# 服务范围

1、对全院已过保的有线网络设备提供软硬件保修服务；

2、对全院网络设备（有线、无线）提供日常巡检维护、保养服务；

3、服务期内提供专用备件服务，设备备件需放置医院机房；

4、提供esight网管平台更新服务；

5、提供1名专职网络工程师驻场服务；

二、维保服务内容

1、服务总体要求

1.1 维护合同期内，对招标方全院已过保的网络设备提供软硬件保修服务(详见清单)，要求服务方提供整机维修和系统维护服务，并承诺不额外收取人工、部件等任何其它费用。

1.2 服务方式：要求服务方安排1名专职网络工程师提供现场服务，提供7\*24小时响应，服务期间服从医院现场管理。

1.3 工作内容要求：对全院有线、无线网络设备进行日常巡检维护、配置变更、AP位置变更、网络优化、故障排查、修复建议等工作。

1.4 服务期内，要求服务方提供专用备件服务；备件包括：数据中心交换机、接入层交换机以及部分接入防火墙，所有备件均需放置到医院机房现场；

1.5 服务期内，要求服务方提供医院内网所需的esight网管平台更新服务；要求服务方购置并提供原厂维保服务：含1套eSight 管理平台和300个eSight 网络管理许可；

1.6 首次维保前，要求服务方提供根据现场情况提供一份完整的网络设备资产清单。

2、技术服务要求

2.1服务方在首次维护前，对项目范围内的网络设备进行一次摸底排查，提供一份完整的设备现状报告，提出相关建议。

2.2协助招标方逐步建立一套规范、科学、高效的IT运维服务体系，包括规范运维工作行为、服务流程和服务标准，有效管控服务过程等。

2.3负责有线、无线网络设备的配置调整工作，包括开局及配置变更；保障网络设备的稳定、健康运行，降低设备故障率，提升设备使用寿命。

2.4协助对招标方的网络系统进行完善设计和实施；配合新系统上线部署与网络压力测试。

2.5协助招标方更新网络拓扑图、点位图等技术资料，定期检查网络设备，发现问题及时反馈。

2.6定期对机房内核心、汇聚、接入网络设备进行检测，分析各种影响系统稳定、安全的因素，提出预防性的意见和应采取的措施。

2.7配合招标方年度重点事项的保障工作，以及信息部门交代的其他临时性事务。

3、设备维保服务

3.1 要求服务方提供项目维保范围内设备的硬件保修服务，备件更换时效≤48小时，如无法及时提供备件的需在故障上报12小时内提供备件替换；

3.2 电话支持服务：提供7×24h技术支持；

3.2 电话支持服务：要求服务方提供7×24h技术支持；

3.3 远程支持服务：要求服务方提供远程操作支持；

3.4 邮件支持：要求服务方提供邮件支持；

3.5 请求式专家现场支持服务：要求服务方按需提供专家现场技术支持，不限次数；

3.6 健康检查周期：要求服务方每月提供一次维保设备的健康检查。

4、巡检及保养服务

4.1巡检服务范围包括医院网络设备（含有线、无线），每月定期提供巡检服务。

4.2服务方每月针对巡检范围内的网络设备进行全面的健康检查，并协助解决医院在日常运维中遇到的故障问题，健康检查内容包含但不限于：架构分析、日志分析、系统的资源运转情况分析、补丁及策略合理性分析、故障隐患分析、优化改进建议、问题跟踪处理等，生成统一报表，巡检服务后7日内提交正式的巡检报告；

4.3 服务方提交的巡检报告中应有描述本期巡检和上期巡检情况对比，以及故障处置的情况。

4.4 服务方每季度针对院方全院弱电间网络设备进行设备除尘保养服务。

4.5 服务方随时了解院方网络设备运行情况，及时预防、遇到问题及时解决，优化系统参数，尽量减少系统故障，保持业务持续性运行，避免了小问题叠加，减少了突发性故障发生率。

4.6 配合好院方的系统切换、停机值守、应急演练等网络系统范畴内的工作。

5、专用备件服务

5.1 服务方应在合同签订后7个工作日内，为医院提供一批完整且未使用的、性能良好且与现有网络设备兼容的备件设备，该批备件为本项目专用，放置于医院信息机房现场供医院使用；采购方将对中标服务方提供的备件设备数量及性能配置现场检查，如发现备件的数量或性能参数与投标响应不符的，将视为虚假响应，并根据《中华人民共和国招标投标法》，上报有关行政监督部门，由相关行政监督部门对虚拟响应行为进行处罚；

备件数量及性能具体要求如下

5.1.1 数据中心交换机备件，备件的功能/性能指标不低于如下要求：

1）数量：2台或以上

2）硬件配置交换容量≥4.8Tbps，包转发率≥2000Mpps；

3）需与医院现有网络设备/系统兼容。

5.1.2 接入层交换机备件，备件的功能/性能指标不低于如下要求：

1）数量：12台或以上

2）硬件配置交换容量≥758Gbps，包转发率≥144Mpps，配置≥1个AC电源；

3）需与医院现有网络设备/系统兼容。

5.1.3服务器区防火墙备件，考虑备件能快速替换现网使用的防火墙，而且端口数量和性能要能满足现网业务需求，要求备件的功能/性能指标不低于如下要求：

1）数量：2台或以上

2）防火墙功能包含应用识别、IPSec VPN、数据防泄漏、带宽管理、Anti-DDoS、虚拟防火墙功能；威胁防护等软件许可能正常使用；

3）需与医院现有网络设备/系统兼容。

5.1.4专网边界防火墙备件备件的功能/性能指标不低于如下要求：

1）数量：2台或以上

2）防火墙功能包含应用识别、IPSec VPN、数据防泄漏、带宽管理、Anti-DDoS、虚拟防火墙功能;威胁防护等软件许可能正常使用；

3）需与医院现有网络设备/系统兼容。

5.2 备件设备应处于随时可投入使用的状态，服务方每月需对备件设备进行加电测试、进行全面检测和维护，确保备件随时可用；备件存放在医院信息机房，以确保在故障情况下能够及时进行更换。

5.3 当医院现有网络设备进行升级或更新时，如所提供的备件不满足医院网络系统所需的性能需求时，服务方应免费对备件设备进行升级或更新，以保持兼容性和稳定性。

5.4 在医院网络设备发生故障时，服务方应在接到通知后的1小时内完成备件的安装和调试，确保网络尽快恢复正常运行。

5.5 当医院原有故障设备修复后，服务方应在3个工作日内（具体时间由医院指定）内将备件取回，并对其进行维护和检测，以备下次使用。

6、应急支持服务

6.1为确保遇到IT基础设施重大故障能及时处理，服务方需为本项目配备应急保障小组，在重大网络/系统/病毒入侵等事件中，应急小组迅速介入从而把损失降至最低。

6.2对于每次应急响应，服务方应保存现场资料，协助分析产生问题的原因，记录维护使用的方法、步骤和参数，制定防止类似问题发生的解决方法，同时提供《应急响应总结报告》。

6.3服务方提供7x24小时不间断响应服务，当医院IT维护人员遇到网络系统故障无法解决时，可随时联系到服务方，服务方应在收到医院IT维护人员保障后10分钟内提供远程支持服务（无限次数），服务方式包括但不限于电话、电子邮件、即时通讯软件、紧急事件上门服务等。

6.4医院整体网络架构与网络安全有重要关联，本项目要求服务方具备网络安全应急服务能力；故要求服务方具有信息安全管理体系认证证书，和中国网络安全审查技术与认证中心颁发的信息系统安全运维服务资质（三级）证书；

6.5在医院发生网络安全相关的紧急或重大事件时，服务方需安排至少1名CISP（中国信息安全测评中心颁发的注册信息安全工程师）持证人员提供上门应急响应服务（要求投标时提供证书扫描件及投标人为其缴交的近三月社保证明）。

7、服务质量保障

7.1文档管理及服务记录：服务方应严格将文档管理贯穿于整个项目全过程中。文档提交及文档质量将作为医院考核的重要依据。巡检、保养需详细记录，按时提交巡检记录和服务报告，发现问题及时整改。

7.2招标方可以对服务单位的服务满意度及投诉数量作为对服务方服务水平监督的指标。通过定期的报表和统计，招标方可以根据服务的满意度及投诉数量对服务单位进行处罚。

7.3服务方需提供服务监督及评价机制，提供服务统计及故障分析。服务方提供服务人员工作量考核机制、服务统计及故障分析数据，接受管理和监督，并向医院及时提交《巡检报告》、《维护记录单》等文档。