**网络维保服务要求**

**一、概况**

**1.背景**

随着我院信息网络化程度的提高，终端设备及移动设备增多，各方面的业务应用系统增加，对当前我院信息网络系统的基础设施运行的稳定性、信息系统内数据传输的安全性、系统故障恢复的及时性提出更高的要求。特别是“新冠疫情”爆发以来，我院以救治患者、控制疫情为目的，改善医患关系，提高患者就医满意度，我院各业务系统的稳定运行起着至关重要的作用。

我院一直致力于信息化系统建设。当前我院信息系统包括基础设施、信息安全系统、灾备数据存储系统等建设较为完善，为我院各个业务系统提供了强有力的安全保障。但我院信息系统基础设施逐渐老化，出现故障的次数逐渐增多，需要专业的网络维护提供商对我院的网络系统基础设施进行维护，优化网络环境，保障信息网络系统稳定运行。

**2.网络现状**

网络基础设施以及网络安全是我院业务系统运行的主干枢纽和重要安全保障，但我院信息网络系统中部分硬件设备比较陈旧，在网运行时间过长，性能低下，安全策略级别较低，基本依赖于医院的高速交换网络以及稳固的网络安全设备、安全策略提供高速数据转发和安全防御。

**二、维保服务要求**

**1.服务方式**

1.1备件服务：提供7×24小时备件，备机支持服务；

1.2远程服务：通过VPN网络接入院方进行远程协助的方式处理维保问题；

1.3现场服务：通过现场的方式直接进行故障的解决处理；

1.4在故障的处理过程中，优先选择最快速恢复业务的服务方式，及时对事件做出响应，缩短故障的解决时间；若远程方式无法有效解决故障，需及时通过现场服务方式进行故障的解决。

**2.服务时间**

2.1提供7×24小时服务台支持

2.2提供7×24小时备件，备机支持

2.3提供7×24小时现场支持

**3.服务指标**

供应商须提供院方所有“产品清单”（详见本节“9.产品清单”）的备件支持（7×24小时），在院方现场放置部分常用及重要备件，并针对业务提供高级别的支持。

**4.具体服务内容**

|  |  |  |
| --- | --- | --- |
| 序号 | 分类 | 具体服务内容 |
| 4**.**1 | 远程问题诊断与支持服务 | 院方可通过指定电话、邮件、网站提出服务请求，服务提供方远程服务工程师需及时与院方沟通，通过电话支持/远程接入等远程方式对服务范围内的设备进行诊断及技术支持。 |
| 4**.**2 | 现场支持服务 | 对于没有条件进行远程支持、或未能通过远程支持诊断解决的问题，服务提供方服务工程师在SLA约定时间内到客户现场进行问题的诊断、并负责硬件相关问题的排除。 |
| 4**.**3 | 备件支持服务 | 根据远程或现场诊断结果，如需更换备件来修复硬件问题，服务提供方在合同规定的服务时效内将备件送至现场并使用备件恢复业务。提供7\*24小时备件，备机支持服务。 |
| 4**.**4 | 紧急故障恢复服务 | 由于客观原因无法及时判断、定位故障的情况下，服务提供方服务工程师将在征求院方的意见后，提供紧急故障恢复服务，利用应急预案或经院方许可的技术方案进行应急处置，优先恢复业务。 |
| 4.5 | 辅助故障定位服务 | 在客户端如出现系统故障难以迅速准确定位的情况，服务提供方服务工程师提供辅助故障定位服务，通过协调、配合相关软硬件服务厂商共同对系统故障进行排查定位，避免因多方推委造成院方业务的损失。 |

**5.运维服务**

5.1要求服务提供方提供从监控/巡检、预防性检查、日常运维到服务请求和事件响应、系统优化的全面支持。通过运维服务，为院方基础架构的扩展提供实施和必要的支持工作。

5.2同时通过专业的技术服务团队通过专业的可以落实的服务方案，高效规范的管理模式、管理流程和管理工具提升院方的运维服务水平。

**6.服务方式**

运维服务的形式采用按需响应式支持服务，主要采用以下两种方式提供：

6.1远程服务：通过VPN等手段进行远程监控和故障的解决处理；

6.2现场服务：通过现场的方式直接进行故障的解决处理；

**7.网络运维服务**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 类别 | 方式 | 服务描述 |
| 1 | 网络监控 | 远程 | 7×24小时对网络设备（含网络安全设备）及网络整体的运行状态，各项硬件资源开销和容量，链路的健康状态等信息进行监控。 |
| 2 | 设备上下架 | 现场 | 根据变更请求，对网络硬件设备（含网络安全硬件设备）实施上架、系统初始化及下架等操作 |
| 3 | 设备巡检 | 现场 | 定期对网络设备（含网络安全设备）进行现场巡检，定期对设备进行清洁 |
| 4 | 故障排查 | 远程/现场 | 分析并处理网络设备（含网络安全设备）及网络链路发生的故障和终端设备断网故障 |
| 5 | 配置调整 | 远程/现场 | 根据变更请求，对网络设备（含网络安全设备）的配置（IP、VLAN、路由及端口等）进行调整，优化，版本升级 |
| 6 | 配置管理 | 远程/现场 | 对机柜位置、网络拓扑、VLAN、IP资源及网络设备的配置（含网络安全设备）进行管理 |
| 7 | WAN管理 | 远程/现场 | 协助客户、其他供应商进行专线、VPN的接入及配置；协助其他供应商进行网络测试、扩容 |
| 8 | 优化建议 | 远程 | 参与到数据中心网络建设项目中并对数据中心网络建设，网络安全和日常运维优化提出建议 |
| 9 | 线路调整 | 现场 | 机房内所有线路，若存在不规范的布线的，给出实施方案并完成规范化布线 |
| 10 | 防病毒管理 | 远程/现场 | 部署、配置终端操作系统防病毒，配置及检查防病毒更新情况 |
| 11 | 新增网络布线 | 现场 | （1）网络线路铺设具体要求：线缆需全程套管，明线部分需走线槽，使用医院铺设好的桥架走线，未铺设桥架部分走线需经信息部审核  （2）标签制作：铺设的网络线缆，要求制作标签。标签按照医院现有的编号规则，使用标签打印机打印，标签要求整洁，清晰  （3）网络测试：要求所有的线缆（八芯）都能够测试通过，传输速度能够达到1000M |
| 12 | 网络线路维修 | 现场 | 根据院方的要求对网络点位进行移点、找点和线路维修 |
| 13 | 系统升级 | 远程/现场 | 配置、检查设备系统补丁，根据系统安全进行系统及补丁升级管理 |
| 14 | 日志分析 | 远程/现场 | 定期对网络设备（含网络安全设备）的日志进行分析，发现安全问题及时上报及处理。 |
| 15 | 现场保障 | 现场 | 医院遇到重大检查时，派服务工程师到现场保障 |
| 16 | 其它要求 | 远程/现场 | 院方在后期会加入路由器、负载均衡、IDS、IPS，上网行为管理等设备，要求投标人具备全设备调试，故障恢复能力 |

**8.运维服务内容**

（1）基础设施管理

* 确保医院信息系统网络通信传输畅通。
* 负责网络布线架的管理，确保配线的合理有序。
* 掌握医院端设备接入网络情况，以便发现问题可迅速定位。
* 采取技术措施，对网络内经常出现的医院需要变更位置和部门的情况进行管理。
* 掌握与外部的链接配置，监督网络通信状况，发现问题后与有关机构及时联系。
* 实时监控局域网络的运行和网络通信情况。

（2）操作系统管理

* 在网络操作系统配置完成并投入正常运行后，为了确保网络操作系统工作正常，首先利用系统提供的各种管理工具软件，实时监督系统的运转情况，及时发现故障征兆并进行处理。
* 在网络运行过程中，随时掌握系统配置情况及配置参数变更情况，对配置参数进行备份更新。随时做到系统环境变化、业务发展需要和医院需求，动态调整系统配置参数，优化系统。

（3）应用系统管理

* 确保各种网络应用服务运行的不间断性和工作性能的良好性。出现故障时应将造成的损失和影响控制在最小范围。
* 对于要求不可中断的关键型网络应用系统，除了在软件手段上要掌握，备份系统参数和定期备份系统、业务数据外，必要时在硬件手段上要建立和配置系统的热备份。

（4）局域网环境检查

* 利用ping命令测试到路由、交换机以及外部网络的连通性。
* 查看所有路由、交换机端口以及状态灯的工作状态，保证设备工作正常。
* 检查网关设备（防火墙、路由）工作状态，确保外网连接正常。
* 检查网络线缆，确保网络线缆完好无损。

（5）终端环境检查

* 检查终端计算机系统是否摆放整齐，检查机箱及显示器是否干净整洁。
* 检查终端计算机系统运行是否正常，磁盘空间是否满足工作需求。
* 检查安装的软件工作是否正常，保证网络环境没有病毒传播问题。一旦发现必须及时做有效性处理。
* 定期对客户机进行抽查，删除无用文件，对储存于工作无关文件的客户机进行删除清理。
* 对于计算机常用外置配件（键盘、鼠标、耳机）进行日常测试维护。
* 计算机的硬件维修、维护及更换。包括计算机无法启动、蓝屏、系统无法登陆等维护。

（6）其他内容

* 网络设备定期清洁、除尘。
* 网络设备标志标记修复。
* 重大检查时派服务工程师到现场保障。
* 网络的调试、网络故障的排除、网络设备的检修、布线系统的故障检修及故障排除等。

**9.产品清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品描述** | **产品数量** | **单位** |
| 一、航天院区一期 | | | |
| 1 | 核心数据交互平台(含4块48口千兆电口板卡、2块24口万兆光口板卡、4块万兆引擎板卡、8个电源、8个风扇) | 2 | 套 |
| 2 | 核心数据交互平台(含4块24口千兆电口板卡、2块24口万兆光口板卡、4块引擎板卡、8个电源、8个风扇) | 2 | 套 |
| 3 | 汇聚数据交互平台 | 3 | 套 |
| 4 | 24口接入数据交互平台 | 98 | 套 |
| 5 | 48口接入数据交互平台 | 87 | 套 |
| 6 | 边界出口防火墙 | 3 | 套 |
| 7 | 网络安全审计平台 | 1 | 套 |
| 8 | 终端安全管理系统 | 2 | 套 |
| 9 | 安全隔离与信息交换系统 | 1 | 套 |
| 10 | 日志审计平台 | 1 | 套 |
| 11 | 运维审计平台 | 1 | 套 |
| 12 | 漏洞扫描系统 | 1 | 套 |
| 13 | 入侵防御系统 | 1 | 套 |
| 14 | 数据库安全网关 | 1 | 套 |
| 15 | 态势感知系统 | 2 | 套 |
| 16 | 数据库审计系统 | 1 | 套 |
| 17 | 文件威胁鉴定系统 | 1 | 套 |
| 18 | 网络安全分析检测指挥平台 | 1 | 套 |
| 19 | 数据中心核心防火墙 | 2 | 套 |
| 20 | 安全接入网关 | 1 | 套 |
| 21 | 抗拒服务统 | 1 | 套 |
| 22 | 网络数据防泄漏系统探针 | 1 | 套 |
| 23 | 数据库脱敏系统 | 1 | 套 |
| 24 | 负载均衡系统 | 2 | 套 |
| 25 | 业务支撑系统 | 4 | 套 |
| 26 | 通信控制系统 | 2 | 套 |
| 27 | 视频会议系统 | 2 | 套 |
| 28 | 会议室多业务网关（带wifi功能） | 1 | 套 |
| 29 | 无线控制器 | 2 | 台 |
| 30 | 无线AP | 50 | 台 |
| 二、航天院区二期 | | | |
| 31 | 核心数据交互平台(含2块引擎、1块24口千兆电口板卡、1块24口千兆光口板卡) | 1 | 套 |
| 32 | 核心数据交互平台(含2块引擎、1块24口千兆光口板卡) | 1 | 套 |
| 33 | 48口接入数据交互平台 | 29 | 套 |
| 三、净居寺院区 | | | |
| 34 | 核心数据交互平台(含2块引擎、1块24口千兆电口板卡、2块24口千兆光口板卡) | 2 | 套 |
| 35 | 互联网出口防火墙 | 1 | 套 |
| 36 | 24口接入数据交互平台 | 16 | 套 |
| 37 | 48口接入数据交互平台 | 11 | 套 |
| 38 | 无线AP | 53 | 台 |
| 39 | 网络线路改造 | 1 | 套 |

**10.技术要求**

由于我院部分硬件设备比较陈旧，在网运行时间过长，性能低下，安全策略级别较低，基本依赖于医院的高速交换网络以及稳固的网络安全设备、安全策略提供高速数据转发和安全防御。因此供应商须提供部分重要设备的备品备件。