个人信息、医疗记录等敏感数据，一旦这些数据泄露或系统遭到破坏，可能会对患者的隐私和安全造成严重影响，也会影响医院的正常运营，进而危害公共利益。因此，医院必须从多个层面引入创新的安全防护措施，以提高其整体信息安全水平。

为应对这一挑战，佛山市第一人民医院需要依托国内顶尖的安全服务团队，提供不仅仅局限于传统防护措施的全方位网络安全服务，在高风险时期，佛山市第一人民医院将结合安全加固、漏洞扫描、系统安全性检测等服务，强化对外部攻击的防护，全面提升医院的信息网络安全和数据保护能力，以保障核心业务的稳定运行与患者数据的安全。

# 服务标准

* 《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2008）
* 《信息安全技术信息系统等级保护安全设计技术要求》(GB/T 25070-2010)
* 《信息安全技术信息系统安全等级保护定级指南》(GB/T 22240-2008)
* 《信息安全技术信息系统安全等级保护实施指南》
* 《信息安全技术信息系统安全等级保护测评要求》
* 《信息安全技术信息系统安全等级保护测评过程指南》
* 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）
* 《信息安全技术信息系统通用安全技术要求》（GB/T 20271-2006）
* 《信息安全技术网络基础安全技术要求》（GB/T 20270-2006）
* 《信息安全技术操作系统安全技术要求》（GB/T 20272-2006）
* 《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2006）
* 《信息安全技术服务器技术要求》（GB/T 21028-2007）
* 《信息安全技术终端计算机系统安全等级技术要求》（GA/T 671-2006）
* 《信息安全技术信息系统安全管理要求》（GB/T 20269-2006）
* 《信息安全技术信息系统安全工程管理要求》（GB/T 20282-2006）
* GB/T 22080-2008/ISO/IEC 27001:2005《信息技术安全技术信息安全管理体系要求》
* IATF《信息保障技术框架》

# 项目范围

医院内部网络及各类信息系统有关之信息应用安全、网络安全、终端安全、操作系统、数据库、常见中间件及服务应用等的安全。

* 1. 要安全设备：

# 服务内容要求

* 1. **驻点安全值守服务**

**提供至少1名或以上专职的信息安全工程师在医院驻点服务，提供一周6X8小时的现场驻点。现场驻点工程师要求：必须拥有1年以上在相关行业从事网络安全现场驻点运维经验，具备CISP等级资质认证。**

**驻点服务内容包括：**

1.1依据医院安全预警平台，协助对医院内网的中毒客户端进行病毒查杀及木马清理，并按医院要求安装防病毒软件客户端。确保医院当月安全预警平台的综合得分达到80分以上。

1.2 依据院方安全感知平台的脆弱性业务风险分析报告，协助服务器管理员消除业务存在风险问题；修复高风险漏洞，确保不存在中高风险业务。利用天擎，对医院内终端进行补丁分发，减少系统漏洞，降低病毒感染黑客风险。对于特别危急的系统漏洞，协助用户对服务器进行补丁手工修复及人工检查确认，确保漏洞已经成功修复，保护关键应用的系统安全。漏洞主要是微软操作系统关键、严重类漏洞。危急类补丁主要是影响范围广，对系统可用性影响极大，例如MS17-010、MS08-067远程执行任意代码漏洞。

1.3查找未安装安全软件的网内设备，确保防病毒软件客户端覆盖达90%以上。

1.4 对已部署的安全产品提供运行维护和技术支持服务，包括医院各类信息安全、网络安全、终端安全系统的日常巡检和运维保障。定期巡查安全产品运行状态；根据实际需要进行策略调整；日常巡检维护、安全策略优化、故障处理、应急处理、安防措施有效性验证等。

1.5 对院内各边界防火墙、互联防火墙安全设备日志分析、安全攻击研判、安全事件应急处置、边界网络访问控制策略开通、梳理及优化配置，策略新增及过期策略回收等，每月形成防火墙策略分析及优化报告。

1.6 对医院上网行为管理平台进行监控，对上网策略优化，违规上网行为审计及处理等。通过权限访问策略，限制用户访问到互联网恶意网页。

1.7 对院内服务器主机安全监控，安全防护客户端安装，日志分析，问题处理，服务器高危漏洞排查及推进修复，配置优化等。

1.8上级单位、主管单位、第三方单位安全报告、排查等安全工作的配合和处理。

1.9攻防期间需要驻点人员在医院7X24小时的现场驻点值守。

形成专业报告，达到安全风险有预防、安全事件有记录、出现问题可追溯的信息安全监控状态，保障医院各系统正常、安全、稳定、高效运行。

* 1. **等级保护安全整改服务**

（1）协助进行有关等级保护的安全整改，收到第三方测评机构出具的测评报告后，需要依据报告协助院方完成有关物理安全、主机安全的加固，在30工作日内完成整改。配合提供安全加固服务，包括各种网络设备、安全设备、主机操作系统、数据库、常见中间件及服务应用等的安全加固及调优测试，协助院方通过第三方测评机构的验收测评。

（2）提供存在互联网资产及端口暴露的医院信息系统的安全监测评估服务，按年提供不少于四次的资产及端口暴露复测服务。新系统上线监测内容包括但不限于物理环境、网络设备、操作系统、应用安全、代码程序和数据等，上线前安全评估服务的实施时间应在应用系统完成编码与测试阶段，部署至生产环境后，正式发布前，需进行端口及应用参数传输方面的安全评估、渗透测试并出具盖章评估报告。对上述已做安全检测的系统，如被第三方具备安全资质检测公司或机构检测到严重的安全漏洞（大量医患敏感数据泄露，服务器远程受控等），并经三方确认的，医院支付给第三方安全检测公司或机构的检测费用由安全服务公司承担。

（3）为医院提供专业化信息安全服务，负责完善医院现有的信息安全体系，并依据国家信息系统等级保护评测要求，包括制定医院的信息安全目标、完善安全管理制度、设立安全基线、完善日常信息安全作业指导书、编制应急处置流程等。

* 1. **7×24小时应急保障服务**

**建立医院网络安全事件应急预案，提供二线技术团队支持，成立应急技术支持小组，应急技术支持小组应由3人以上的技术专家级工程技术人员组成，365×24小时提供紧急响应服务。**

当医院网络及信息系统出现服务人员无法解决的信息安全事件或出现大规模的有害程序事件(如病毒/蠕虫/木马/僵尸网络)、网络攻击事件(拒绝服务攻击/后门攻击/漏洞攻击/网络扫描/网络钓鱼)、信息破坏事件(篡改/假冒/泄露/窃取/丢失)等，应立即启动紧急响应服务，协助处理信息安全事件。

应急响应小组人员应15分钟内响应，2小时内到达用户现场。

每次服务完成后2周内，服务商必须提交完整的事件分析报告，内容至少包括事件原因分析、已造成的影响。详细说明事件原因、经过和处理方式等，而且对用户以后整改的方向提供适当的解决方案；

* 1. **安全巡检服务**

每月进行对防火墙、防病毒服务器、入侵检测系统、日志审计等安全设备状态进行检查，对记录的事件和日志分析，检查策略是否有效，配置是否安全，是否有可疑事件发生，必要时进行安全策略的调整。

* 1. **安全基线核查服务**

每月进行一次安全基线核查，若当期安全形势危急，或上级有安全要求可进行多次。

通过工具扫描及安全服务工程师对客户信息系统进行安全基线检查，及时发现信息系统存在的各种安全隐患，如：网络设备、安全设备、服务器主机、操作系统、数据库和用户账号、口令等配置问题，以及系统运行状态，提出系统加固建议以及相关的应急措施。

基线核查内容包括但不限于以下内容：

（1）操作系统安全检查

业务系统涉及到的操作系统，如Windows、Linux等进行安全配置缺陷的检查与评估。核查内容包括（但不限于）：身份鉴别方式、帐号安全设置、多余帐号和空口令检查、默认共享检查、文件系统、系统访问控制、日志及监控审计等安全情况。

（2）网络、安全设备配置检查

对用户信息系统涉及到的网络安全设备，如防火墙、入侵检测系统、路由器、交换机等进行安全配置缺陷的检查与评估。核查内容包括（但不限于）：帐号安全设置、管理权限和角色设置、多余帐号和缺省口令检查、备份和升级情况、访问控制、日志审核、远程访问等安全情况。

每次检查完成后2周之内，服务商必须提交完整的基线检查报告，详细说明用户有可能存在的安全风险，含整改的手段及方案。

* 1. **安全漏洞扫描服务**

**利用专业工具进行安全漏洞扫描，**每月至少一次，若当期安全形势危急，可进行多次；安全漏洞扫描围绕该系统的操作系统和应用系统是否存在后门或漏洞为目的；

安全漏洞扫描实现的方式应包括但不限于以下方式：工具测试；

每次安全漏洞扫描完成后2周之内，服务商必须提交完整的漏洞扫描分析报告，详细说明用户有可能存在的安全风险，含整改的手段及方案。

* 1. **系统安全性评估服务**

按要求对院方指定的系统进行系统安全性评估服务，并出具详细的评估报告及整体建议，整改后需进行二次评估来验证，直至程序漏洞修复完成为止。服务商应从用户的外部及内部，形式手段不限地以多种方式尝试测试该系统的操作系统和应用，找出系统存在的后门或漏洞、页面漏洞、后台管理账号、用户弱密码等一切安全风险；

每次开展系统性安全性评估前，服务商必须提交系统安全性评估方案，详细说明系统安全性评估工作的范围和采取的方式，待用户同意后方能实施；

每次评估完成后1周之内，服务商必须提交完整的评估分析报告，详细说明用户有可能存在的安全风险，含整改的手段及方案，并尽全力恢复好测试的系统原状态；

* 1. **全网病毒态势分析服务**

为达到快速、没死角的病毒防控水平，需提供全网病毒态势分析服务。通过定制化的防病毒运维服务，实现以下维度的病毒日志分析：

（1）年度全网病毒感染趋势图；

（2）感染病毒主机数趋势图；

（3）Top10病毒、感染数；

（4）Top10感染病毒计算机（当期、历史）；

（5）病毒传播及感染方向分析，包括本机内横向扩散病毒数、通过移动存储感染病毒数、通过互联网感染病毒数、局域网横向传播病毒数等；

（6）高危病毒全网扩散性趋势分析；

（7）全网高危计算机感染分析，近十天内，感染病毒天数前十的计算机；

* 1. **、APP安全监测服务**

APP安全检测服务是帮助客户对包括android，ios平台各个版本的漏洞检测，包括对Android组件、权限管理、dex保护、数据安全(传输、存储、输出)，以及对危险调试信息等常见的漏洞风险进行检测，如Activity安全、Broadcast Receiver安全、Service安全、WebView安全、数据安全检测调试信息、输入检查 、数据传输完整性 、远程数据通讯协议等。从而发现APP应用代码编写过程中可能出现的安全漏洞、编码隐患等，减少因安全风险漏洞可能造成的应用内信息泄露、远程代码执行、本地拒绝服务等多种安全问题，保障APP应用的正常运行。

APP安全检测范围注入如下：

|  |  |  |
| --- | --- | --- |
| **Android客户端** | **IOS客户端** | **服务端** |
| 客户端程序安全 | 客户端程序安全 | Web安全 |
| 敏感信息安全 | 敏感信息安全 | 业务逻辑安全 |
| 网络通信安全 | 网络通信安全 | 中间件安全 |
| 进程安全 | 进程安全 | 服务器安全 |
| 安全策略设置 | 安全策略设置 | - |
| 组件安全 | - | - |

* 1. **网站加固服务**

网站安全加固服务针对重要网站的软硬件技术架构、网站运行状态和最新的安全威胁等因素提高网站安全防护能力，该服务包括但不限于底层操作系统安全、通信安全、网站开发平台、网站日志、网站漏洞补丁和最新安全风险防护等协助加固工作。服务期内提供网站的安全加固协助服务，安全加固后，不影响正常业务。

* 1. **渗透性测试服务**

每月对院方指定的5个系统进行渗透测试服务，并出具详细测试报告及整改建议，整改后需进行二次测试报告来验证，直至程序漏洞修复完成为止。服务商应从用户的外部及内部，形式手段不限地以多种方式尝试渗透该系统的操作系统和应用，找出系统存在的后门或漏洞、页面漏洞、后台管理账号、用户弱密码等一切安全风险；

渗透性测试实现的方式应包括但不限于以下方式：人工渗透、社会工程学、爬虫、工具渗透等；

每次渗透性测试前，服务商必须提交渗透性测试方案，详细说明渗透性测试的范围和采取的方式，待用户同意后方能实施；

每次渗透性测试完成后1周之内，服务商必须提交完整的渗透性测试分析报告，详细说明用户有可能存在的安全风险，含整改的手段及方案，并尽全力恢复好测试的系统原状态；

* 1. **安全通告**

服务商以邮件、微信、电话、走访用户、培训等方式，将安全技术和安全信息及时传递给用户，使用户能保持对信息安全最新动态的认识，提前预知风险，安全预警和通告的内容包括但不限于以下几个方面：紧急安全事件通告、业界最新动态、国际、国内行业安全政策及法律法规。

* 1. **安全迎检服务**

服务商需配合我方迎接上级部门或其他相关单位网络安全检查。

配合做好上级部门不定期的安全检查配合工作。做好信息自查和准备工作，满足对信息安全要求各类指标。包括各种检查内容的实际情况调查、完成相关检查表格准备并及时进行整理。提供安全检查所需资料和文档，并按照检查结果进行后续整改工作，确保圆满完成安全检查和达标考核。

检查时期需派1名工程师到达现场进行协助。

* 1. **安全加固服务**

安全加固服务指针对信息系统、网络设备、应用程序及网站的安全增强服务，旨在通过技术手段和管理优化，主动识别和修复潜在漏洞、降低安全风险，从而提升系统的整体防御能力，抵御外部攻击或内部威胁。服务期内需根据用户方实际需求开展安全加固协助服务。安全加固后，须不影响正常业务。

* 1. **安全教育与培训服务**

一年四次，需由我院推荐具有相关资质的培训讲师，面向全院人员进行培训。

信息安全培训的对象:管理层、信息安全管理人员、系统管理员、员工。

信息安全培训的内容：安全体系及安全职责分工培训、新员工入职安全培训、员工安全技术教育、各项安全专业技术教育、安全专业资格认证、信息安全内部考核（含培训）等内容。

协助获取专利、软著等知识产权，协助出版书籍、论文刊物、共同撰写数据标准体系、协同科研申报等，打造佛山市第一人民医院信息安全中心学习型、知识型、创新型的信息安全组织队伍。

**提供医院2个名额信息安全相关培训及认证名额，含培训期间食宿安排。**

* 1. **应急演练服务**

针对应急演练需要，提供应急演练场景，并按应急演练方案进行演练，一年提供1次。

投标方应根据招标人的实际情况对应急演练的内容提出建议，并有针对性的制定应急演练实施方案，根据实施方案开展相关准备工作和负责组织实施。在应急演练结束后，认真总结评价，并提交总结报告，对不足之处进行有针对性的整改，以提高应急工作的整体水平。

# 服务商资质要求

服务商应具备为我院提供优质安全服务的能力，至少满足以下条件：

1.满足应急响应2小时抵达现场的要求；

2.具备信息安全风险评估、信息安全应急处理服务资质三级或以上资质；

3．项目经理需具有PMP及CISP专业认证。

# 服务质量

1、本服务项目将每年对服务商服务成果进行考核扣分，扣分项目如下（基础分为100分）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 考核项 | 考核内容 | | | 扣分分值 |
| 安全事件 | 重大故障，系统瘫痪，无法运行，院级业务停顿 | 4小时及以上 | | 5分/次 |
| 2-4小时 | | 3分/次 |
| 1小时以内 | | 1.5分/次 |
| 受市级及以上管理部门信息及网络系统安全事件通报或下发整改通知书 | | | 3分/次 |
| 由第三方有资质安全公司对我院资产暴露扫描，发现我院互联网资产普通漏洞经证实每个扣1分，高危漏洞经证实每个扣3分 | | | 1或3分/个 |
| 系统部分设备故障，影响和限制了部分业务运营 | | 4小时及以上 | 3分/次 |
| 2-4小时 | 2分/次 |
| 1小时以内 | 1分/次 |
| 重大故障2小时未到现场 | | | 2分/次 |
| 参照《佛山市卫生健康系统2025年度网络安全工作责任制执行评估表》 | | | 10分/次 |
| 服务质量 | 未按时安全服务计划内项目 | | | 1.5分/次 |
| 未按时提交文档方案及报告 | | | 1分/次 |
| 按月检查未能达到安全预警平台指示80分 | | | 1分/次 |
| 《佛山市卫生健康系统2025年度网络安全工作责任制执行评估表》项目细项未协助落实 | | | 1分/项 |
| 加分项 | 协助培训本院信息安全人员参与市级以上信息安全技能比赛取得名次第一到第三名，加分3-1分（按次最多加3分），省级依次翻倍。 | | | +3分 |

2、基于医院信息安全的维保是一个长期战略性目标，为保证项目稳定，服务商考核评分为90分及以上，可按合同继续执行下一年度维保。

3、年度评分90分-70分，本院有权决定下一年度服务合作方向及评分，依据医院实际情况决定是否继续执行次年合同或合同终止重新招标。

4、为保证服务质量，任意年度服务考核如服务商得分为70分及以下，则自动终止下一年度服务合作计划，并且重新招标。

# 付款条件

第一年度考核评分为80分及以上，支付合同总价按年50%第一年度考核款；如考核评分区间为70--80分则支付按年30%第一年度考核款。70分以下支付按年20%第一年度考核款。

第二年度考核评分为80分及以上，支付合同总价按年50%第二年度考核款；如考核评分区间为70--80分则支付按年30%第二年度考核款。70分以下支付按年20%第二年度考核款。

**项目价格**

|  |  |  |  |
| --- | --- | --- | --- |
| **采购内容** | **数量** | **完成期** | **最高限价** |
| 信息系统安全服务  （两年） | 一项 | 自合同签订之日起2年内 | 依据审计及招标管理科组织的项目询价会议确定最高限价。 |

# 报价明细表

|  |  |  |  |
| --- | --- | --- | --- |
| **服务名称** | **服务内容** | **形式** | **报价** |
| **佛山市第一人民医院信息系统安全服务** | 驻点安全值守服务 | 现场 |  |
| 等级保护安全整改服务 | 现场 |
| 7X24小时应急保障服务 | 现场 |
| 安全巡检服务 | 现场 |
| 安全基线核查服务 | 现场 |
| 漏洞扫描服务 | 现场 |
| 系统安全性评估服务 | 现场 |
| 全网病毒态势分析服务 | 现场 |
| 安全迎检服务 | 现场 |
| 安全加固服务 | 现场 |
| 安全教育与培训服务 | 现场 |
| 应急演练服务 | 现场 |
| 其它 |  |
|  | |

# 服务方案

**9.1服务商需要提供详细服务方案，格式自拟。**

**9.2投标现场需讲解PPT版本的服务方案，时长15分钟内。**