机房运维服务需求

一、采购需求

机房整体打包运维管理，含数据库系统设计、虚拟化系统设计、服务器操作系统维护、网络系统维护、安全系统规划设计、虚拟环境系统维护、数据备份、恢复及维护。

我院现有机房包含数据系统、应用系统、虚拟化系统，包含多种硬件设备和软件系统。

服务器系统包含多台X86服务器系统。

存储系统有华为、曙光等品牌。

网络与安全系统包含核心交换机、路由器、防火墙等设备。

软件系统包括LINUX操作系统、Windows操作系统、服务器虚拟化系统、双机集群软件、数据库软件等。

具体内容如下：

|  |  |
| --- | --- |
| **（1）** | **数据库系统设计** |
|  | **生产系统数据库** |
|  | 数据库(database)的设计 |
|  | 数据库分区（Partitaion）的设计 |
|  | 聚簇（Cluster）的设计 |
|  | 表空间（TableSpace）的设计 |
|  | 表及索引（Table/Index）的设计 |
|  | Oracle用户（User）设计 |
|  | 数据库角色（Database Role）设计 |
|  | 数据库接口设计 |
|  | 物理设计 |
| **（2）** | **虚拟化系统设计** |
|  | **生产区数据库主机规划与设计** |
|  | 主机系统拓扑设计 |
|  | 主机资源规划 |
|  | 主机命名规则 |
|  | 主机容错设计 |
|  | 虚拟化日常维护 |
| **（3）** | **操作系统维护** |
|  | **生产区数据库主机操作系统规划与设计** |
|  | 操作系统补丁管理与验证 |
|  | 用户及组的权限管理设计 |
|  | 文件系统设计 |
|  | 容错及并行系统设计 |
|  | **生产区应用主机操作系统规划与设计** |
|  | 操作系统补丁管理与验证 |
|  | 用户及组的权限管理设计 |
|  | 文件系统设计 |
|  | 容错及并行系统设计 |
|  | **磁盘阵列规划与设计** |
|  | 根据信息生命周期管理设计存储资源 |
|  | 磁盘分布及IO设计 |
|  | 读写Cache比例设计 |
|  | RAID设计 |
|  | Hotspare设计 |
|  | LUN划分设计 |
|  | Snapshot设计 |
|  | **SAN交换机的规划与设计** |
|  | 根据应用划分ZONE |
|  | SAN交换机安全控制设计 |
|  | 端口绑定(Trunk)设计 |
| **（4）** | **网络系统维护** |
|  | **网络系统整体规划与日常维护** |
|  | 网络系统需求分析 |
|  | 网络系统结构和容量规划 |
|  | 网络系统日常维护 |
|  | **网络系统逻辑结构设计** |
|  | 业务种类划分 |
|  | 信息流量流向分析 |
|  | 网络设备安全控制规划 |
|  | IP地址规划 |
|  | LAN(局域网)设计 |
|  | MAN(城域网)设计 |
|  | WAN(广域网)设计 |
|  | 子网/VLAN规划 |
|  | Qos/CoS规划 |
|  | 网络设备命名规则 |
|  | 网络系统拓扑结构设计 |
|  | 网络系统路由协议设计 |
|  | **网络系统物理结构设计** |
|  | 信息资源分布 |
|  | 信息站点分布 |
|  | 传输链路路由设计 |
| **（5）** | **安全系统规划、设计** |
|  | **安全系统整体规划** |
|  | 物理层安全设计 |
|  | 链路层安全设计 |
|  | 网络层安全设计 |
|  | 主机操作系统安全设计 |
|  | 数据库系统安全设计 |
|  | 中间件系统安全设计 |
|  | 应用系统安全设计 |
|  | 网络系统安全审计设计 |
|  | 防病毒系统设计 |
|  | 安全域逻辑隔离与访问控制设计 |
|  | 网络入侵检测规划 |
|  | 网络安全漏洞扫描设计 |
|  | 跨安全域隔离与数据提取设计 |
|  | CA认证系统规划 |
| **（6）** | **虚拟环境系统维护** |
|  | 虚拟机环境安装与部署 |
|  | 虚拟机环境备份与恢复 |
|  | 虚拟机环境配置与调优 |
|  | 虚拟机环境维护与故障排除 |
| **（7）** | **数据备份、恢复及维护** |
|  | 生产数据库备份与恢复 |
|  | 生产数据库配置与调优 |
|  | 数据库维护与故障排除 |

二、资质要求

1.投标人必须有至少1名ORACLE OCP认证工程师，1名H3C、华为或思科网络认证工程师，1名VMWARE VCP证书，1名PMP项目管理证书；

2.投标人要有近三年医院机房运维服务相关经验。

三、服务方式及服务标准

**1.****预警服务**

为了避免出现重大故障，在不干扰业务运行的前提下，通过常规巡检，对网络、设备、系统及数据库等进行性能测试和效能分析，以便及时发现故障征兆。

**2.协助服务**

主要指针对系统运行而进行的使用咨询、疑难问题解决和系统升级方案设计等，完成一些重大业务，如参数设置、数据转移、突发事件处理等维护服务活动。

**3.建档造册服务**

梳理并统计我院各节点网络设备、安全设备、服务器设备、存储设备等信息，并做好变更管理。系统设备铭牌日志（如设备名称、合同采购号、产品生产日期、保修期限、IP地址、安装位置以及供应商、联系人名称、电话等）和系统设备现场情况书（如系统设备现场连接拓扑图、各系统设备接口永久不褪色标签标记，变更记录表等），形成《中心机房设备资产统计表》。

**4.定期巡检**

为了建立高效、完善的质量管理和保证体系，在技术服务的系统巡检过程中，制定系统巡检管理办法，用以在规范系统巡检项目的工作行为，使系统巡检的工作规范化和正规化。系统巡检规范能保证系统巡检过程按照科学合理的流程进行，让我院及早预知设备故障、及时排查潜在隐患、减少设备发生故障的概率，通过系统调整等手段，减少设备发生故障的概率，保证设备稳定、高效运行。提供现场健康检查服务，定期对系统设备的运行状况进行全面的健康检查，**巡检次数为每月一次。**具体内容如下：

服务期提供设备现场巡检服务，按照我院维保系统预防性维护管理规程的相关要求，对我院设备进行细致全面的健康检查。检查的内容包括软件、硬件检查，电源、告警及设备运行环境的检查等，以及对现场进行环境评估与指导，并及时提供巡检报告。完成现场设备巡检后需配合我院工程师填写《设备巡检记录表》。

需为我院建立设备维修档案，并根据设备运行情况向我院提供设备升级、改造、更换的建议和方案。

除根据维护要求对系统进行维护外，维护人员每月对医院信息系统平台进行性能测试一次，并结合测试情况，修改不符合性能要求部分。

在信息中心的指导下，对本院网络系统进行定期的回访，解决院内网络系统中存在的问题。

**5．应急处置服务**

为了确保维护设备和系统发生故障或面对意外灾难时，相关服务能在最短时间内得以恢复以使正常的业务运营继续进行，保证用户端数据安全，将损失降低到最小限度，将协助我院制定应急方案。

具体应急方案建议如下：

（1）应急预案体系架构原则

应急保障预案体系的建立，以强化安全意识，全面提高各相关部门应对突发事件的综合管理水平和应急处理能力，确保网络安全畅通，通信快速恢复为目的。

应急预案由服务方和我院共同编制，针对不同的故障级别将制定相应的应急预案。所编写的应急预案应具有实用性、可操作性，预案中各角色职责明确。

应急体系原则上每年更新一次，出现以下情况的须及时更新或新建立：

上一级主管部门职能、结构发生变动，影响到本部门应急预案实施。（包括联系人、联系方式变动、处理流程发生变化的）

本部门职能、结构发生变动，影响到本部门应急预案实施。（包括联系人、联系方式变动、处理流程发生变化的）

有新的网络或业务正式投入使用，没有与之相符的应急预案与之相对应的。

（2）应急预案的内容

应急预案由服务方和我院共同编制，针对不同的故障级别将制定相应的应急预案。应急预案主要包括如下内容：

1）应急预案的启动条件

2）应急预案执行所需要的资源

3）应急预案的操作流程

（3）应急小组人员安排

为了保证在故障发生时能够得到快速、有序地处理，事先要与用户、厂商等商量建立起项目应急处理工作小组，小组成员包括相关各方主管领导、项目经理、接口人、技术专家组成。

主管领导：帮助组织、进行指导，协调资源；

项目经理：协调各方资源，组织进行故障排除；

接口人：在故障发生时保持与各方联系，帮助进行协调处理，可以由项目经理或驻场工程师担任。

技术专家：由项目相关各产品责任技术专家组成，负责处理项目中产品发生的故障。

**6.保障体系及响应要求**

（1）7×24小时畅通的申报热线

提供全年365天7×24小时的热线支持，保证院方在需要帮助无论何时都能方便快捷的得到专业工程师的响应和支持，遇紧急故障，提供技术专家2小时到达现场支持服务。

（2）人员的培训

对于我院，服务方将提供适当的现场培训，以提高现场管理员的技术水平，并对机房设备的操作规范提出我方的建议，规避不正确的操作可能造成的严重后果。

（3）专家支持

对于我院系统调整等重大事件，服务方将积极配合给予支持，并在需要的时候安排专家对相应方案给出评审意见，以保障我院变更的顺利实施。

（4）升级原厂

有IBM、HP、华为、Oracle、EMC、H3C、迪普等原厂合作经验，可在处理我院故障问题的时候获得原厂技术支持。

（5）问题报告

在每个事件（每次服务）处理之后给我院提供《事件问题处理报告》，每季度结束后的5个工作日内，向我院提供《季度服务总结》及《季度服务清单》，以便我院全面准确的了解维保服务实施情况。

《季度服务总结》内容包括但不限于:

**a.服务情况的总结:**对上个季度的设备整体运行情况进行总结，评估每次巡检的效果；总结分析遗留问题处理情况；

**b.故障分析报告:**对故障的发生原因、处理过程和处理结果进行详细说明，并给出预防该类故障再次发生的建议；

故障概率、趋势分析；

**c.计划执行分析:**分析技术支持服务实施计划的执行情况，对计划未执行项或未按时执行项进行原因分析。对出现服务质量问题及不符合合同约定的情况需提出分析报告和整改措施；

**d.问题分析:**对巡检过程中出现的未曾预见的问题，及时分析总结并给出解决建议。

《季度服务清单》内容包括但不限于:每次服务的日期、故障设备名称及序列号、故障描述、故障状态、处理过程、处理结果、备件名称及序列号、确认人、联系方法等。