**关于邀请参加项目采购前综合论证的函**

**各相关供应商：**

威海市立第三医院拟对编号LZ2023-25XX的信息网络安全运维服务项目实施采购前综合论证，欢迎相关供应商积极参与。

拟参与供应商务必全面、认真阅读本函所有内容，并严格按本函要求落实参与事宜。未按要求履行程序或者未按要求提供资料的供应商，无法取得参与资格。

**一、论证的时间**

2023年8月31日14:00，当日13:45至13:55签到

**二、论证的地点**

威海市立第三医院三楼西区第二会议室

**三、论证的内容**

一年期医院网络安全运维服务，具体包括附件5《信息网络安全运维服务需求明细》。

项目付款方式为医院收到首次巡检报告后的30日内支付总费用的50%，其余50%于服务期结束后的30日内支付。

**四、论证的报名**

拟参加的供应商应当于 2023年8月29日17:00前派员持公司《营业执照》复印件和附件1《报名信息表》各1份到医院招标办报名。

**五、论证的目的与方式**

通过与供应商进行沟通与谈判，掌握相关产品与服务的质量层次、价格水平、配置方案、保障体系、市场应用等相关信息，为未来实施采购提供标准和依据。

论证参照竞争性蹉商方式，商谈的顺序按照报名的先后顺序反向进行。

供应商不可就本项目的全部或者部分提供超过一种方案要求医院实施选择。

**六、论证现场需要的资料**

**（一）供应商资质**

1.《营业执照》复印件1份

2.如，服务属于经营行政许可管理或者经营强制认证管理的，提供相关资质复印件1份

**（二）参与人员资质**

附件2格式的《法人授权委托书》1份

**（三）报价单**

附件3格式的《报价单》3份

**（四）服务方案与质量保障措施**

自定义格式A4纸正反面打印的《服务方案与质量保障措施》3份

**（五）市场应用**

附件4格式的供应商《市场应用情况表》3份（顺序为威海区域在前，其他区域在后，数量不超过20家）

**（六）其他资料**

原则上不需提供其他资料，但如果供应商认为确有必要追加提供的，可提供不超过2种、每种1份的其他资料

**注意：**以上（一）至（六）严格按照要求的种类、数量、顺序整理为一套资料（严禁乱提供非本函要求的资料），每页加盖供应商的红章，使用长尾夹固定。

**七、其他事项要求**

（一）医院接受供应商在论证前的合理时间来院勘查与咨询，但在来院前需要与医院招标办联系确定相关事宜。

（二）参与供应商在论证当日签到时，应当同时确认与其他参与供应商无出资、隶属、关联或者实际控制关系。存在上述关系的供应商，只能有一家参与论证。隐瞒、漏报上述关系的，医院将取消全部关联供应商的参与资格，已经获取推荐意见的，推荐意见作废。

**八、联系人与联系方式**

联系人：王博

电 话：0631-5960192

邮 箱：slsyzbb@163.com

附件：1.报名信息表

2.法人授权委托书

 3.报价单

4.市场应用情况表

5.网络安全运维服务需求明细

 威海市立第三医院

2023年8月21日

附件1

报名信息表

编号：

名称：

以下为具体报名信息

|  |  |
| --- | --- |
| 报名日期 |  |
| 公司全称 |  |
| 办公固话 |  |
| 电子信箱 |  |
| 公司地址 |  |
| 联系人 |  |
| 手机号码 |  |

附件2

**法人授权委托书**

本授权书声明： （公司名称）法定代表人 （姓名），代表本公司授权 （姓名）为本公司的合法代理人，参加威海市立第三医院 （项目编号）项目的论证，并以本公司名义处理一切与之有关的事宜。

本公司已充分理解本项目邀请函的全部内容，并承担因理解错误所导致的不利后果。

法定代表人签字：

 （授权单位在此处盖章）

被授权人签字：

被授权人身份证复印件粘贴于下框：

|  |
| --- |
|  |

附件3

**报价单**

|  |  |
| --- | --- |
| **项目** | **价格（元）** |
| 一年期医院网络安全运维服务 |  |

必须额外满足的付款要求和对于报价的追加说明（如有）：

供应商盖章：

附件4

**市场应用情况表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序****号** | **产品/服务采购单位** | **采购年度** | **联系人** | **联系电话** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

供应商盖章：

附件5

**信息网络安全运维服务需求明细**

**1. 服务的范围**

服务的空间范围包括中心机房及各信息弱电间。服务的对象范围包括信息系统主机、存储系统、数据库系统、网络系统、安全系统以及相关的软硬件、数据库、操作系统软件、UPS、配电、动环系统等。加强主要业务系统的信息系统安全方面工作（例如信息安全风险评估、安全管理体系建设、信息安全培训等）。

**2. 服务的内容**

**2.1 资产登记服务**

每半年对中心机房内的各类设备设施做全面普查，做出资产登记表和主要设备的运行情况表，对设备设施的运行情况进行总体评估，向医院提交普查报告。提供的文件：资产登记表，机房普查报告。运维服务启动时提供一次，随资产的增加或减少每季度及时修订。

**2.2 网络梳理服务**

每年根据实际的网络情况和数据流向完善网络拓扑图，需由主流网络设备厂商认证高级工程师参与梳理整体网络架构，结合医院的业务和安全现状，通过查看安全设备的配置制定符合客户现状的安全策略，建立符合目前业务安全性的安全基线标准。

**2.3 漏洞扫描服务**

应用系统上线前或新版本应用发布前对应用系统进行漏洞扫描服务，提前发现其中存在的高危漏洞，并提出修补建议，协助做好漏洞的封堵。

每半年利用漏洞扫描工具扫描网络中的核心服务器及重要的网络设备(包括服务器、交换机、防火墙等)，以对网络设备进行安全漏洞检测和分析，对识别出的能被入侵者利用来非法进入网络或者非法获取信息资产的漏洞，从而全面掌握内部网络安全面临的弱点。根据漏洞扫描工具输出的结果进行评估，采取不同的技术手段或管理手段加强漏洞管理。从而有效地降低安全风险，提高安全防护能力。

**2.4 渗透测试服务**

为客户HIS系统、门户网站及所有与互联网相连的系统，开展一年一次的安全渗透测试服务。对目标系统的安全作深入的探测，发现系统最脆弱的环节。发现系统最脆弱的环节和可能被利用的风险点，提出安全整改建议，并对整改实施过程中遇到的问题提供技术支撑。所有的渗透测试行为将在客户的书面明确授权和监督下进行。

**2.5 风险评估服务**

网络安全风险评估是从风险管理角度，运用科学的方法和手段，每半年系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解信息安全风险，将风险控制在可接受的水平，最大限度地保障信息安全提供科学依据。

**2.6 重大安全事件告警服务**

收集和整理最新安全事件，包括但不限于系统或软件漏洞、安全事件、行业资讯等信息，不定期发送预警通告，遇紧急高危漏洞或重大信息安全事件告知并排查，如发现问题确认可处理则安排技术人员跟进解决。

**2.7 培训服务**

每年提供不少于 2天 5 人次的培训，培训内容包括但不限于：机房运维知识培训、服务器、存储培训、网络安全培训、信息安全知识等培训。培训人员、时间及地点由采购方确定，师资等由服务供应商提供。

**2.8 主机及存储运维**

对服务器及存储提供监控服务及应急故障响应服务。

主机服务内容如下：

主机日常运维需求响应，如参数调整，服务搭建。排错及故障处理，若涉及生产环境配置变化，按变更流程发起相应操作。

操作系统的安装，环境初始化（如：杀毒软件安装、备份部署，用户设置，按卫健委相关文件要求配置主机安全基线等）。

监测主机CPU、内存、网络流量、磁盘空间、应用服务等运行状态，并以月度为单位结合历史数据对每台主机进行性能分析，合理调整服务器CPU、内存配置，并对现有环境剩余资源进行容量评估，提前通知用户进行扩容准备。

存储运行状态日常监测，包括存储IO，资源利用率，SAN交换机链路状态，包错误率等，并以月度为单位输出磁盘空间使用情况。

存储日常巡检，每周进行一次日志巡检，每月进行一次现场巡检，检查硬件状态、结合日志对存储的运行情况进行分析与评估。

存储日常配置调整与故障处理，如存储划分、扩容、资源回收，硬件问题诊断与修复等。

**2.9 网络设备运维**

对网络设备进行监测，主动发现网络设备中存在的如环路、链路质量差、丢包、stp震荡等影响业务正常使用的问题。

收集网络运行性能信息，如CPU、内存利用率，带宽使用情况，及时对发现的问题进行告警，并进行相应问题的解决。以月度为单位，进行现场巡检，对网络的总体运行情况及剩余资源容量进行评估，提前通知用户进行扩容准备。

提供外网链路中断应急处置能力，如遇网络中断、网络故障、网络瘫痪，能短时间到达现场进行问题排查和恢复。

对安全设备进行每周巡检，发现其中的安全事件，并及时进行事件的处理，对于即将过期或已过期的安全设备特征库，及时通知用户进行升级续费。

对网络整体架构进行周期性（每半年一次）评估，发现其中的不合理部分，并出具整改方案，待与用户确认后进行网络整改。

响应用户的其它日常网络需求及安全策略设置需求，按变更流程进行相关配置的变动。

**2.10 操作系统等运维**

每季度对服务器上运行的操作系统（LINUX 和 WINDOWS ），双机软件等进行运维和支持服务。

操作系统运行状态检查、监控及预警

操作系统性能分析、设备日志检查分析等

操作系统配置优化、性能调优、垃圾数据清理等

操作系统故障响应、排查、诊断和处理

操作系统的安装、备份及恢复计划

操作系统补丁升级，

核心应用需甲方与第三方软件厂商确认方可补丁升级

补丁如果产生费用由服务采购方承担

操作系统安全加固

**2.11 虚拟化运维**

对虚拟化及超融合环境进行5\*8小时日常运维响应，紧急故障提供7\*24小时响应。

每月对虚拟化/超融合环境剩余资源进行容量评估，通知用户进行扩容准备。

每季度对虚拟机CPU/内存资源使用情况进行全面分析，对于造成资源浪费的虚拟机进行资源回收，对资源不足的虚拟机及时进行资源上调。

确保虚拟化集群/超融合集群HA、DRS等功能持续可用，并每月进行一次巡检。

对虚拟化/超融合资源的扩容、改造、跨集群迁移、安全补丁更新等提供支持，出具相应技术方案与用户确认后进行实施。

**2.12 机房配电基础运维服务**

查看各个开关及仪表显示是否正常；

检查电压、电流是否正常UPS电池定期充放电（半年次）

UPS供电支撑性评估（半年次）

精密空调过滤网定期更换（每年次）

精密空调室外机清洗（每年2次）

空调按需充氟，机房水过滤耗材更换（根据加湿使用要求每年次）

设备寿命评估

**2.13 等级保护合规运维**

每年随等保测评提供基于信息安全等级保护测评后的网络调优、基础设施配置、安全策略优化、安全管理中心搭建、制度建立等全方位整改相关服务（应用软件除外），确保最终测评结果为良及以上。

提供以下文件

《等级保护测评差距分析整改报告》

（含整改过程中的实物照片、策略调优截图、整改预期效果等）

《信息化资源现状/资源利用分析报告》

《信息化资源整合整改分析报告》

《信息化资源整合整改阶段报告》

《信息化资源整合整改结果汇报》

《巡检报告》

《服务事件记录》、《故障报告》

**2.14 重大事件应急处置服务**

如客户即将或已经经历重大事件（例如即将召开重要会议直播、要员来访、法定重要日期、黑客攻击、病毒或木马发作等），及时派出技术人员提供保障或应急处置，如解决问题需软硬件采购可由服务商先行垫付，在处置完成后由院方支付，每年限2次。

**2.15 数据库操作系统安装服务** 按需

根据用户的硬件平台推荐适合的操作系统类型和版本

根据 Oracle 数据库的要求，科学地安装和配置操作系统

调整必要的操作系统运行核心参数

定制数据库服务器上的操作系统服务程序，减少不必要的服务，节约资源

及时推荐和安装操作系统补丁，保障操作系统安全

设置数据库用户在操作系统中的运行环境

配置合适的数据库存储方式

配置数据库的自动启动脚本，减少开机的复杂性

**2.16 数据库单机安装服务** 按需

合理安装数据库软件

根据应用系统创建合适的数据库

根据应用系统的要求分配数据空间

设置合理的数据库运行参数

检查和设置数据库用户的安全性和访问的安全性

设置数据库的监听程序

培训用户的数据库基本操作流程

提供完善的数据库安装报告

**2.17 优化配置和性能调整服务** 每月

需oracle行业认证工程师

对数据库的运行况进行监控，及时发现资源不足，锁，慢查询等可能导致业务异常的问题，及时发出告警，并进行应急处理。

分析用户的应用类型和用户行为

确立明确的调整目标

查找数据库运行瓶颈和原因

评价并修改 ORACLE 数据库的参数设置

评价并调整 ORACLE 数据库的数据分布

评价应用对硬件和系统的使用情况，并提出建议

利用先进的性能调整工具实施数据库的性能调整

培训用户有关性能调整的概念

提供用户完整的性能调整报告和解决方法

**2.18 数据库安全检查及配置服务** 每季度

利用完整的数据库安全检查列表来评价数据库系统的安全性

识别数据库系统里的安全风险

识别导致破坏性的后门程序

识别安全级别低的用户和密码

提供用户名称和口令相同的用户名单

清除所有威胁数据库的安全隐患

**2.19 数据库补丁安装服务** 按需

评估当前数据库软件的运行版本

查找和准备可用的补丁

认证补丁安装的必要性，评估补丁安装的利弊

明确补丁可以解决的问题，确定补丁安装的时机

为安装补丁备份好软件和数据库

和用户协调计划停机时间

实施补丁的安装

完成补丁安装的后续服务

检查操作结果并记录备案，提供补丁安装过程报告

**2.20 数据库迁移服务** 按需

合理规划迁移方法及步骤

制定详细的迁移过程

准备必须的迁移工具

实施迁移过程

迁移后的修改工作

确认系统在 Oracle 数据库上的稳定运行

完成其他后续事宜

检查操作结果并记录备案，提供数据库迁移过程报告

**2.21 数据库容灾服务** 每季度

容灾备库方案选择（DATAGUARD\XTTS\OGG等软件）

根据用户容灾需求进行规划

根据制定的方案进行容灾系统实施搭建

对用户提供容灾系统日常维护的指导

提供完整的容灾系统文档

**2.22 数据备份服务**（用户提供备份设备）

根据不同的业务级别，对虚拟机/数据库/应用程序进行数据备份部署

每周对备份任务进行巡检，及时随业务系统上下/下线进行备份任务调整

对于备份失败的任务进行排错，确保数据备份正常。

每季度进行一次数据恢复演练，验证数据可恢复性。

对于需要长时间归档的数据，及时为用户提供可行的归档方案，并与用户确认后进行实施。

**2.23 服务器和存储设备故障演练**

制定服务器、存储设备发生故障时的应急预案及故障处理流程，并模拟故障发生时的状态进行故障应急处理演练。

提供的文件：应急演练预案。

**3. 服务的团队要求**

3.1 服务方就本项目组建专门的运维服务团队，提供7x24小时技术支持服务，做到随时响应、1小时内到达现场开展工作、4小时内解决故障或者针对故障提出解决方案。

3.2 服务团队由日常运维工程师，重大保障工程师，专家级工程师组成。

3.3 日常运维工程师负责按照项目服务体系的日程规划组织日常运维服务，完成医院交办的各项任务,及时汇报项目整体运维情况，保障信息系统稳定运行。

3.4 重大保障工程师不少于2人，在医院承担重大工作期间和日常运维工程师一起为重大工作提供技术保障。

3.5 专家级工程师负责指导日常运维工程师和重大保障工程师开展工作，在重要节点提供现场技术支持，每半年进行一次信息系统运行趋势评估，提出优化改善建议。