#### 以下所有内容均包含中医药数据中心，五个部分分开报价

#### IT驻场服务要求

| **序号** | **名 称** | **主要服务要求** | **数量/单位** |
| --- | --- | --- | --- |
| 1 | 网络系统及安全系统维护驻场工程师 | 1、协助院内网络及安全设备资产的全生命周期的管理；2、负责全院网络及安全系统的日常管理；3、负责网络及安全系统软硬件的升级、维护等工作；4、协助处理医院的各类网络及安全突发事件、紧急事件，确保各部门网络通畅，不得因网络问题影响医院正常工作；5、协助建立并在院方监督下严格执行计算机网络及安全管理制度；6、协助院方做好网络及安全设备的资产管理，每日做好设备巡视并有工作日志；7、能熟练利用系统运维工具对网络设备进行日常监管理、配置维护；并能及时应答和回复使用部门提出的各类网络及安全有关问题；8、协助医院做好等保测评工作；9、医院内网核心交换机为H3C-12508，外网核心交换机为H3C-7506E，需具有运维此类型核心交换机的能力； | 1人/年 |
| 2 | 数据中心维护驻场工程师 | 1、协助数据中心各项资产的全生命周期的管理；2、每日定时对机房内的各类服务器（包括数据库服务器、应用服务器等）进行日常巡视，并做好工作日志；3、每日定时对主、备机房内的存储设备进行日常巡视，并做好工作日志；4、每日监控数据存储备份的情况、状态，并做好工作日志；5、每日监控服务器防病毒设置的状态，并做好工作日志；6、能熟练利用运维工具对数据存储设备进行管理、配置维护；7、每半年对数据中心进行一次评估，对存在的弊端、风险，提出优化与应对的策略和改进方案。8、数据中心专家级运维，针对虚拟化系统、超融合系统、存储系统、灾备系统极端故障、疑难问题进行故障排查，恢复生产。每季度出检测报告一份。 | 1人/年 |
| 3 | 桌面与终端维护驻场工程师 | 1、协助院内各部门终端电脑、打印机资产的全生命周期的管理；2、负责院内各部门电脑终端、打印机及院方指定的各种关联输入输出设备的日常管理、运维3、负责各类IT设备系统软件、安全软件以及常用工具软件的升级、维护等工作；4、每当接到报修电话，应问清报修的部门、设备的名称、故障的现象，并做好维护记录；5、协助院方制定终端的管理制度，尤其是防病毒措施，及时下载最新的病毒库，防止终端受病毒的侵害；6、能熟练运用系统运维工具对终端设备进行管理、配置维护；7、在需要的情况下能在2小时内赶到招标人单位，否则视为当季度考评不合格 | 3人/年 |
| **合计** |  | **5人/年** |

##### （1）驻场服务

驻场服务是指根据用户需求安排特定技术人员在用户现场进行维护的一种服务。服务的范围主要是根据服务的产品和具体服务的内容进行确定。驻场服务的主要目的是全面掌握系统的情况，并针对目前系统的情况进行定制化维护和优化，以避免维护性故障的发生，并解决系统存在的性能问题。驻场服务的主要内容包括：

* 确保设备的正常运转
* 故障应急响应
* 问题解决
* 系统健康性评估
* 系统全面优化
* 系统补丁与安全防护的部署

为确保院方相关设备完好，运转正常，驻场技术服务包括规范性日常维护，故障应急响应，设备问题解决等范围，具体工作包括但不限于以下内容：

**①网络管理及维护**

* 协助院方制定网络建设及网络发展总体规划，协助院方制定网络管理相应规章制度，并在院方监督下负责实施和执行；
* 掌握各种交换设备和服务器的安装、配置技术，管理交换设备和服务器的密码，处理各种网络设备的故障；
* 协助院方规划并配置网络设备安全策略；
* 规划网络IP分配策略，负责网络IP地址分配；
* 负责公用网络实体，如服务器、交换机、集线器、路由器、防火墙、网关、配线架、网线、接插件等的维护和管理；
* 负责服务器和网络软件的安装、维护、调整及更新；
* 监视网络运行，调整网络参数，调度网络资源，保持网络安全、稳定、畅通；
* 在出现设备硬件损坏时及时免费给予更换，如维修时间较长，需提供同档次备件；
* 密切关注互联网安全形势，能够及时有效处理突发安全问题。
* 针对院方安全上的不足，具备提出切实可行的预防措施的能力，并在院方监督下实施。
* 确保院方网络基础服务稳定运行，如内外网DHCP服务、网络准入服务、NAT服务、端口流控、防止ARP攻击等。
* 对网络存在的弊端、风险进行评估，提出优化与应对的策略和改进方案。

**②机房管理及维护**

* 在院方统一协调安排下，指派专人定期对机房供配电、空调、温湿度控制等设施进行检查记录；
* 指派专人出入机房，并及时登记，另外服务器的开机、关机等重大工作需专人进行记录并报备院方；
* 按照合同附件资产清单，建立服务器及网络设备的档案，形成不易破坏的醒目标识，并定期更新相关内容；
* 对资产清单所列的各种设备、线路等，做好检查维护工作，发现故障，及时报告，并安排服务联系或维修，对维修情况提交书面报告；
* 对资产清单所列的各种设备、线路运行及维修记录，按重要性级别，定期书面报告；
* 形成每日巡视制度，对机房中相关设备（包括空调、UPS等）的运行状态、告警信息等实际状态进行记录。

**③数据中心管理及维护**

* 服务器系统安装

根据用户需要，配合安装院方提供的服务器操作系统(Windows/Linux)，并对系统进行相应的配置，以满足用户对服务器使用的需求，提交服务器安装文档。

* 服务器监控

通过专业的监控和管理软件，对服务器的运行情况进行实时的监控，及时发现服务器运行过程中的异常问题，并对发现的问题进行相应的记录，提交服务器异常记录表，为后续的服务器优化、服务器故障解决提供依据；

* 服务器故障解决

在服务器出现故障时，及时对故障进行分析和定位，提出故障解决的方案，提交服务器故障分析解决报告；

* 服务器硬件维保

针对服务器的实际运行情况，对服务器硬件进行维护和保养。在出现设备硬件损坏时及时免费给予更换，如维修时间较长，需提供同档次备件；

* 服务器巡检

定期对服务器的硬件状态和运行情况进行巡检，提交服务器巡检报告。

文件服务维保要求保证文件的传输速率和文件服务器的系统安全。文件服务器具体内容包括两台文件服务器和FTP服务器。

服务器系统服务维保包括服务器系统安装、服务器环境的搭建和服务器系统性能的测试。

* 存储配置

根据用户需要对用户的存储进行合理的配置，以满足用户的使用需求，提交存储安装配置文档。

* 存储设备故障解决

在用户存储出现故障时，对故障进行及时的分析和定位，并提供故障解决方案，提交存储设备故障分析解决报告。

* 存储硬盘故障

存储硬盘故障或损坏时，免费提供存储硬盘的维修、更换等服务。

* 存储设备维保

对存储硬件设备进行常规的维护和保养，在出现设备硬件损坏时及时免费给予更换，如维修时间较长，需提供同档次备件；

* 存储设备巡检

根据需要定期对存储设备硬件状态和运行情况进行巡检，提交存储设备巡检报告。

* 虚拟化集群软件安装调试及运维

根据用户需要，为用户提供虚拟化集群操作系统、数据库、集群管理软件等相关服务，并在合同期限内承担虚拟化集群系统的安装调试，升级更新，日常维护、故障处理等工作，以满足用户的需求，提交集群软件安装文档。软件故障排查。安装调试质量需要达到原厂标准。

当集群软件出现故障时进行问题的定位和排查，提交故障分析解决报告。

* 集群策略调整

根据实际的需求对相关策略进行调整和优化。

* 配合用户安装数据库

配合用户安装oracle、mssql、mysql等数据库。

根据需要和数据库的版本发布情况，经讨论确认，在必要的情况下，做好数据库版本升级方案，确保数据库安全、平稳升级，保证软件版本为最稳定版本。

* 数据迁移

根据用户需要，对用户的数据进行迁移，提交用户数据迁移文档。

* 数据备份和恢复

对用户数据进行定期的备份和数据出现问题时进行数据恢复。

* 数据库故障排查、数据库运行环境巡检

当用户的数据库应用出现故障时，及时作出分析和排查，提供故障解决方案，提交数据库故障分析解决文档。

数据库服务维保要求对数据库进行定期备份，并监测备份、作业执行是否正确。数据库数量和种类根据用户指定，不低于20个。

* 数据中心进行评估，对存在的弊端、风险，提出优化与应对的策略和改进方案。
* 数据中心专家级运维，针对虚拟化系统、超融合系统、存储系统、灾备系统极端故障、疑难问题进行故障排查，恢复生产。

**④监控和安全服务**

* 通过IT资源监控系统，对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录、妥善保存并按重要性级别，定期书面报告；
* 指派专人期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；
* 指派专人，负责网络运行日志、网络监控记录的日常维护和报警信息分析和处理工作，提出优化建议及方案；
* 根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
* 定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时修补；
* 对关键的网络设备服务配置文件进行定期离线备份；
* 指派专人进行核心服务器的工作压力监控，针对业务的增长定期生成主服务器的工作压力报表，并且预估业务增长对服务器压力的影响提出合理化建议；
* 指派专人进行核心数据库的工作压力监控，定期生成报告，并就改进提出合理化建议。
* 提供有效手段，实现服务器、存储、网络设备的实时监控，要求采集的数据时间间隔不大于12小时。
* 提供有效手段，实现虚拟化环境的实时监控。

**⑤技术档案管理及备份服务**

* 做好计算机网络资料的整理和归档；
* 编制网络拓扑图、网络接线表、设备规格及配置单、网络管理记录、网络运行记录、网络检修记录等网络资料；
* 每年对单位计算机网络的效能进行评价，提出网络结构、网络技术和网络管理的改进措施。
* 负责对所有设备的应用操作，每季度提交每个设备的配置和存储应用情况报告、网络拓扑报告、IP分配报告；
* 对新应用的设备需求，驻场工作人员应及时提交设备配置现状及设备规划报告，以便该应用能及时实施；
* 掌握设备的运行情况，就保修期、存储空间等及时进行提醒；
* 建立相关系统软件各种故障的恢复流程及应急措施；
* 建立每台维保设备的台账，如实记录包括计算机名称、品牌、配置参数、网络地址、操作系统，端口等信息；服务器、网络设备的拓扑结构。并根据设备的增加、替换、废弃及时更新档案，每月提交一次。
* 建立单位内应用软件台账（包含所用服务器、网络、依赖服务、名称、版本、系统环境、厂家、负责人等信息），并根据变化及时更新资料，每月提交一次。

**⑥终端维护服务**

* 安装操作系统、业务软件及常用工具软件

在院方的指导下为办公终端安装操作系统、业务软件和常用的办公工具软件及其它院方工作需要制定的软件。

* 终端系统故障解决

解决用户办公终端的系统故障。

* 终端应用故障解决

解决用户办公终端的应用软件故障。(如经甲方确认为第三方问题，有权拒绝再次处理)

* 终端硬件故障判断

判断用户办公终端的硬件故障点，提出解决方案，如果需要更换故障设备，更换过程由中标方全程处理，全程送修、送回。

* 终端系统安全

勒索病毒补丁、禁用U盘、部署杀毒软件，确保系统安全。

##### （2）日常巡检服务

* 驻场人员每天对院方相关IT设备提供一次现场巡检，对采购人维保对象全面检查。检查的内容包括软、硬件运行状态和设备运行环境的检查等。
* 在重要保障期间,系统升级、扩容、投产、年终结算等重要时点之前，中标人应按照院方要求对关键设备和系统进行针对性重点巡检。
* 中标人完成现场巡检后需填写设备巡检记录表。
* 中标人需为院方建立设备维修档案，并根据运行情况向院方提供设备升级、改造、更换的建议和方案。在设备巡检过程中中标人需根据院方需要对院方工程师进行现场培训。
* 中标人每月须提交一次巡检报告，并与院方沟通报告内容中需要紧急处理的问题。院方可以根据需要要求中标人增加或修改设备巡检内容。

##### （3）服务报修和管理

* 多渠道报修：系统由服务端、管理端、报修端三端组成，报修人员可以通过微信、电话、WEB等多种渠道报修；服务人员支持微信、WEB处理报修工单.
* 派单模式：系统支持3种派单模式：手工派单、智能派单、延时智能派单；
* 智能派单：系统可根据运维项类型以及工程师繁忙程度，代替管理员进行自动派单（投标文件中提供截图证明并加盖原厂公章）；
* 延时智能派单：管理员优先手工派单，当超过一定时限后，系统代替管理员进行智能派单，自动分派工程师，并支持设置延时智能派单时间（投标文件中提供截图证明并加盖原厂公章）；
* 报修进度查询：支持报修人通过微信随时查看工单进度，派单，处理，完成，每个工作节点系统都会自动给报修人发送消息，让报修人清楚地知道工作进展；
* 增援:支持服务人员发起增援，增援请求被接受后，多人可共同处理一个工单。
* 转派：支持将已受理的工单派给其他服务人员
* 支持工单挂起和解除挂起，工单挂起后，停止计算服务人员工时。挂起解除后，工单将继续计算服务人员工时。
* 工单录入方式：支持系统录入和人工补录两种方式，并可按照工单录入方式筛选工单。（投标文件中提供截图证明并加盖原厂公章）；
* 统计分析：支持完成工单数量、效率、平均满意度、运维项统计、申报用户等统计维度；
* 工单综合报表：报表支持查询、筛选、导出，工单综合报表展示的字段包含但不限于：申报用户、申报组织、工单录入方式、工单耗时、工单状态、运维项、满意度（投标文件中提供截图证明并加盖原厂公章）；
* 日常任务管理：通过任务推送帮助运维人员合理的安排各种任务表单，支持日推送、周推送、月推送，任务表单模板支持可配置（投标文件中提供截图证明并加盖原厂公章）；
* 工单操作：支持接单、转派、挂起、恢复等工单操作；
* 提供数字化项目管理功能，包括项目看板、项目进度、项目交付物管理、任务管理、项目沟通留痕等，支持微信端使用。
* 接听电话不能准确判断故障的，请及时到现场处理；如果判断为第三方故障且不能处理的请做好登记与移交登记。
* 接听或现场处理报修时，能够基本判断常见问题的故障点，并能够进行任务指派或转交。

##### （4）重要时刻保障服务

* 重要时期保障期间，院方根据需要向中标人提出重要时期保障服务请求，中标人收到请求后与院方共同制定重要时期保障期间的设备保障方案。
* 重要时期保障期间包括院方重要业务系统上线、系统切换、数据迁移、重要设备搬迁等。在重要时期保障期间，中标人需在原有驻场人员之外根据需要安排技术支持工程师团队到现场巡检及完成技术保障服务。在合同执行时院方根据需要向中标人提出此类服务的日期和时间，中标人必须无条件服从。

##### （5）应急预案服务

* 中标人应与院方一起制定一套紧急情况处理流程并为院方提供紧急情况处理服务。由中标人负责工程师，技术支持专家小组，与院方共同配合，制定切实可行的紧急状况处理流程，并在可能的情况下进行实际演练，以保障突发故障状态下的有效应对处理和取得故障原因分析所需的数据。
* 在出现紧急故障或问题的情况下，院方与中标人应依照对应应急处理流程，积极配合，在最短的时间内解决问题。
* 应急处理服务完成后，中标人应及时向院方提供紧急情况应急处理服务报告。

##### （6）培训服务内容

* 常规培训：根据医院现有的系统，将制定培训计划，并分系统分时间进行培训，也可以结合用户感兴趣的内容，做相关培训的调整。
* 应急培训：针对院方经常出现的故障点做针对性的培训，使院方自己的维护人员能够处理常见的相关故障，提高用户的日常维护和应急能力。

##### （7）优化整改服务

* 根据驻场人员现场收集的和巡检的情况，提供优化整改服务报告，报告中应详细记录设备运行状况和相关解决办法或建议。同时，每半年还应提供深入的系统分析，并提供优化建议方案。

##### （8）服务报告

* 中标人在每个事件（每次服务）处理之后给院方提供《事件问题处理报告》，每季度结束后的5个工作日内，向院方提供《季度服务总结》及《季度服务清单》，以便院方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:
* 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，评估每次维保行动的效果；统计评估维保行动实施了的服务包的内容；总结分析遗留问题处理情况；
* 一级故障分析报告: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、杀毒趋势分析；
* 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；
* 问题分析:对维保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。

（9）其他

* 中标方可使用采购人的现有各类管理软件，也可以在用户允许的情况下使用第三方软硬件进行管理，所有额外支出费用由中标方自行承担。
* 投标人必须在标书中以独立形式明确承诺：一旦中标，在服务过程中使用的第三方软件应具有合法的使用许可，没有相关法律纠纷，否则，导致损失由中标人承担。
* **合同期内新增的硬件设备等纳入该维保范围内，合同期内托管的社区医院纳入上述维保范围**
* **三级医院、等保测评、互联互通、电子病历评级、智慧医院等测评工作全程支持工作**

#### 2、IT基础设备维护服务

投标人须针对采购人以下设备提供一年维保服务，维保为硬件全包方式，即维护、维修中的所有故障硬件及易损耗材均由中标人免费提供和更换。

说明：

1、出厂时间超过六年的设备，因备件短缺等客观因素导致无法维修，由乙方提供评估报告，甲方决定是否做报废处理。

2、只负责IT硬件维保，合同服务期内，软件持续使用若需缴纳费用，由甲方与厂商协商购买；

设备清单（详细清单见附件）

**安徽中医药大学第一附属医院自有设备**

|  |  |  |  |
| --- | --- | --- | --- |
| 设备类别 | 在保 | 过保 | 总计 |
| 路由器 | 2 | 1 | 3 |
| 存储 | 3 | 5 | 8 |
| 服务器 | 9 | 31 | 40 |
| 安全设备 | 5 | 15 | 20 |
| 交换机 | 11 | 176 | 187 |
| SAN交换机 | 1 | 4 | 5 |
| 总计 | 31 | 232 | 263 |

|  |
| --- |
| 中医馆设备 |
| 设备类别 | 在保 | 过保 | 总计 |
| 路由器 | 0 | 2 | 2 |
| 存储 | 0 | 2 | 2 |
| 服务器 | 0 | 18 | 18 |
| 安全设备 | 0 | 15 | 15 |
| 交换机 | 0 | 8 | 8 |
| SAN交换机 | 0 | 2 | 2 |
| 总计 | 0 | 47 | 47 |

#### 3、IT基础设备升级扩容服务

| **序号** | **名 称** | **主要技术参数** | **数量单位** |
| --- | --- | --- | --- |
| 1 | CDP扩容 | 1、原有EMC设备扩容1T容量；**★**2、提供原厂商针对本项目的服务承诺函原件；**★**3、提供原厂商工程师进行安装调试，需提供原厂商出具的服务证明函； | 1项 |

#### 4、安全巡检服务

| **序号** | **名 称** | **主要技术参数** | **数量单位** |
| --- | --- | --- | --- |
| 1 | 安全巡检服务 | **★**1、每季度提供专业安全厂商的安全巡检服务；需提供厂商出具针对本项目的服务函原件；**★**2、所选安全厂商需与现有防毒墙，以及终端的防毒产品兼容和联动；需提供厂商的出具承诺函原件；3、服务所需工具由服务商提供；4、服务内容如下：1）、网络系统、安全系统专家级运维，针对医保、农合网络极端故障、疑难问题的处理；针对安全系统的安全分析、安全策略、主动防御配置及安全排查等。2）、对数据中心的网络数据流量进行监测监控，对异常流量、攻击行为或未知威胁进行识别，分析，判断和处置，提供阶段性安全报告；3）、可以根据需要对无法联网或封闭操作系统的信息设备或医疗设备（如CT机、自助机等）进行离线杀毒；4）、对终端的数据传输流量进行监测，对异常流量、攻击行为或未知威胁进行识别，分析，判断和处置，提供阶段性安全报告；5）、每半年对网络存在的弊端、风险，提出优化与应对的策略和改进方案。 | 1项 |

#### 未知威胁检测服务

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **主要技术参数** | **数量单位** |
| 1 | 未知威胁检测服务 | 1、未知新型网络攻击监测探针监测到的威胁信息，可以在运维服务平台上自动生成的相应级别事件工单，由值守中心工程师按SLA约定的时间内响应及启动运维事件流程；**★**2、支持Office、PDF、HTML、JS、EXE、CHM、SWF、可执行脚本文件、媒体文件、LNK文件、压缩文件、图片文件等40+类型文件还原及检测（投标文件中提供截图证明并加盖原厂公章）；3、支持识别超过100多种应用程序协议，可识别主流的文件传输协议如HTTP、 SMTP、POP3、IMAP、FTP、SMB等，从而确保识别通过这些协议传输的恶意文件；4、沙箱镜像具备风险安全评估技术分析:包含针对操作系统注册表、内存、程序、网络活动、文件系统等变化进行记录与分析；**★**5、运维服务平台采用AI分析使用多种AI算法，对异常事件进行AI分析，确定异常范围，异常时间，预测异常概率（投标文件中提供截图证明并加盖原厂公章）；6、支持扩展的定制化沙箱可侦测到大规模文件篡改、文件加密、存储备份篡改等勒索软件触发的异常行为；7、未知新型网络攻击监测探针本身支持外部抓取的流量包导入进行离线分析。 | 1项 |

### 二、招标清单

|  |  |  |
| --- | --- | --- |
| 序号 | **服务内容** | **数量** |
| 1 | IT驻场服务 | 1项 |
| 2 | IT基础设备维护服务 | 1套 |
| 3 | IT基础设备升级扩容服务 | 1项 |
| 4 | 安全巡检服务 | 1项 |
| 5 | 未知威胁检测服务 | 1项 |

### 评 分 办 法

|  |
| --- |
| **分值构成（总分100分）** |
| **项目** | **分值** | **评 分 办 法** |
| 投标报价（30分） | 价格分统一采用低价优先法，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：投标报价得分＝（评标基准价/投标报价）×30％×100 |
| 投标人企业资信和案例（16分） | 投标人企业资信 | 4 | 1、投标人具有ISO/IEC 27001、ISO/IEC 20000认证证书的，全部提供得2分，本项最高得2分，不提供或提供不全不得分；2、投标人具有由中国网络安全审查技术与认证中心颁发的信息系统安全集成服务资质证书，得2分；**备注：投标文件须提供证书扫描件或复印件，并加盖投标人公章，否则不得分。(原件备查)** |
| 投标人案例 | 10 | 投标人具有2017年3月1日以来医疗行业信息化“运维服务”项目案例的1、合同金额100万及以上的，每增加一个得4分；2、合同金额在50万（含）至100万之间的，每增加一个得2分；3、合同金额小于50万的，每增加一个得1分；**备注：****1、本项最高得分为10分；****2、同一业主单位的若有多个符合要求的合同，可累计得分；****3、投标时提供中合同复印件，并加盖投标人公章，否则不得分。(原件备查)****4、投标人需要提供业务单位固定电话，招标人有权对中标人提供的案例进行复核，若发现弄虚作假，直接做废标处理。****5、投标人须在投标文件中提供内容完整的合同复印件作为打分依据，不得遮挡、缺页，否则视为无效业绩合同。** |
| 投标人优秀案例 | 2 | 投标人在上述案例中获得业主单位的表扬信或问卷调查为满意的（原件盖业主单位公章），得2分。**备注：****1、投标时提供复印件，并加盖投标人公章，否则不得分。(原件备查)****2、投标人需要提供业务单位固定电话，招标人有权对中标人提供的案例进行复核，若发现弄虚作假，直接做废标处理。** |
| 技术部分（30分） | 技术指标响应程度 | 25 | 根据投标文件对招标文件要求指标的响应程度评分：加★号的指标，每有一项不满足扣3分，其他指标每一条不满足扣2分；扣完为止； |
| 服务方案 | 5 | 投标人应根据招标人实际情况，结合招标文件要求，写出详细服务实施方案，方案应包含但不限于以下内容：1)方案应编制完整、格式规范、内容齐全、表述准确、条理清晰，内容无前后矛盾，1分；2)方案应符合招标文件相关要求，1分；3)方案中应结合实际情况对服务内容有详实、符合现场实际要求的维护方案，2分；4)方案中应有驻点人员的明确、可操作性的考核办法，1分； |
| 服务能力（24分） | 驻场人员服务能力 | 8 | 驻场人数5人，详情见技术要求一、**网络系统及安全系统维护驻场工程师（4分）**提供1名网络系统及安全系统维护驻场工程师具有以下证书专业人员得分，投标文件中须列出人员名称及相关证书复印件或截图（证书必须是同一个人，每得一个证书得一分）：1、获得过招标人核心安全厂商认证证书的，得1分；2、获得过招标人核心网络厂商认证证书的，得1分；3、具有工业和信息化部颁发的网络工程师认证证书的，得1分；4、具有工业和信息化部颁发的信息系统项目管理师的，得1分；**二、数据中心维护驻场工程师（4分）**提供1名数据中心维护驻场工程师具有以下证书专业人员得分，投标文件中须列出人员名称及相关证书复印件或截图（证书必须是同一个人，每得一个证书得一分）：1、获得过招标人核心网络厂商认证证书的的，得1分；2、获得过招标人核心存储厂商认证证书的，得1分；3、获得过招标人所使用的虚拟化产品厂商认证证书的，得1分；4、具有工业和信息化部颁发的信息系统项目管理师的，得1分；三、驻场负责人（4分）驻场5名工程师中有1人需承担驻场负责人角色，该负责人具有以下证书或证明文件得分，投标文件中须列出人员名称及相关证书或证明文件的复印件或截图：1、个人获得过甲方的服务类荣誉证书的（盖甲方公章），得2分；中标公示期间，需对相关信息进行公示；2、担任过三甲医院驻场服务负责人的，得2分。提供所服务的三甲医院名称和信息科负责人的联系方式。中标公示期间，需对相关信息进行公示。**注：****1、投标时提供以上证书复印件或官网截图证明并加盖投标人公章，否则不得分；****2、投标时提供证书拥有者最少六个月社保证明并加盖投标人公章，否则不得分；****3、网络系统及安全系统维护驻场工程师和数据中心维护驻场工程师，不可兼任；****4、如驻场人员替换须保证替换人员具有同等资质，否则视为违约；****5、投标人需提供证书查询网址和证书号，或现场提供证书原件备查；若发现弄虚作假，直接做废标处理。****6、项目经理如不满足院方要求，中标人需要无条件更换，更换两次仍不满足要求的，予以废除合同处理，全部损失由中标人承担** |
| 投标人技术团队服务能力 | 12 | **一、技术类：（9分）**1、投标人技术团队中具有ORACLE OCP工程师认证证书的，得1.5分；2、投标人技术团队中具有Vmware的工程师认证证书的，得1.5分；3、投标人技术团队中具有IE网络工程师认证证书的（HCIE、H3CIE、CCIE均可），得1.5分；4、投标人技术团队中具有EMC厂商认证工程师证书的，得1.5分；5、投标人技术团队中具有趋势厂商认证工程师证书的，得1.5分；6、投标人技术团队中具有宏杉存储厂商认证的高级技术工程师证书（MSSE）的，得1.5分；**二、管理类：（3分）**1、投标人技术团队中具有中国电子技术标准化研究院颁发的IT服务项目经理证书（ITSS）的，得1.5分；2、投标人技术团队中具有中国网络安全审查技术与认证中心颁发的信息安全保障人员认证证书（安全集成方向）的，得1.5分；**注：****1、投标时提供以上证书复印件或官网截图证明并加盖投标人公章，否则不得分；****2、投标时提供证书拥有者至少六个月社保证明并加盖投标人公章，否则不得分；****3、投标人需提供证书查询网址和证书号，或现场提供证书原件备查；若发现弄虚作假，直接做废标处理。** |