采购需求

**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 | 安全及网络设备维保项目 | 软件和信息技术服务业 |

**项目属性：服务类。**

**二、技术要求**

2.1、项目概况及总体要求

医院部分安全设备与网络设备维保项目即将到期。这批安全设备与网络设备是保障医疗体系稳定运行的核心环节。安全设备和网络设备是医疗信息化的基础，规范的维保能减少系统宕机风险，确保诊疗服务连续性。此外，由于这批设备已经使用6年以上，专业的预防性维护可延长设备寿命，降低突发故障产生的高额维修成本。为确保医院计算机网络、系统、数据中心的持久、稳定、高效、安全地运行，现计划采购相关维保服务。

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，从而能有效的进行系统运维管理，及时预防系统故障、发现系统故障并排除故障。

2.2、维保清单一览表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌型号 | 单位 | 数量 |
|  | 防火墙 | 天融信NGFW4000-UF NG-51228 | 台 | 2 |
|  | Web应用防火墙 | 天融信TopWAF TWF-61138 | 台 | 1 |
|  | 数据库审计系统 | 天融信TopAudit TA-11314-DB | 台 | 1 |
|  | 虚拟化平台防病毒软件 | 亚信Deep Security | 套 | 1 |
|  | 杀毒软件 | 亚信OfficeScan安全防毒网络版 | 套 | 1 |
|  | 桌面管理系统 | 盈高（MSEP）MSEP2000-ZJ | 台 | 1 |
|  | 图书馆核心交换机 | H3C S12508X-AF | 台 | 2 |
|  | 图书馆汇聚交换机 | H3C S7503E-M | 台 | 2 |
|  | 门诊楼核心交换机 | H3C S10508-V | 台 | 2 |
|  | 门诊楼接入交换机1 | H3C S5130S-28P-EI | 台 | 40 |
|  | 门诊楼接入交换机2 | H3C S5130S-52P-E I | 台 | 10 |
|  | 网络监控管理系统 | H3C IMC/ D5200-G2 | 台 | 1 |
|  | 全闪存储 | EMC UNITY 400 AFA | 台 | 1 |
|  | 虚拟桌面 | 深信服Adesk-STD-200H | 台 | 140 |
|  | 超融合服务器务器 | 深信服VDS-6550 | 台 | 5 |
|  | 数据中心超融合服务器 | DELL EMC XC730XD | 台 | 10 |
|  | 超融合万兆交换机 | DELL S4048 | 台 | 2 |
|  | 日志审计系统 | 思福迪LogBase日志管理和审计系统 | 台 | 1 |
|  | 漏洞扫描 | 绿盟RSAS NX3-X | 台 | 1 |
|  | 流量清洗 | 天融信TopADS 3000 TX-51428 | 台 | 1 |
|  | 内网准入系统 | 盈高 (ASM)ASM6503-ZJ | 台 | 1 |
|  | 上网行为管理 | 深信服AC-1700-H | 台 | 1 |
|  | 备份一体机 | 爱数 VX2400 | 台 | 1 |

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15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16和17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18至23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 |
|  | 服务团队及驻场要求 | *要求维保服务提供不少于8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，且要求在故障保修后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，且要求在故障保修后10分钟内到达现场处理；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，不经甲方允许，投标人中标后在服务期内不得擅自更换专职工程师。* |
|  | 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。 |
|  | 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2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。* |
|  | *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。* |
|  | *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。* |
|  | 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）图书馆核心交换机S12508X-AF 主控制引擎模块1个；  （2）门诊楼汇聚交换机H3C S10508-V 电源1个；  （3）图书馆汇聚交换机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 400 AFA SSD 硬盘2块；  （7）超融合服务器EMC EMC XC730XD ssd硬盘硬盘2块； |
|  | 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。* |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 重大任务保障要求 | 甲方实施的重大工作，需要运维工程师全程参与和支持。主要工作是按照甲方的总体安排，参与重大工作项目，做好现场值守服务。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 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。 |
|  | 服务质量要求（含罚则条款） | 服务响应时间：未在规定时间内响应的或未在规定时间内修复故障按5000元/次扣除合同款。 |
|  | 未按合同要求保质保量完成日常巡检、月度巡检养护工作的，按2000元/次扣除合同款。 |
|  | 未在规定时间内提交日常巡检记录、月度巡检记录、抢修记录、运维总结的，按2000元/次扣除合同款。巡检质量不符合要求，对于网络安全隐患应该发现，却未能发现的，造成网络安全事件，按5000元/次扣除合同款。网络安全事件包括，但不限于公安、网信系统的整改函、通报函、整改通知书等。 |
|  | 服务质量严重不到位的，采购人将对中标供应商处以整改通知书，中标供应商收到整改通知书后应于一周内向采购人提交整改报告。若逾期不提交整改报告或一年之内被二次处以整改通知书的，采购人有权中止合同并采取相应措施保障设备正常运行，期间产生的费用由中标供应商承担。 |
|  | 验收标准要求 | 季度度工作结束后，按照甲方验收的有关制度，组织对服务商项目整体执行情况进行考核。内容包括但不限于以下几个方面：  （1）工程师是否按照甲方要求完成各项服务内容，是否遵守安全管理制度。  （2）投标供应商和运维工程师各项工作是否达到考核管理和处罚的要求。  （3）运维工程师必须按照要求，提交相应文档，并保证文档质量。所有文档必须符合文档管理规范。文档验收以抽样方式进行。  （4）验收时按照各类文档对投标供应商的服务质量进项考评，甲方有权根据服务质量扣除投标供应商相应的运维费用。 |

三、商务要求

3.1、合同款项的支付方式及进度安排

3.2、付款支付时间：在本合同签署后，甲方按服务进度付款，每半年（六个月）对乙方维保服务行为进行考核，考核合格后，在3个月内，向乙方支付本合同总金额的六分之一；如考核不合格，甲方有权扣除当前半年的维保费用，并终止本合同。

四、其他要求

4.1、项目属性:服务类项目。

4.2、本项目不接受进口产品及服务投标。

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. 软件升级、规则库升级、远程技术支持等

（3）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；

（4）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、服务团队及驻场服务要求

要求维保服务提供不少于8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，且要求在故障保修后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，且要求在故障保修后10分钟内到达现场处理；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。

5.5、安全设备整改服务方案要求

要求投标人提供的安全整改服务方案，包括但不限于：

（1）根据采购人要求，在每年等级保护测评及整改、数据安全风险评估及整改、密码应用安全性评估及整改、网络资产识别梳理等工作 时，根据测评情况做好所有网络和安全设备的安全整改。

（2）整改服务内容包括但不限于：网络设备密码的修改、补丁升级、策略调整等相关工作，确保安全整改过程中及整改后网络设备的正常运行。

5.6、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‌。

5.7、咨询服务

针对采购人的现有系统，中标人应对用户信息系统进行月度的维护管理、系统评估及配置优化，确保用户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，并且能根据用户信息化发展需要，提供信息系统运行的合理化建议和方案。

5.8、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。

5.9、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。

5.10、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）投标人应具有质量管理体系认证证书、环境管理体系认证证书、职业健康安全管理体系认证证书、信息安全体系认证， 售后服务认证证书（五星级）资质认证证书。

（2）投标人应具有4个自2022年3月1日以来（以合同签订日期为准）与本项目类似业绩（至少包含网络设备或服务器设备运维方面）**。**

6.2、人员基本要求

投标人应具提供不少于8人的专业服务团队，其中项目经理1人、驻场工程师1人、项目运维团队成员6人。

项目经理应具备有效的信息系统项目管理师、高级工程师、信息系统业务安全服务工程师（高级）证书。

项目运维团队成员（除项目经理）应具备有效的系统分析师证书、网络规划师证书的， 系统集成项目管理工程师、网络工程师、中级工程师（通信工程师/通信专业技术人员职业资格（中级））、数据库系统工程师证书、网络与信息安全管理员证书。