**项目需求**

**一、采购标的清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 采购包 | 序号 | 采购标的 | 对应中小企业划分标准所属行业 |
|  | 1 | 中心机房设备维保项目 | 软件和信息技术服务业 |

**二、技术要求**

2.1、项目概况及总体要求

我院于中心机房的部分设备，主要包括服务器、存储、超融合软件平台、防火墙、深度检测模块、内外网数据交换系统、堡垒机、负载均衡、态势感知、准入系统、桌面管理系统、核心交换机、接入交换机等总共174套设备，今年8月底即将到期。

这些设备上在运行的系统均为医院核心业务，为了更好的保证各系统及数据中心的安全稳定运行，现计划采购维保服务。

2.2、维保清单一览表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌型号 | 数量 | 单位 | 购买时间 |
| 1.
 | 超融合物理服务器 | 浪潮 NF5270M4 | 3 | 台 | 2018年 |
|  | 超融合软件平台 | 深信服aCloud 5.0 CPU\*6 | 1 | 套 | 2018年 |
|  | 万兆交换机 | H3C S6520X-30QC-E | 2 | 台 | 2018年 |
|  | 内网边界防火墙 | 深信服AF-1000-F440 | 2 | 台 | 2019年 |
|  | 内网数据中心防火墙 | 天融信.NGFW400 | 2 | 台 | 2019年 |
|  | 内外网数据交换系统 | 联软.UNXG-2050 | 1 | 套 | 2019年 |
|  | 深度检测模块 | 亚信Deep Security DPI深度包检测模块176件 | 1 | 套 | 2019年 |
|  | 外网日志审计系统 | 天融信.TopAudit  | 1 | 套 | 2019年 |
|  | 外网堡垒机 | 齐治. SHTERM-HQ5-X | 1 | 台 | 2019年 |
|  | 外网终端准入设备 | 盈高.ASM6305 | 1 | 台 | 2019年 |
|  | 外网VPN 设备 | 深信服. VPN-1000 | 1 | 台 | 2019年 |
|  | 外网负载均衡设备 | 深信服 AD-1000 | 1 | 台 | 2019年 |
|  | 威胁感知系统 | 360天眼威胁感知系统 | 1 | 套 | 2019年 |
|  | 数据库服务器 | ThinkSystem SR860 | 2 | 台 | 2019年 |
|  | 核心存储系统 | DELL-EMC Unity450F | 1 | 套 | 2019年 |
|  | 存储虚拟化系统 | DELL-EMC VPLEX VS6 | 1 | 套 | 2019年 |
|  | SAN光纤交换机 | DELL-EMC 6505 | 2 | 套 | 2019年 |
|  | 核心交换机1 | H3C S7506E-V | 2 | 台 | 2018年 |
|  | 核心交换机2 | H3C S7503E-M | 2 | 台 | 2018年 |
|  | 汇聚交换机 | H3C S5560X-30F-EI | 8 | 台 | 2018年 |
|  | 接入交换机1 | H3C S5130S-52P-EI | 28 | 台 | 2018年 |
|  | 接入交换机2 | H3 S5130S-28P-EI | 76 | 台 | 2018年 |
|  | 网络监控管理设备 | H3CiMC-智能管理平台 | 1 | 台 | 2018年 |
|  | 数据库维护保障 | DSG维护 | 1 | 批 | 2018年 |
|  | 云存储 | DellEMC Isilon X210 | 3 | 台 | 2018年 |
|  | 服务器 | IBM 3850X5 | 4 | 台 | 2013年 |
|  | 刀片刀箱 | IBM eServer  | 2 | 台 | 2013年 |
|  | 刀片服务器 | IBM HX5 | 12 | 台 | 2016年 |
|  | 磁盘阵列 | EMC VNX5500 | 2 | 台 | 2013年 |
|  | 存储虚拟化设备 | EMC VPLEX VS2 | 1 | 台 | 2013年 |
|  | 光纤交换机 | 思科 MDS-9148-16 | 2 | 台 | 2013年 |
|  | 千兆交换机模块 | IBM BladeCenter  | 4 | 台 | 2016年 |
|  | 存储扩展柜 | EMC VNX5500扩展柜 | 2 | 台 | 2016年 |

2.3、★设备维保要求

（1）本项目服务期限为：自合同签订之日起3年。若本次项目合同签订时间晚于该设备目前维保到期时间，则该设备续保时间为本次项目合同签订之日起三年。（脱保期费用由应标方负责）。

（2）服务清单1至24项为“原厂质保”的设备，投标时投标方须提供书面承诺，承诺中标并获取中标通知书后5个工作日内，提供相关设备制造商出具的带有本项目名称和本项目对应设备的《服务厂商授权函》(加盖制造商公章)。否则采购人不予签订合同并追究中标单位相关责任。

（3）服务清单25项的EMC设备，需提供原厂授权的第三方服务。投标时投标方须提供书面承诺，承诺中标并获取中标通知书后5个工作日内，提供第三方服务提供商出具的带有本项目名称和本项目对应设备的《服务厂商授权函》（第三方服务提供商具备EMC的ASN(Authorized Service Network)、ASP（Authorized Service Provider）授权，中标后该EMC授权也应一并提供）。否则采购人不予签订合同并追究中标单位相关责任。

（4）服务清单26至33项的安全设备，投标时投标人须提供书面承诺，承诺免费更换相关维保设备的故障硬件（使用原厂配件），不再收取任何其他的相关费用，如劳务、交通费等。否则采购人不予签订合同并追究中标单位相关责任。

2.4、维保服务技术要求

|  |  |  |
| --- | --- | --- |
| 序号 | 服务项目 | 服务要求 |
| 1 | 服务团队及驻场要求 | ★要求维保服务提供不少于10人的专业服务团队，其中专职工程师1人。服务团队必须是中标供应商公司人员，供应商在投标时只提供资格承诺函的，中标后在签订合同前必须提供距开标时间三个月内任意一个月供应商为其缴纳社保的证明。专职工程师需精通网络技术、虚拟化技术、存储技术等，需要有同等级数据中心运维经验，且要求在故障报修后10分钟内到达现场处理。专职工程师服务方式为电话7\*24小时服务；并且在采购人开展重要技术维护升级工作期间，专职工程师以驻场方式为按采购人需要提供驻场支撑。驻场人员需与采购人签订保密协议，听从用户相关负责人安排并完成运维管理系统相关的工作。为保证服务质量，不经招标人允许，投标人中标后在服务期内不得擅自更换专职工程师。 |
| 2 | ▲在法定节假日（元旦、春节、五一、十一等）期间、重大活动（由采购人指定并提前告知）前及其举行期间，应根据采购人的具体要求对相关维保设备进行额外的维护巡检，确保设备及系统在此时期的正常工作，必要时应派专业工程师在现场实施驻点保障服务。 |
| 3 | 硬件设备维护要求 | ★响应时间：供应商保证用户方计算机信息系统全年7\*24小时安全、稳定、高效运行。供应商维护范围内任何影响用户方业务的故障，维护人员必须立即响应，10分钟内到达故障现场并排查原因，非硬件故障2小时内恢复，硬件故障24小时内恢复，保证系统能够正常运行。对于影响到医院业务正常运行的各类故障，能提供条件允许的最快响应与技术支持。 |
| 4 | ★要求维保服务单位必须为本项目中所有的设备提供全年7×24小时值守服务，明确到人，晚班值班人员不得无故离岗、脱岗。非硬件故障2小时内恢复，硬件故障24小时内恢复，提供备品备件库支持；其他隐患类故障，恢复时间由供应商与采购人协商决定，原则上不超过3个工作日。在规定处置时间内无法修复故障的，服务供应商提供备品、备机。 |
| 5 | ★投标时投标人须提供书面承诺，承诺中标后提供“设备清单”内所有设备的软、硬件三年 7\*24小时维护服务。 |
| 6 | ▲备件库：中标供应商需根据用户需要，购买相应备品备件并放置采购人机房，以满足用户单位计算机信息系统的维修需要，具体备件数量不少于一下要求：（1）核心交换机-1 1S7506E-V主控制引擎模块1个；（2）核心交换机-1 1S7506E-V 电源1个；（3）核心交换机-2 H3C S7503E-M 交换路由引擎模块1个；（4）备用24口接入交换机H3C S5130S-28P-EI交换机2台；（5）备用48口接入交换机H3C S5130S-52P-EI交换机2台；（6）数据存储设备EMC UNITY 450 AFA SSD 硬盘2块；（7）云存储EMC EMC XC730XD 硬盘硬盘2块； |
| 7 | 巡检要求 | ★每日一次现场常规巡检，每月进行一次系统全面维护，对两机房（主机房及容灾机房）内设备进行预防性维护，每月进行一次弱电间巡检（有信息中心设备的弱电间，无设备的不巡查），排除系统的隐患，解决系统出现的故障。协助采购人进行网络安全建设，日常巡检中包含网络安全设备、网络日志巡检。每次巡检应提供巡检报告，并根据巡检报告，及时与用户进行交流，及时协调解决维护工作中的问题。 |
| 8 | ▲每月巡检要求对主机房及容灾机房的服务器、核心存储、数据库系统、备份系统、网络等进行详细巡检工作，对服务器、存储、网络作全面分析，包括外观检察、日志分析抓取、性能分析抓取、空间使用情况、网络故障排查等，并制作一份详细的巡检报告，并提交与用户。 |
| 9 | ▲每日巡检中包含主机房及容灾机房的相关设备巡检。每次巡检应提供巡检记录，并根据巡检报告，及时与用户进行交流，及时协调解决维护工作中的问题。 |
| 10 | 检查设备前后面板指示灯（电源、硬盘、故障、光纤等）、电源电压、电源风扇、控制器情况、负载均衡、磁盘使用率、IO 状态等。 |
| 11 | 故障处理及架构调整要求 | 在现有设备范围内，中标供应商应对用户方信息系统进行定期的维护管理和配置优化，确保用户方整个信息系统运转的高效、稳定和安全，减少和避免系统性能瓶颈，杜绝信息系统安全事故，并且能根据用户方需要，提供信息系统运行的合理化建议和方案。 |
| 12 | ▲中标供应商应定期检查用户方存储系统的运行状态，确保数据存储安全可靠，确保系统的可恢复性，及时根据用户的数据存储量和数据安全要求问题，调整数据备份策略，保证备份存储介质的可用性和安全性，及时更换存在故障的存储备份设备。 |
| 13 | 应急预案要求 | 制定针对该项目的应急保障预案，方案中应主要包括应急处理保障机制与应对突发事件的解决措施。方案中应急处理保障机制完善，应对突发事件的解决措施。 |
| 14 | 软件维护要求 | ▲软件维护的范围包括但不限于服务内容中相关计算机软件产品，维护期内采购人新增计算机软件产品的运行及升级，采购人服务器虚拟化系统、数据库等软件出现问题，均由供应商负责恢复至故障前状态。 |
| 15 | 根据软件系统的运行情况，提供软件系统性能优化方案，并与用户进行信息交流，及时协调解决维护工作中的问题。 |
| 16 | ▲免费对操作系统、数据库软件、备份软件等系统软件进行版本更新、补丁安装等工作，确保系统稳定高效地安全运行。 |
| 17 | 定期对主机系统进行检查，包括配置设置与系统操作的评估，以及有关系统、磁盘性能、I/O 通信、软件版本、可用性和安全性的信息，及时提供改进方案和纠正措施的详细建议。 |
| 18 | 定期对存储系统检查，包括评估存储系统的配置和版本等级，确定可能影响存储系统性能和可用性的硬件、软件、固件版本以及配置状况；提出改进和优化存储子系统性能、容量与可用性的具体建议从而保护用户的业务。 |
| 19 | 与业务系统软件商深度配合要求 | ▲与软件商配合，完成与本项目相关设备的应用系统硬件设备的维护工作。 |
| 20 | ▲与软件商配合，完成与本项目相关设备的运行的核心数据库的联调及优化工作，确保数据库稳定、高效运行。 |
| 21 | 服务质量要求 | （1）对用户无论通过何种方式提出的技术支持请求，最迟必须在 30 分钟内给予响应；（2）运维工程师在工作中应使用普通话、热情有礼、自然得体、音量适中；（3）对用户做到有问必答，有答必准，灵活应变；（4）工作要耐心细致、不急不燥，不厌其烦；（5）谈话中不得夹带口头语，切忌言语粗鲁。 |
| 22 | 其他服务要求 | 维保公司还需在用户发生需求时，提供不限次数的如下现场原厂商人工服务：提供应用系统上线、变更等必要的存储及备份的现场值守服务；提供各设备用户单位服务期系统实施、变更所需的现场值守服务。具有以上系统的综合系统优化支持能力；服务期内提供与本项目相关的技术咨询服务。 |
| 23 | 重大任务保障要求 | 招标人实施的重大工作，需要运维工程师全程参与和支持。主要工作是按照招标人的总体安排，参与重大工作项目，做好现场值守服务。 |
| 24 | 文档记录要求 | 供应商应建立完整的文档记录，按时向采购人提供装订成册的纸质版与电子版，供应商要建立专门的系统维护台账。供应商工程师第一次到现场巡检时，要做出保修设备的详细配置清单、所使用的操作系统、版本号、系统的使用情况及系统的配置参数。每次巡检为每台保修设备填写巡检表，记录设备的运行情况、出现过的问题和解决的办法、设备的配置变动等情况，并建立科学合理的巡检台账。 |
| 25 | 签订维保合同10天内，供应商提交《系统日常巡检作业指导书》，《系统日常巡检作业指导书》经采购人审核、批准后，由工程师执行日常巡检。 |
| 26 | 签订维保合同10天内，供应商提交《维保设备信息登记表》，记录保修设备的详细配置信息，核对网络结构拓扑图。 |
| 27 | 维保期内应及时维护和更新《维保设备信息登记表》和网络结构拓扑图，包括位置、参数、配置的变更。 |
| 28 | 每个自然月的3日前向采购人提供上月的巡检报告，详细记录巡检日期、巡检人、巡检内容、问题、采取措施及建议等内容，双方签字确认；巡检成果应详细列明被巡检设备当前软件版本（系统软件、特征库、病毒库等），制定合理、科学的升级加固方案并付诸实施。 |
| 29 | 故障抢修后的1个工作日内向采购人提交《故障检修报告》，每个自然月的30日前向采购人提供当月的抢修统计记录，其中至少记录接报修时间、报修人、到达现场时间、修复时间、故障原因、故障现象、抢修过程等。 |
| 30 | 维保期每半天提供一次半年维保服务总结报告，维保服务合同到期后的3天内，提供维保服务总结报告。 |
| 31 | 保密要求 | 运维人员在工作现场未经采购人工作人员允许，不得接触涉密信息和敏感信息；不得私自进入服务器等设施设备存放场所。在工作过程中因需要，确需接触涉密信息或敏感信息和进入上述场所的，应在取得采购人管理人员同意后进行操作。 |
| 32 | 运维人员在工作过程中，不得以任何形式私自外传、记录、下载和存储本系统中的任何信息和数据；不得使用未经采购人许可的计算机和存储设备对上述信息和数据进行运行和操作。 |
| 33 | 运维人员未经采购人管理人员许可，不得将本系统中的任何信息和数据以任何形式在任何网络和媒体上发布和传播。 |
| 34 | 运维工作人员因工作失当违反本要求的，未造成严重后果或用户方信息泄密的，经用户方批评教育后，按罚则条款相关规定进行处罚；运维工作人员三次及以上违反本要求或者造成用户信息系统破坏和数据泄密等严重后果的，采购人将即时终止合同更改维护单位，并依据《中华人民共和国网络安全法》及其实施办法严格追究相关责任人的法律责任。中标供应商须加强运维人员的保密培训，进场开展运维服务前须与采购人签署保密协议。 |
| 35 | 网络运维能力要求 | 投标人需要具备针对中心机房相关设备的整体网络运维服务能力。主要能力要求如下：（1）▲具备设备监管能力，提供多种类型的设备接入纳管，包括操作系统、服务器硬件、网络设备、存储设备、安全设备的接入纳管，以及采集到设备的实时数据和历史数据，提供此项功能截图证明。（2）▲为便于项目后期运维管理，网络运维支持运维流程派单，可进行告警自动派单以及人工派单，有效支持事件管理、问题管理、变更管理、发布管理、400报障等运维流程工单，工单流传可上传附件、点评、工单流程可视化，提供此项功能截图证明。（3）▲自动生成运维报告，支持自动化导出运维服务报告，包括业务总体健康概览、平台容量分析、设备运行指标分析、业务自动拨测分析、工单闭环管控分析、告警统计、告警分析等数据，提供此项功能截图证明。 |

2.5数据库服务要求

|  |  |  |
| --- | --- | --- |
| 序号 | 服务项目 | 服务要求 |
| 1 | 数据库维护服务 | 本次数据库系统的维保范围是整体打包,包含并不限于HIS、电子病历、LIS、病理、体检、PACS、RIS、输血、OPACS、营养食堂、急症、重症、移动护理、手麻、平台、SPD等数据库系统。 |
| 数据库系统健康检查，出具相关报告:（1）检查数据库运行状态。（2） 检查数据库空间的使用情况,协助数据库空间的规划管理。 （3）检查分析系统日志及跟踪文件，发现并排除数据库系统错误隐患，并给出书面报告。（4）检查数据库备份的完整性（5）检查数据库运行效率、是否存在安全隐患、备份方式是否合理、备份数据是否可恢复。（6）根据数据库运行情况建议是否需要oracle,mysql 新的补丁，并负责补丁的安装。（7）检查系统存储空间的增长情况，提供对存储空间增长需求的预估。  |
| 协助工作人员监控空间异常快速增长。并对每一季度的空间增长提供书面报告。评估数据库运行性能，提供系统性能调整并对可能的潜在问题提出警告。检查数据库安全及用户管理，排除可能的数据库安全隐患。 |
| 数据库安装、版本升级；数据库系统性能调优，参数优化，碎片整理，数据库运行状况巡检；巡检工作结束后，提交用户《系统巡检报告》，对错误进行分析，提出解决方案及预防措施。 |
| 例行维保每季度进行一次，出具相关检测报告；每季度进行一次数据恢复验证，出具相关验证报告（lis、pacs等国五要求） |
| 数据库基础运维和管理培训；如有大型检查、评审，需要工程师到现场协助配合 |
| 此次数据库维保包括但不限于医院所有生产及灾备数据库的维护工作，投标人需要配合医院进行定期灾备系统应急演练等非故障性事务的处理以及日常灾备数据库的维护工作。投标人须提供医院现容灾软件工程师认证证书。 |
| 2 | 数据库迁移服务 | 配合医院进行系统间数据迁移工作，包括且不限于：windows到linux，linux到linux，sqlserver到Oracle，Oracle到Oracle，Oracle到其他信创数据库，要求提供在线数据迁移及迁移保障服务。 |
| ★本次需提供专业数据迁移软件来完成本次数据迁移服务，能够实现核心业务系统数据库数据迁移要求，须提供软件著作权证书及数据迁移软件正版许可证明文件。 |
| 提供服务所用数据迁移软件需支持基于数据库在线重做日志的分析复制，支持以逻辑复制的方式将源端数据复制到目标端，并支持在目标端实现复制数据的自动加载； |
| 数据迁移增量数据实时同步效率每小时不低于200GB/小时（提供迁移服务所用软件此项功能官网截图证明）； |
| 为保障生产安全，提供服务所用数据迁移软件部署不得干预源端生产业务，禁止对源端数据库及操作系统做任何的参数修改，禁止重启服务器； |
| ▲提供服务所用数据迁移软件必须尽可能少的占用系统资源，CPU占用不大于5%，内存占用不大于1G（提供此项功能官网截图证明）； |
| 提供服务所用迁移软件支持中间机部署模式，无需在生产数据库服务器上安装代理程序（提供此项功能官网截图）； |
| 在数据迁移初始化过程中，业务不能停止；在异构平台或跨数据库版本之间的数据初始化过程中不需要人工干预； |
| 支持任意硬件平台异构实时同步复制迁移，此次需要支持windows操作系统到linux操作系统的数据同步迁移（提供此项功能性截图证明文件）； |
| 支持异构数据库之间的数据实时同步迁移，包括并不限于Oracle、DB2、sybase、mysql、SQLServer、Informix、Gbase、达梦、浪潮K-DB、PostgreSQL、antdb、万里开源、人大金仓、南大通用、OceanBase、TDSQL、Goldendb、GaussDB等； |
| 针对不同数据库的部分非法数据，自动按照目标端规范调整适配（提供此项功能性截图证明文件）； |
| 支持不同大数据组件（HDFS/HBASE/HIVE/KAFKA/ES等)、大数据平台(CDH/华为/星环等）的异构数据同步迁移 |
| ★提供服务所用数据迁移软件在迁移sqlserver数据库过程中，目标数据库须始终处于可用状态，数据同步过程中，支持关闭CDC代理作业，避免对生产库性能造成影响（提供sqlserver数据库此条截图证明文件，须明确标示出sqlserver数据库版本及功能关键点）。 |
| ▲软件支持源端SQL server到Oracle异构数据库环境下的数据实时复制迁移（两端延时在5秒以内），且目标端Oracle数据库可实时查询，当生产端插入（Insert/ Update/delete）一千条数据后，目标端Oracle数据库无需启动，始终处于实时打开验证状态，并通过数据库select语句在5秒以内，查询到该一千条数据变化。提供此项功能截图，截图内容为真实环境或者自己搭建模拟环境，源端、目标端IP地址、数据变化轨迹以及软件运行日志需在一个截图展现； |
| 数据一致性比对：提供服务所用数据迁移软件自身自带数据比对平台，支持对迁移数据条数、内容进行对比并展示（提供此项功能性证明文件） |
| ▲提供服务所用数据迁移软件能够将核心生产库数据实时同步到目标数据库，同时记录数据内容/操作类型（插入/删除/更新之前/更新之后）/操作时间，记录某些行数据的操作时间/操作类型/操作之前内容，做到生产库数据被人为恶意篡改的数据回溯、数据保护（提供此项功能性证明文件） |
| ▲为避免提供服务所用数据迁移软件是国外产品封装或者开源产品简单封装而成，避免不必要的安全漏洞风险，软件核心模块的开源代码占比不得超过20%，提供工信部授权检测机构的评估报告 |
| ★投标人需要承诺支持根据用户需求进行功能定制开发，提供承诺函原件。 |
| 4 | 数据库基础架构新建、改造 | 提供新建数据库基础架构服务，建立多套Oracle rac集群，配合应用测试，进行数据库基础架构改造工作 |
| 6 | 其他服务要求 | 在用户业务系统性能低下的时候，协助应用开发商制定业务系统级的优化方案，并对信息系统数据库性能进行系统级调优，提高业务系统运行性能； |
| 配合用户进行定期灾备系统应急演练等非故障性事务的处理； |
| 当系统出现故障时，需立即响应，先远程应急处理，确保系统正常运行，24小时内提出书面故障处理报告或整改建议； |
| 维保系统如果出现故障，不能工作或者部分有问题需要维修，需要到现场处理时，在任何时间派技术人员4小时内抵达现场，检测问题，确保业务系统运行，24小时内提出书面故障处理报告或整改建议； |
| 在接到现场人员无法及时解决的故障处理报告后，应及时调集相关技术力量予以解决，确保系统正常运行，响应时间小于30分钟；遇到4小时内仍无法解决的系统故障，供应商须提出应急处理方案，保证系统稳定性和整体安全；在故障处理结束后24小时内应向招标单位提出书面故障处理报告，内容应包含故障设备、故障详情、处理结果等，应有维修工程师、使用科室负责人签字； |

**五、方案要求**

投标人在充分理解本项目的需求的基础上，应制定完善齐套的运维方案，主要包括日常维保方案、安全设备整改服务方案、应急响应方案，对相关工作的内容、流程、方法、要求等进行明确，更好地指导日常运维和各项拓展服务实践。

5.1、维护管理服务总体要求

针对本次维保范围内的设备提供三年技术维护服务。

5.2、网络设备、安全设备及服务器运维要求

仔细梳理院内各医疗业务系统对网络安全的需求，按需配置安全隔离与信交换系统、安全运维审计系统、准入系统，定期检查各个安全系统的防护机制；

5.3、日常维保方案要求

要求投标人提供的服务器、存储、安全设备、交换机等设备软、硬件维保服务的内容及详细方案的安全性、合理性、科学性等情况。

要求投标人提供的日常维保方案方案，包括但不限于：

（1）定期检查和测试，确保维保设备的正常运行；

（2）预防性维护，包括所需的工具和材料、检查的具体内容及预期效果；

（3）维保记录管理，对设备的维修历史进行记录，为后续的维保工作提供参考等。

5.4、数据库服务方案要求

要求投标人提供的数据库服务方案，包括但不限于：

（1）数据库服务内容包括但不限于：数据库健康检查、数据库性能评估、数据库优化、数据库升级等相关工作。

（2）数据库迁移服务内容包括但不限于：数据库迁移工具、数据库同步、策略调整等相关工作，确保数据迁移过程中数据安全和系统的正常运行。

（3）其他服务内容包括但限于:数据库基础架构改造工作、定期灾备系统应急演练等相关工作。

5.5、应急响应方案要求

要求投标人提供应急方案，主要明确问题类别、响应时限、力量配置、程序方法、具体措施、安全保障等内容。

要求投标人提供的应急响应方案，包括但不限于：

（1）制定明确的应急响应计划和策略‌：应急响应计划应包含明确的应急响应目标和责任分工，确定事件分类分级标准并建立相应的应急预案库；

（2）‌‌组织指挥体系‌：明确维护指挥体系，包括各级技术人员的职责和权限，确保在突发事件发生时能够迅速、准确地启动应急响应机制‌。

5.6、培训要求

现场培训：中标供应商为采购方提供操作维护培训，直至其能熟练独立操作设备及日常维护与保养，设备及业务系统简单故障诊断与排除。

5.7、其他要求

配合目前院内各业务系统厂商，完成配置、优化、诊断、资源优化及解决各类应用平台涉及的硬件支撑平台问题；

对机房调研，包括机柜、设备分布情况进行统计，所有网络设备、安全设备、服务器设备，存储进行统计分类，机房现网中服务器端口连接情况、网络设备的端口链接情况进行统计。

5.9、保密责任要求

中标供应商在本次招标及服务履行期间了解到的采购单位信息，包括但不限于标书中提供的采购单位设备信息及维保信息等内容，未经采购方书面同意，不得泄露于第三者。服务期满或终止后亦同。

**六、履约能力**

6.1、企业基本要求

（1）投标人具有ISO9001质量管理体系认证证书、ISO20000信息技术服务管理体系认证证书、信息安全服务资质认证证书

（2）投标人应具有5个自2022年7月1日以来（以合同签订日期为准）与本项目类似业绩（至少包含网络设备、安全设备、服务器存储设备运维方面）。

6.2、人员基本要求

投标人应具不少于10人的专业服务团队，其中专职工程师1人（驻场）。

项目经理应具备有效的电子信息工程师证书（高级）、信息系统项目管理师证书（高级）、信创规划管理师证书（高级）。

项目实施团队专职工程师应具备有效的信息系统项目管理师证书（高级）、系统分析师证书（高级）、网络工程师证书。

项目运维团队成员（除项目经理、专职工程师外）应具备有效的高级网络信息安全工程师、国产化操作系统运维证书（如麒麟、欧拉、统信等操作系统）、人社部门颁发的网络规划设计师证书（高级）、信息安全管理(高级)证书；