#  采购需求

**一、项目概述**

采购人门户网站自2023年11月29日正式上线，至今已开设多个栏目与页面，并购置多项安全产品服务，为保障采购人门户网站安全正常的服务于患者，确保采购人信息发布及时、安全与通畅，维护安全的网络环境，充分保障患者享有的医疗服务权益，现委托具有维护能力供应商，为采购人进行网站安全与维护工作，进一步加强医院门户网站的维护管理与技术能力。

**二、技术服务要求与内容**

**1.售后运维服务的门户网站主要栏目：**

|  |
| --- |
| **陕西省交通医院门户网站栏目汇总表** |
| **主要栏目** | **二级栏目** |
| 医院概况 | 医院简介、医院领导、专家介绍、组织架构、资质荣誉、医院文化、医疗设备、医院环境、联系我们 |
| 新闻中心 | 医院动态、医疗动态、公示公告、招标公告、科普宣教 |
| 科室一览 | 临床科室、医技科室、行政后勤科室 |
| 医疗服务 | 门诊就诊指南、医保政策、价格服务、病历复印、便民措施、院内感染控制 |
| 患者服务 | 预约挂号、预约体检、满意度调查、体检项目介绍 |
| 护理园地 | 护理动态、教学科研、护士风采 |
| 党群建设 | 党建活动、党务公开、党风廉政、工会工作 |
| 人事管理 | 人事任免、招聘职位 |

**2. 门户网站云产品参数要求：**

服务商根据以下技术参数为采购方提供门户网站云服务与安全产品，但不仅限于以下服务，可依据自身技术能力提供额外安全产品与安全服务，确保采购人门户网站满足二级网络安全等级保护测评标准。

|  |  |  |
| --- | --- | --- |
| **产品名** | **主要参数** | **数量** |
| 云服务器 | CPU：≥8核(国产)内存：≥16G系统盘：≥50G，增强型SSD云盘数据盘：≥500GB网络类型:专有网络 5Mbps操作系统：支持国产操作系统数据库：支持国产数据库 | 1台（租赁期1年） |
| 云安全管理 | 实现实时识别、分析、预警安全威胁，并具备威胁检测、响应、溯源、防御的自动化安全运营闭环，有效保护云上资产和本地主机并满足监管合规。产品具备云蜜罐、网页防篡改、恶意文件检测与安全大屏展示等技术防护服务器台数: ≥1台；日志存储天数：≥180天；日志存储空间：≥120Gb；恶意文件检测次数：≥10万次防勒索存储空间：≥50Gb； | 1年 |
| 云防火墙 | 可防护公网IP数：≥20个（含IPv4与IPv6）；NAT防火墙实例数：≥1个NAT防火墙公网流量处理能力：≥10 Mbps；提供云防火墙的防御能力总览，展示最近7天访问流量统计数据和已检测出的安全风险统计数据。支持对私网IP访问公网的流量进行访问控制，有效拦截内部网络到公网的未授权访问。支持服务器安全组中的高危风险规则检测，并提供修复建议。实时监控云资产主动访问互联网的行为。检测云防火墙防护的云资产暴露在公网的IP地址、端口、应用数据，提供可视化分析报表。内置威胁检测引擎，支持配置攻击防护规则，实现更精准地识别和阻断入侵风险。实时展示入侵防御、漏洞防护、失陷感知的防御数据，支持查看防御详情，并提供威胁检测引擎实时检测入侵活动的处置方案。提供事件日志、流量日志与操作日志审计分析；提供7天日志审计功能。实时地自动采集、存储和分析出、入方向的流量日志，存储时长可自定义7-365天；支持基于特定指标，定制实时的监测与告警，确保在关键业务发生异常时能够及时响应。支持资产异常告警：在资产出现流量异常、主机失陷、异常外联活动、漏洞风险、未开启保护、未开启入侵防护时，可以及时通过短信或邮件发送通知。账号管理：支持多账号统一管理。支持公网资产的入方向和出方向流量的访问控制（南北向），有效防止外部恶意攻击和黑客入侵，并且严格控制主动外联的出流量。日志存储容量：≥1000 GB； | 1年 |
| waf应用防火墙 | 域名数：≥10个业务请求峰值：≥10个支持自定义放行具有指定特征的请求（白名单）。支持一键封禁特定的IP地址的访问能力（黑名单）。支持对符合自定义规则的请求进行观察、拦截、验证等处理。防御常见的CC攻击，支持内置的防护和防护-紧急两种模式。支持高频扫描封禁、目录遍历封禁、扫描工具封禁。锁定网站页面，防止内容被恶意篡改。支持电话号码、身份证、银行卡等重要隐私数据的泄露防护。支持重保威胁情报、重保防护规则组、重保IP黑名单、Shiro反序列化漏洞防护。支持防御DDoS攻击。 | 1年 |
| 日志审计 | 日志存储容量：≥40 GB；支持云资产多维度的安全日志，提供多维度的报表。支持SQL语法分析功能。具备网站状态监控、攻击排查、溯源定位等功能。 | 1年 |
| 防篡改 | 防护服务器台数：≥1台支持防止网站服务器中的静态网页文件被复改。支持防止网站数据库中动态网页内容被复改。保障网站信息不被恶意篡改，出现挂马、黑链、非法植入恐怖威胁、色情等不良内容 | 1年 |
| 保垒机 | 支持Windows系统、Linux系统运维。支持常用的运维协议：SSH、RDP。支持手动新建以及一键导入第三方云资产。支持短信、邮箱及手机TOTP令牌等双因子认证。支持Mstsc、Xshell、SecureCRT、Putty等客户端工具登录堡垒机访问主机。使用本地WinSCP、Xftp、SecureFX等SFTP客户端工具登录堡垒机进行文件传输。支持实时监控正在进行的会话，并可随时阻断会话。支持对RDP运维时，粘贴板上传或下载、磁盘映射等操作进行控制。支持SSH运维时，设置命令黑白名单阻断及审批策略，控制高危、敏感命令执行。支持在运维过程中，对文件的上传、下载、删除、重命名，文件夹的创建、删除等操作进行控制。支持启用运维二次审批，只有在管理员批准后，运维员才能访问资产。支持限制登录堡垒机的用户、资产的来源IP及登录时段。支持设置运维空闲时长限制及总时长限制。支持针对运维操作全程进行日志及录像审计，可通过录像清晰地还原并追溯运维过程。支持对文件传输进行审计。支持生成运维报表，可导出PDF、HTML、WORD三种格式的报表。支持将会话审计日志转存至SLS及通过日志备份下载到本地。支持OpenAPI接口调用。带宽：≥8 Mbit/s存储：≥1 TB |  |

**3.医院故障分级标准及响应时间要求**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **故障等级** | **故障情况描述** | **响应时间要求** |
| 1 | 一级故障 | 网站瘫痪，或出现攻击篡改页面，严重影响医院门户网站正常运作。 | 服务商应在10分钟内响应，并启动相应急预案，1小时内到达现场，4小时内解决问题，或提供相应解决方案直至系统恢复正常。 |
| 2 | 二级故障 | 网站因遭受攻击性能严重降级，或由于系统性能失常严重影响用户的业务动作。 | 服务商应在10分钟内响应，2小时内到达现场或远程维护，6小时内解决问题，或提供相应解决方案直至系统恢复正常。 |
| 3 | 三级故障 | 门户网站部分功能受损，影响部分栏目或功能，医院信息发布受阻。 | 服务商应在10分钟内响应，6小时内到达现场或远程维护，12小时内解决问题。 |
| 4 | 四级故障 | 网站出现一般性问题，对患者与信息发布几乎或无影响。 | 服务商应在10分钟内响应，12小时内到达现场或远程维护，24小时内解决问题。 |

**4.售后运维服务要求：**

服务商根据以下要求内容提供售后运维服务，但不仅限于以下服务，可依据自身技术能力提供额外服务。

4.1、根据采购人的需求提供网站栏目的更新、网站版面的改版及页面风格的更新等服务；

4.2、根据采购人提供的素材与文稿提供网站图文页面编辑排版服务，并提交采购人审核，待审核通过后及时上传网站。定期梳理网站各栏目，协助采购人栏目管理部门进行栏目更新；每月对已发布的图文进行差错核查，并形成报告及时通报采购人管理部门。

4.3、提供网站系统的日常保障服务。保障门户网站正常运转，提供网站各应用层面的运行维护服务，做好访谈、交互功能等现场支撑和应急技术支持工作，避免网站无法正常访问、访问出错、宕机、网站错误等现象的发生。

4.4、提供网站系统定期保养服务。每三个月对操作系统进行一次全面维护；每三个月对数据库进行一次全面维护，包括垃圾数据清理、log日志整理、数据备份等；每月定时对网站服务器进行维护，包括网络安全和网络性能检查和修正；提供阶段性系统维护和升级建议，并提供最新版本升级服务；及时协助采购人信息支持部门对操作系统、中间件和数据库进行升级。

4.5、提供网站系统软件的运维服务。提供操作系统、应用软件及数据库的安装配置和维护服务；及时提供系统补丁包升级服务，LOG日志及垃圾文件清理等；及时向采购人提交软件升级情况报告及升级建议方案；定期提供相关产品高版本的升级和补丁升级服务，保证所提供产品升级与补丁的稳定的、安全的，并附有完整的升级说明、新增功能说明、对应用的影响说明等文档；及时提供升级产品的操作培训；提供软件开发代码、维护参数配置、权限管理、流程配置等。

4.6、提供网站安全运维服务，配合网络安全测评公司完成等保测评，根据测评整改建议。对网站系统可能存在的安全隐患提供修补服务；提供网站系统的安全维护和升级建议；及时处理上级单位或其他机构检测到的网站安全问题。

4.7、针对节假日和重要时期提供网站监测和应用层面的网络、网站安全服务。主要包括：安全备份，24小时专人不间断远程值守，故障通报，事故快速上门等。

4.8、定期为采购人提供网站运维相关技术培训，年度培训时长≥20学时

**5.售后服务方案与技术能力要求：**

5.1.服务商应根据院方信息化建设情况与信息系统使用情况，制定详尽的售后服务方案。内容应涵盖以下几点：

5.1.1. 售后运维服务的承诺。

5.1.2. 提供售后运维服务的具体内容。

5.1.3. 售后运维服务的具体措施。

5.1.4. 售后运维服务相关管理制度。

5.1.5 售后运维服务的应急预案。

5.1.6 售后运维服务人员的考核方案。

5.2. 售后服务技术能力要求：

5.2.1. 提供售后服务人员组织架构。

5.2.2 技术人员要求：服务商拥有技术团队人员≥10人

**6.数据安全与信息保密要求：**

6.1 服务商应具有数据安全相关管理制度。

6.2 服务商拥有数据安全方面技术人员，需提供相关技术能力证明材料，提供近三年的公司为其缴交社保证明材料。

6.3 提供服务商信息保密相关管理制度与公司员工保密协议。

**二、商务要求**

**1、合同内容及金额：**即成交单位的响应内容、现场澄清确认内容（若有）及其成交总金额。

**2、服务地点：陕西省交通医院**

**3、服务期：1年**。

**4、项目考核与验收**

4.1项目由采购人组织相关人员或其邀请的专家进行考核评价验收，考核与验收时成交人应无条件予以配合并提供所需的全部资料：

4.2考核标准：项目考核依据《信息系统售后运维服务质量评价标准》评分。评分90－100分为优秀，70－89为合格，70分以下（不含70分）为不合格。

4.3验收依据：项目考核汇总表、采购文件、响应文件、合同文本、国内相应的标准、规范。

**5、结算方式**

5.1结算单位：采购人结算，结算前成交人须开具等额发票给采购人，采购人收到发票后，按照5.2的付款方式结算，（未开具发票采购人有权拒付合同款项），否则导致的付款延误，责任自行承担。

**5.2付款方式：**

双方签订合同后5日内付合同价款的50%，剩余部分待2025年12月经采购人组织相关专业人员依据考核评价标准对服务商2025年运维服务情况考核验收后，7个工作日内根据考核验收情况支付。考核评价成绩为优秀，采购人支付合同额剩余的50%；考核评价成绩为合格，采购人扣除合同额的10%，支付合同额的40%；如考核评价成绩为不合格，采购人扣除合同额剩余的50%。

**6、知识产权**

6.1供应商应保证投标服务及货物不会出现因第三方提出侵犯其专利权、商标权或其它知识产权而引发法律或经济纠纷，否则由供应商承担全部责任。任何被供应商用于未经授权的商业目的行为所造成的违约或侵权责任由供应商承但。

**7、违约责任**

7.1按《中华人民共和国民法典》中的相关条款执行。

7.2成交人未按合同要求提供货物与服务或货物与服务质量不能满足合同、单一来源采购文件、响应文件要求，且在规定时间内未使采购人满意的，采购人有权单方解除合同，合同解除后，成交人应赔偿解除合同给采购人造成的全部损失，并按照合同总价的30%向采购人支付违约金。同时采购人会将成交人的违约行为上报同级监管部门。

7.3合同期内，若成交人未按采购文件及合同要求的时限响应并排除故障的，每出现一次，按照合同总价的【 】%向采购人支付违约金，合同有效期内前述情形累计出现【 】次的，视为成交人根本违约，采购人有权单方解除合同，合同解除后，成交人应赔偿解除合同给采购人造成的全部损失，并按照合同总价的30%向采购人支付违约金。同时采购人会将成交人的违约行为上报同级监管部门。

**注：本项目技术要求及商务要求不允许负偏离。**

**8.信息系统售后运维服务质量评价标准**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评价项目分类** | **评分分值** | **评分标准** |
| **分项分值** | **明细分值** |
| 1 | 日常售后运维服务 | 故障问题解决的及时性 | 依据服务商在服务期内处理相应故障等级的响应时间与招标文件、投标文件与合同中相关内容完成情况进行评价。 | 5 | 2 | 1、服务期内出现一级故障响应时间超时大于10分钟以上扣【2】分/次； |
| 1.5 | 2、服务期内出现二级故障响应时间超时大于10分钟以上扣【1】分/次； |
| 1 | 3、服务期内出现三级故障响应时间超时大于10分钟以上扣【0.5】分/次； |
| 0.5 | 4、服务期内出现四级故障响应时间超时大于10分钟以上扣【0.1】分/次； |
| 依据服务商在服务期内处理相应故障等级的解决时间与招标文件、投标文件与合同中相关内容完成情况进行评价。 | 15 | 6 | 1、服务期内出现一级故障解决时间超时或未按要求时限解决问题大于4小时以上扣【6】分/次； |
| 4 | 2、服务期内出现二级故障解决时间超时或未按要求时限解决问题大于6小时以上扣【2】分/次； |
| 3 | 3、服务期内出现三级故障解决时间超时或未按要求时限解决问题大于12小时以上扣【1】分/次； |
| 2 | 4、服务期内出现四级故障解决时间超时或未按要求时限解决问题大于24小时以上扣【0.2】分/次； |
| 运维服务质量评价 | 依据招标文件、投标文件与合同中运维服务约定内容，对服务商在服务期内完成情况进行评价。 | 25 | 10 | 1、服务期内服务商是否按相关文件约定项目提供售后运维服务，依据日常工作记录评价。 |
| 10 | 2、服务商对采购人日常登记或提出的售后问题解决情况，有无推诿、拖延等现象。 |
| 5 | 3、售后运维服务工作记录完整情况。有无存在篡改、虚报工作记录等现象。 |
| 数据库运维服务质量 | 依据招标文件、投标文件与合同中约定的相关服务内容，服务商运维人员工作完成情况进行评价。 | 10 | 2 | 1、服务期内定期巡检完成情况，巡检次数不少于2次。 |
| 3 | 2、服务期内依据巡检情况为采购人提供合理化建议，或提供建设与整改方案。 |
| 3 | 3、服务期内为采购人提供数据库优化服务的完成情况，次数不少于1次。 |
| 1 | 4、服务期内服务商按合同约定的数据库服务项目完成情况。 |
| 1 | 5、数据库运维服务各类记录完整，问题分析详细，解决及时。 |
| 3 | 系统升级更新服务 | 系统升级服务 | 结合系统升级服务相关工作记录，对服务商该项工作完成情况与服务质量进行评价。 | 5 | 1 | 1、升级服务项目管理组织能力情况，是否成立项目专班，组织架构合理，技术能力强。 |
| 4 | 2、升级服务准备工作完善，信息收集全面，功能模块测试到位，升级过程系统无重大故障发生。 |
| 服务质量 | 依据服务商提供的升级服务工作日志记录与服务质量调查表情况评价。 | 3 | 1 | 1、升级各工作日志记录完整，有测试报告、问题分析、实施方案。 |
| 2 | 2、升级服务后续无遗留问题，使用部门评价达标率≥90% |
| 4 | 网络安全与数据安全服务 | 网络安全服务 | 根据采购人提供的网络安全等保测评报告整改建议书组织进行相应问题的整改完成情况进行评价。 | 10 | 2 | 1、是否成立技术专班，逐项细致分析问题，且依据整改建议书制定整改方案。 |
| 5 | 2、整改方案是否及时、有效落实到位。 |
| 3 | 3、整改完成后，协助医院进行等保复测，复测达标率≥80%。 |
| 数据安全服务 | 依据国家相关信息系统数据安全标准，对服务商提供的数据安全服务进行评价。 | 5 | 2 | 1、是否为采购人建立数据安全保护机制，提供信息系统数据安全方面合理建议。 |
| 3 | 2、是否通过提供技术方案保障采购人数据安全。 |
| 数据信息保密 | 依据国家数据信息保密相关法律法规及保密协议约定的条款，综合对服务商数据信息保密工作进行评价。 | 4 | 0.5 | 1、服务商是否建立数据信息保密制度或相关保密机制。 |
| 1 | 2、服务商与采购人是否签定保密协议。 |
| 1 | 3、服务商是否与服务人员签定保密协议，且制定相关绩效考核制度。 |
| 1.5 | 4、保密协议期内是否存在信息泄露事件，如发生重大泄密事件，除根据协议追究服务商法律责任外，数据信息保密项目所有分值扣除。 |
| 5 | 培训服务 | 依据服务采购合同，评价服务商在服务期内提供的培训服务质量。 | 5 | 2 | 1、依据合同是否制定的培训计划。 |
| 3 | 2、培训计划落实情况，少一次扣【1】分/次。 |
| 6 | 配套产品运维服务 | 依据服务采购合同，服务商对网站配套云产品提供的运维服务完成情况进行评价。 | 5 | 5 | 1. 服务商是否对网站配套云产品提供的运维服务，且工作记录完整。
2. 服务期内配套云产品未发生重大故障。
 |
| 7 | 服务满意度 | 依据采购人对服务商服务满意度调查表情况评价。 | 5 | 5 | 1. 服务满意度≥90%。
2. 服务期内无关于服务商工作人员服务质量相关的重大投诉案件。
 |
| 8 | 项目管理评价 | 依据网站管理部门对服务商在服务期内项目管理工作评价表情况综合评价。 | 3 | 3 | 网站各栏目管理部门根据服务商日常项目管理工作及协调能力评价达“合格”以上。 |
| 9 | **合计** | **100** | **100** |  |