**珠海市第五人民医院网络安全租赁项目**

**项目预算：人民币33万(¥330000.00元)**

**服务期限为半年（6个月）**

**服务质量要求**

**（一）网络安全防护系统**

1.中标人为我院方提供网络安全防护系统，其中，网络层吞吐量 30Gbps、应用层吞吐量10Gbps、最大并发连接数1000万、新建连接数15万/秒。

2.中标人需在合同签订后5个工作日内完成系统安装，确保防护系统与我院现有网络系统无缝对接且正常运行。

3.中标人需为该防护系统提供特征库与病毒库升级授权，确保防护系统持续匹配最新网络安全威胁。

**（二）安全系统提供与部署**

服务期间，中标人需为我院提供并部署以下安全系统，确保系统正常运行且满足医疗行业信息安全防护要求：

1.运维安全管理系统：具备账号统一管理、权限细粒度控制（按岗位分配操作权限）、操作行为审计（全程记录运维操作）、会话监控功能，防止未授权操作引发数据泄露或系统故障。

2.日志审计系统：可采集医院服务器、网络设备、安全设备，支持日志分析、异常行为实时告警、日志存储（周期不低于 6 个月）及合规报表生成，符合《网络安全法》《数据安全法》对日志留存的要求。

3.态势感知系统：具备网络威胁实时监测、漏洞扫描、安全事件分析、风险预警功能，可视化展示网络安全态势，每月生成《网络安全态势分析报告》，包含威胁统计、风险预警及应对建议。

**（三）医院内部网络梳理**

中标人需在合同签订后2 个月内完成我院内部网络梳理，为后期网络规范化建设奠定基础，具体内容包括：

1.网络拓扑梳理：排查院内交换机、路由器、防火墙等设备的部署位置、型号、IP 地址、连接关系，绘制《医院内部网络物理拓扑图》、《逻辑拓扑图》；

2.网络资产梳理：统计服务器、存储设备、办公终端、诊疗设备的数量、型号、所属部门、IP 地址、操作系统及运行应用系统，形成《医院网络资产清单》；

3.问题排查与优化建议：排查网络带宽瓶颈、设备老化、架构不合理等问题，提出针对性优化建议，形成《医院网络优化方案》；

4.成果交付：上述拓扑图、资产清单、优化方案需经我院信息安全管理部门确认，确认通过后存档作为后期网络建设参考依据。

**（四）驻场服务与团队支撑**

驻场人员配置：中标人至少安排 1 名专职网络安全技术人员驻场服务，服务时间与我院信息安全管理部门协商（含节假日）。驻场人员需具备《网络工程师认证》、《信息安全等级保护测评师（初级及以上）》同等证书或资质，熟悉行业网络安全规范，主要职责包括：

日常巡检：每日 1 次检查防火墙、安全系统运行状态，记录设备负载、带宽使用、安全告警等信息，形成《每日巡检日志》；

基础运维：负责防火墙基础策略调整、安全系统日常操作，协助甲方处理办公终端、诊疗系统网络连接问题；

团队协同支撑：当遇驻场人员无法独立解决的复杂问题（如网络攻击事件、防火墙深度故障、安全系统兼容性问题等），中标人需在 1 小时内启动团队支撑机制，调动中标人技术团队（含网络架构、安全防护、系统运维专业人员）提供支援，包括 24 小时内现场支援、联合故障排查，确保重大问题 48 小时内解决、一般问题 24 小时内解决，并提交《问题处理报告》。