**招 标 文 件**

采购项目：**银丰（济南）医院信息安全项目**

采 购 人：**银丰（济南）医院**

日 期：**2024年 7月18日**

## 第一部分 采购公告

**1.采购人**

1.1采购人：银丰（济南）医院

1.2采购人地址： 山东省济南市凤山路2001号

1.3技术联系人： 陈立华19953155789刘国栋 19953158448

商务联系人：王国栋 19953150903

**2.采购项目**

项目名称：银丰（济南）医院信息安全项目

采购内容：详见附件一：项目建设需求

**3.资金来源**：自筹资金

**4.采购方式：**公开招标

**5.资格审查方式：**资格预审

（需查验的资料：

1、营业执照副本及企业业绩合同。

1. 本地化团队社保证明
2. 以上资料需原件或复印件。复印件均需加盖公司公章及法人章，简单装订，否则视为无效。）

**6.投标人资格要求：**

6.1投标人必须具备独立法人资格，能够独立承担法律责任，有固定的办公场所，满足招标项目要求的服务能力及其他条件的制造商（厂商）。

6.2业绩：具备近三年（2021年5月至今）不小于150万元的网络安全项目业绩；

6.3具有良好的银行资信和商业信誉，没有处于被责令停业、财产被接管、冻结、破产状态。

6.4 投标供应商需取得产品原厂对本项目的投标授权。

6.5不允许联合体承包该项目。

6.6 仅限国产品牌的软硬件参与。

**7.采购日程安排**

7.1报名截止时间：2024年7月23日12:00前将各资质文件、参与投标标段、联系人方式发送至联系邮箱yfyycg@yinfeng.com.cn

7.2报名结果通知：7月23日23:00前，招标人通过邮箱进行报名结果通知。

7.3 投标文件递交时间：截止至开标前30分钟。 (逾期送达的或者未送达指定地点的投标文件，采购人不予受理)。

7.4投标文件递交地点：银丰医院 B9 会议室。

7.5 采购会议开始时间：

|  |  |
| --- | --- |
| 标段 | 开标时间 |
| 信息安全项目 | 2024年7月25日14:00 |

7.6会议地点：银丰医院 B9 会议室。

**8.投标报名费**

8.1截止时间：2024年7月24日17:30前

8.2报名费金额：500元人民币

8.3汇款信息

单位名称：银丰（济南）医院有限公司

银行账号：1602 0932 1910 0100 623

开户银行：工商银行济南未来城支行

注：接报名成功的邮件通知后再打报名费，报名费不退，无发票，可开收据，开标现场核验报名费付款凭证。

**9.投标保证金**

9.1投标保证金支付：2024年7月24日17:30前，报名企业需对公付支付投标保证金。

9.2保证金金额：5万元人民币。

9.3返还时间：未中标企业在评审结束后15日内返还；中标企业在双方签订合同并生效后15日内返还。

9.4收款账户：（参照报名费收款账户）。

**注：未尽事宜，以招标公告为准。**

## 第二部分 投标须知

**1.总则**

1.1本次采购遵循“公开、公平、公正”的原则，并严格按有关规定操作。

1.2要求合格的投标人：投标人必须具有企业法人资格，承认和履行采购文件中的各项规定。

**2.投标方相关文件资料的编制**

2.1 投标方编写的相关文件资料应包括：

2.1.1 按采购人要求出具证明文件（见第三部分投标文件目录）并加盖投标方公章。

2.1.2投标方应递交五份投标文件，一正四副，胶装成册。正本与副本不相符时以正本为准，文件封页（见格式一）加盖公章。提供电子版投标文件（U盘形式）

2.2 报价表

2.2.1应在报价表上标明拟提供项目单价和总价，提供具体详单。

2.2.2 投标方的报价为含税全部价，币种：人民币（元）。

**3.评审办法**

3.1评审工作遵循公开、公平、公正、科学择优的原则。

3.2本次评审采用百分制评分法，细则详见附件二：项目招标评价表

3.3 当参加投标会议的投标方少于三家时，招标会议终止。

**4.合同的签订**

采购人根据评审结果，通知确定的成交投标方与采购人签订合同。

**5.交付**

5.1交付执行地点：采购人所在地。

5.2付款：采购方以首款40%+验收款50%+质保金（10%，1年）的形式支付。具体的支付节点与金额，以双方合同为准。

5.3供货周期：首付款后15日历日，如遇工期紧张，以采购人要求为准。

## 第三部分 投标文件目录

1．项目报价；

2．有效的企业营业执照（三证合一，复印件）；

3．法定代表人资格证明或法定代表人授权委托书（详见附表一）；

4．法定代表人及授权委托人身份证复印件；

5．项目技术方案；

6．公司情况介绍；

7．财务要求：投标人须提供近两年（2023年-2024 年）经会计师事务所或审计机构审计的财务审计报告（包括资产负债表、现金流量表、利润表和财务情况说明书）（新成立公司提供自成立以来的年度审计报告）。

8.其他需要说明的内容

**注：资质证明材料须加盖公章**

## 第四部分 投标文件格式

**附表一**

**银丰（济南）医院信息安全项目报价单**

供应商名称：

项目名称 ：

|  |
| --- |
| 投标总报价（元） |
| 大写：元整 |
| 小写：元 |

说明：1．所有价格均系用人民币表示，单位为元。

2．投标报价包括本项目采购需求和投入使用的所有费用，包括但不限于主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

法定代表人或法人授权代表（签字）：

加盖公章

年 月 日

**附表二：**

**法定代表人身份证明**

投标方名称：

地址：

成立时间： 年 月 日

姓名（签字）：性别： 年龄：职务：

系（投标方名称）的法定代表人。

特此证明。

投标方： （盖单位章）

年 月 日

**法定代表人授权委托书**

本授权书声明：注册于 省 市 县工商管理局的 （单位名称）在下面签字的 （法定代表人姓名和职务）授权 （单位、部门名称）在下面签字的 （职务、姓名）为本公司的合法代理人，就 （招标编号）采购文件的 （产品名称）投标谈判及合同的签订、履行直至完成，并以本公司名义处理一切与之有关的事务。本授权书于 年 月 日签字生效。

法定代表人签字或盖章：

法定代表人身份证号码：

被授权代理人签字：

被授权代理人身份证号码：

单位名称（公章）：

单位地址：

被授权代理人联系电话：

日期： 年 月 日

**格式一 投标文件封页格式**

**封 页**

**XX项目**

**投标文件**

**时间： x 年 x 月 x 日**

**单位名称（加盖公章）**

## 附件一 项目建设需求

### 项目概况

银丰（济南）医院为一所集医疗、科研、教学和健康管理为一体的三级综合医院。围绕医疗市场需求与国家政策导向，医院将以严谨规范、科学高效、以人为本、精益求精的工作理念，目标建成济南最好的医院。医院将建立三大研究中心：干细胞临床研究中心、免疫细胞临床研究中心、基因检测精准医学研究中心；三大服务中心：健康管理中心、患者随访中心、医生服务中心；五大平台：影像中心、检验中心、病理中心、药学中心、营养膳食中心；十二个重点学科：心内科、神经内科、消化科、血液病科、肿瘤科、急诊科、普外科、疼痛科、妇产科、儿科、保健科、中医科。同时，太平洋保险集团源申康复医院（康复科）、济南市口腔医院（口腔科）入驻银丰医疗广场。其余专科BCD继续完成租赁合作或者自营建设。

根据医院的业务发展，为满足搭建“三位一体”智慧医院的总体架构，着重建设智能化管理、精细化运营、精准化服务的信息化网络，满足减少患者就医流程、减轻医护工作流程、可视化大数据分析方便领导决策分析的具备银丰特色的信息化三层服务体系，需完成网络安全等级保护体系建设，保障医院业务软件硬件基础设施底座保驾护航，保障医院核心业务稳定运行、核心数据安全可靠。

### 建设依据

#### 政策规范

《国务院办公厅关于促进“互联网+医疗健康”发展的意见》（国办发〔2018〕26号）；

《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》（国办发〔2016〕47号）；

《国家卫生计生委关于印发“十三五”全国人口健康信息化发展规划的通知》（国卫规划发〔2017〕6号）；

《关于印发公立医院高质量发展促进行动（2021-2025年）的通知》（国卫医发〔2021〕27号）；

《国家卫生健康委办公厅关于印发国家三级公立医院绩效考核操作手册（2022版）的通知》（国卫办医函〔2022〕92号）；

《国务院办公厅关于印发“十四五”国民健康规划的通知》（国办发〔2022〕11号）；

《关于印发“十四五”全民健康信息化规划的通知》（国卫规划发〔2022〕30号）。

#### 信息标准规范

《医院信息系统基本功能规范》（卫办发［2002］116号）；

《基于电子病历的医院信息平台建设技术解决方案》（卫办发〔2009〕130号）；

《电子病历系统功能规范（试行）》（卫医政发〔2010〕114号）；

《中医电子病历基本规范》（国中医药发〔2010〕18号）；

《中医医院信息系统基本功能规范》（国中医药办发〔2011〕46号）

《三级综合医院医疗质量管理与控制指标（2011年版）》（卫办医政函〔2011〕54号）

《国家健康医疗大数据标准、安全和服务管理办法（试行）》（国卫规划发〔2018〕23号）；

《电子病历系统功能应用水平分级评价方法及标准》（国卫办医函〔2018〕1079号）；

《医院智慧服务分级评估标准体系（试行）》（国卫办医函〔2019〕236号）；

《国家卫生健康委办公厅关于印发有关病种临床路径（2019年版）的通知》（国卫办医函〔2019〕933号）；

《医院信息互联互通标准化成熟度测评方案（2020年版）》（国卫统信便函〔2020〕30号）；

《国家卫生健康委办公厅关于进一步加强单病种质量管理与控制工作的通知》（国卫办医函〔2020〕624号）；

《医院智慧管理分级评估标准体系（试行）》（国卫办医函〔2021〕86号）；

《公立医院运营管理信息化功能指引》（国卫办财务函〔2022〕126号）；

《三级医院评审标准（2022年版）》（国卫医政发〔2022〕31号）；

#### 信息安全规范

《中华人民共和国网络安全法》

《中华人民共和国密码法》

《中华人民共和国计算机信息系统安全保护条例》；

《信息安全等级保护管理办法》（公通字〔2007〕43号）；

《信息系统安全等级保护定级指南》（2020年11月1日实施）；

《贯彻落实网络安全等保制度和关保制度的指导意见》（公网安〔2020〕1960号）；

《GB∕T 14394-2008 计算机软件可靠性和可维护性管理》；

《网络安全等级保护条例》（公安部，2018年6月27日）；

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

### 建设原则

#### 先进性原则

硬件系统必须严格遵循国际标准、国家标准和国内网络安全行业的规范要求；

所有的系统处于先进的技术水平，确保较长时间内技术上不落伍；

硬件系统的处理能力要达到业内领先水平，对于本次业务要留有一定的性能余量，以满足后续升级的需求。

#### 易维护原则

系统支持简体中文，通俗易懂，操作方便、简单；

系统支持WEB管理方式或集中管理方式。

#### 可靠性原则

应用系统需支持7×24h连续安全运行，性能可靠，以支持医院业务运行；

软件系统需支持不同系统类型，满足医院不同业务科室的系统使用需求；

网络关键设备按照冗余设计，提升设备间的容错性。

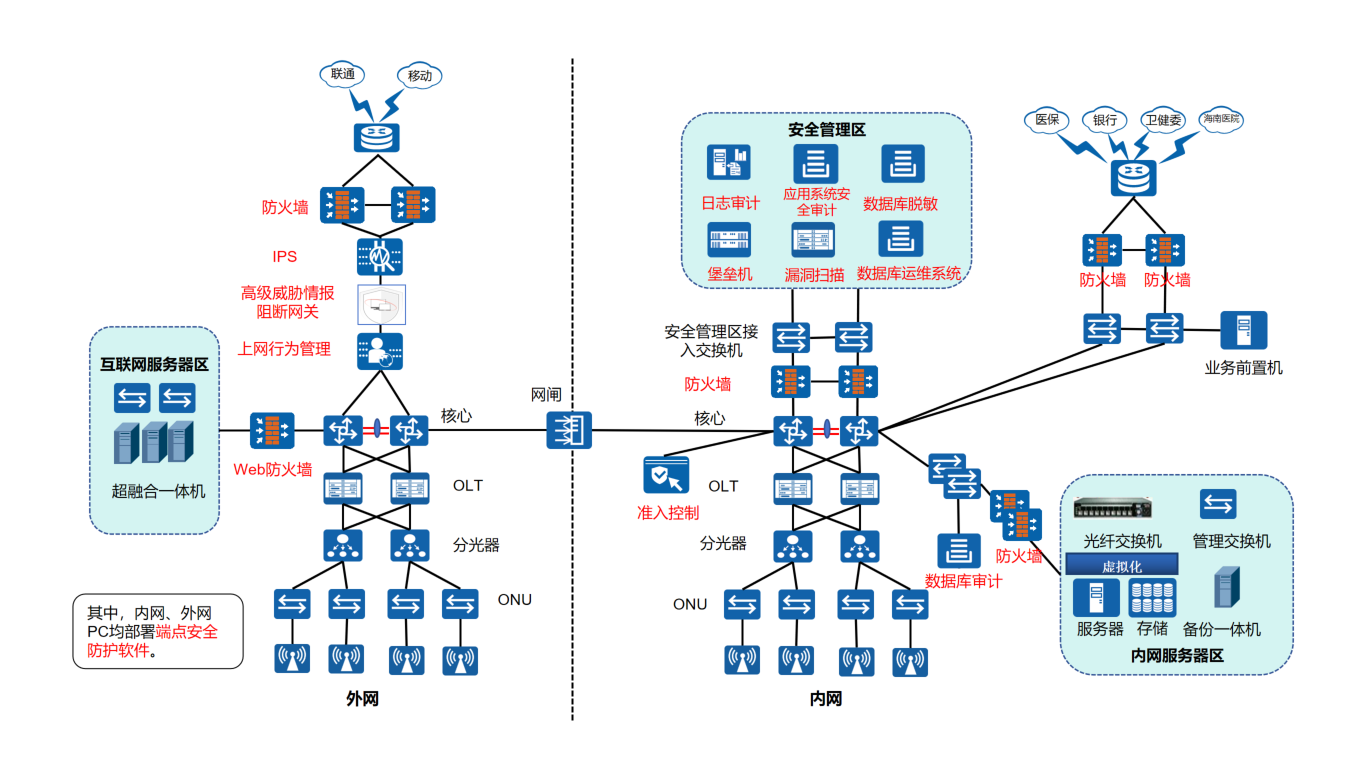
#### 合规性原则

硬件系统、软件系统应满足相关国家标准、行业标准的要求；

信息安全体系建设完成后，应满足国家、行业、集团等对于网络安全的要求。

### 总体技术要求

依照《网络安全法》、《医疗卫生机构网络安全管理办法》、《信息安全技术网络安全等级保护基本要求》等法规政策要求，结合银丰（济南）信息安全的规划、不同业务系统及业务科室的个性化安全需求，开展网络安全体系规划设计。整体方案遵循网络安全等级保护“一个中心，三重防护”的技术理念，安全技术与安全管理并重，整体设计方案如下：



### 技术参数

#### 互联网边界防火墙（含IPS、上网行为管理功能）

1.产品架构：软硬一体化1U标准机架式设备；业务接口：≥8个千兆电口，≥12个万兆光口；网络层吞吐：≥16Gbps；最大并发连接数：≥500万；每秒最大新建http连接数：≥10万；三年硬件维保和规则库升级。

2.支持硬件一键重启功能。

3. 支持自动生成安全策略。可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率；

4.支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；

5.支持基于不同安全策略设定会话长连接老化时间；

6.支持多虚一部署；

7.支持将一台逻辑上的设备虚拟化成多个虚拟防火墙；

8.支持MPLS；

9.为保证业务连通性，设备支持CPU利用率过高时，自动停用部分应用层攻击防护功能；

10.支持配置回滚，并可对比回滚前后配置文件中的不同；

11.支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作；

12.访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式；

13.支持二层模式（透明模式）、三层模式（路由和NAT模式）和混合模式；支持链路聚合功能、接口状态同步功能；

14.支持静态路由、等价路由，支持RIP、RIPng；OSPFv2/v3动态路由协议；支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP或者目的IP进行连接数控制；

15. 配备病毒库、IPS库、APP库、URL库和WAF库，使防火墙本身具备病毒检测、入侵检测、上网行为管理、WEB应用防护等功能；

16.支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护；

17.支持SYN Flood、ICMP Flood、UDP Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测；

18.双机支持A/S，A/A方式部署，支持配置同步，会话同步和用户状态同步；

19.支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限；

20.支持对HTTP，FTP，SMTP，POP3协议进行病毒文件检测；

21.检测到病毒后的操作支持阻断，记录杀毒日志；

22.入侵防护漏洞规则特征库数量在6000条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞名称，危险等级，对应CVE编号；

23.支持对信任区域主机外发的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为；

24.支持应用识别及URL过滤功能，可识别3000种以上应用，支持URL重定向；

25.提供SQL注入攻击、XSS攻击的检测和防御功能，对Web服务系统提供保护。

26.设备应具备中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书EAL4证书》。

#### Web应用防火墙

1.产品架构：软硬一体化1U标准机架式设备；业务接口：≥8个千兆电口, ≥12个万兆光口（向下兼容千兆）；≥2个扩展槽；硬盘≥4TB；网络层吞吐：≥12Gbps；冗余电源；

2. 支持透明模式、代理模式、网关模式和旁路模式，且模式之间切换不需要重启设备或者检测引擎，可多种模式共同运营；

3. 支持对Web流量的镜像阻断功能，并且支持指定阻断报文发送接口；

4. 支持虚拟化技术，实现将一台物理设备虚拟成多个虚拟WAF

5. 支持对网站添加网站锁，只允许网站访问，禁止修改网站内容，防止网站被篡改，同时可以自行设定网站锁生效的时间；支持网站一键下线，上下线时间可自定义，通过对网站进行下线避免特殊时期被攻击

6. 支持对HTTP协议请求方法进行设置过滤，防止攻击者通过非业务需要的请求方法进行漏洞探测、信息收集等，支持设置的过滤方法包含Web服务器特定方法、RFC标准常用方法、RFC标准其他方法，支持的方法种类不得少于30种

7. 支持基于全局设定请求、响应头域字段名最大长度、头域字段值最大长度、是否禁止重复头域等角度进行设定，防止头域异常数据导致的服务器问题；支持HOST、Referer、User-Agent、Range、Accept、Accept-Charset、Content-Length、Content-Encoding等正规化规则设定，有效避免特定头域字段值不符合RFC标准规范要求，以及设定参数要求导致的服务器异常。

8. 支持对命令行注入、SQL注入、LDAP注入、XPATH注入、SSL注入、Mail注入、跨站脚本攻击、文件穿越、文件包含、Struts2漏洞等常见Web攻击进行防护，针对检测到的攻击可以进行告警、阻断、推送、重定向等动作，并且可以联动黑名单，黑名单生效时间可自定义；针对不同的攻击类型可以设置不同的处理动作，并且可以设置网页白名单不进行攻击检测（网页白名单支持精确到Host、URL、参数名称以及大小写），实现精细化的防护要求；

#### 外网端点安全管理软件

1.支持按攻击面维度统计并展示已知资产、互联网暴露面资产的攻击点，攻击点包括：未安装的高危补丁、开放的高危端口、存在的弱口令账号、连接的外设资产

2.支持以推荐措施的维度，展示针对系统内所有风险的推荐措施，措施信息包括：风险描述、处置措施步骤、受影响终端的统计与信息展示、受影响策略、推荐时间、所属类别

3.能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁；

4.对于恶意文件处理措施至少支持三种以上，包括厂家推荐措施、统一处理措施、以及针对不同类型病毒/恶意软件提供不同处理措施，同时不同病毒/恶意软件类型不少于5种分类，提供产品证明截图并加盖厂商公章；

5.为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时CPU占用比例，分高、中、低三个级别；

6.支持终端防火墙功能，可依据以下标准设定规则：远程IP、方向（出站\入站），协议（所有协议\ICMP\TCP\UDP\TCP+UDP）、端口；

7.具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新，提供产品证明截图并加盖厂商公章；

8.具备预测机器学习技术，可检测可疑进程中或来自可移动存储、Web邮件等各渠道的文件中的新兴未知安全风险威胁；

9.支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施；

10.本项目提供600点PC端授权。

11.为方便统一运维管控、快速响应，平台保留扩展能力，可基于数据和日志接口，可根据需求开放能力接口与第三方平台系统联动对接，如终端软件安装资产数据信息的对接，安全日志、告警信息的对接，提供产品证明截图并加盖厂商公章

#### 外网云主机安全产品

1.系统控制台支持横向扩容，支持多节点集群化部署，保证系统高可用性。控制台离线，客户端仍可进行安全防护

2.支持本地扫描和云扫描，支持实时扫描（文件落地即扫描）、预设扫描、手动扫描和快速扫描；如发现特殊情况 （如业务高峰期），可支持终止操作

3.支持扫描办公文件、压缩文件、Office宏病毒、文本文件等各种类型文件，支持配置扫描类型、文件大小、压缩层级、数量等参数

4.支持通过行为监控的方式，如检测可疑活动和未经授权的更改，防止勒索软件感染，并提供针对勒索软件事件专有历史纪录和勒索软件统计的监控组件

5.提供多种病毒的处理措施：包括不限于清除、删除、拒绝访问、隔离、不处理等，并针对不同的恶意软件类型，定制处理措施

6.支持和外部沙箱实现集成，同步沙箱的检测结果，检测未知威胁并处理，提供产品证明截图并加盖厂商公章

7.支持网络入侵攻击的防护，包含支持防护SQL注入,Cookie 注入，命令注入，跨站脚本(XSS)，跨站请求伪造(CSRF)，WebShell攻击防护等

8.通过流量检测技术，实现漏洞利用的攻击防护，支持操作系统、数据库、邮件服务、办公软件、中间件、Web应用、应用等类型的漏洞

9.支持0Day漏洞暴露后，快速定制入侵防御规则，包括不限于签名、特征码、XML等方式，进行0day的快速防护，同时可支持配置优先级、检测或阻止模式、严重性等，提供产品证明截图并加盖厂商公章

10.支持虚拟补丁规则自定义，虚拟补丁规则不少于 6000条，需显示补丁实际功能描述，提供产品证明截图并加盖厂商公章

11.外网云主机安全防护应支持弹性授权本项目提供外网3个节点超融合的安全防护，提供不少于300个虚拟机的安全防护能力，提供厂家声明函并加盖厂商公章

#### 网闸

1、产品架构:软硬一体化机架式设备，具备千兆电口≥6个，万兆光口≥2个，支持扩展槽≥1个；

2、整机吞吐量≥1Gbps，并发连接数≥20万，系统整体时延<0.1ns；

3、用于内外网安全隔离，隔断攻击行为，支持文件交换、数据库交换等安全能力；

4、支持图形化的系统运行状态；

5、支持主流数据库 0racle、SQL Server 等主流数据库；

6、文件同步支持FTP、SMB、NFS等文件传输协议，可以实现内网到外网、外网到内网、双向的文件传输；支持文件传输方向可控，实现单向或双向传输；

7、可以同时发送和接收一个关系数据库中的多个表；可分别定义增加、修改的数据传输；根据指定字段值进行条件传输；支持大字段数据同步交换包括BLOB、CLOB、Long等；

8、支持根据源IP、源端口、目的IP、目的端口自定义IEC规则；

9、支持对访问源地址、目的地址、源端口、目的端目、域名进行访问控制；

#### 内网外联防火墙

1.产品架构：软硬一体化1U标准机架式设备；业务接口：≥8个千兆电口，≥2个千兆光口；扩展槽≥2个；网络层吞吐：≥8Gbps；最大并发连接数：≥300万；每秒最大新建http连接数：≥7万；三年硬件维保和规则库升级。

2.支持硬件一键重启功能。

3. 支持自动生成安全策略。可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率；

4.支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；

5.支持基于不同安全策略设定会话长连接老化时间；

6.支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备；

7.支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的CPU和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙；

8.支持MPLS；

9.为保证业务连通性，设备支持CPU利用率过高时，自动停用部分应用层攻击防护功能；

10.支持配置回滚，并可对比回滚前后配置文件中的不同；

11.支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作；

12.设备应具备中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书EAL4证书》。

#### 安全管理区接入防火墙

1.产品架构：软硬一体化1U标准机架式设备；业务接口：≥8个千兆电口，≥2个千兆光口；扩展槽≥2个；网络层吞吐：≥8Gbps；最大并发连接数：≥300万；每秒最大新建http连接数：≥7万；三年硬件维保和规则库升级。

2.支持硬件一键重启。

3. 支持自动生成安全策略。可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率；

4.支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；

5.支持基于不同安全策略设定会话长连接老化时间；

6.支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备；

7.支持将一台逻辑上的设备虚拟化成多个虚拟防火墙；

8.支持MPLS；

9.为保证业务连通性，设备支持CPU利用率过高时，自动停用部分应用层攻击防护功能；

10.支持配置回滚，并可对比回滚前后配置文件中的不同；

11.支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作；

12.设备应具备中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书EAL4证书》。

#### 数据中心防火墙

1.产品架构：软硬一体化1U标准机架式设备；业务接口：≥8个千兆电口，≥2个千兆光口；扩展槽≥2个；网络层吞吐：≥8Gbps；最大并发连接数：≥300万；每秒最大新建http连接数：≥7万；三年硬件维保和规则库升级。

2.支持硬件一键重启功能。

3. 支持自动生成安全策略。可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率；

4.支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查；

5.支持基于不同安全策略设定会话长连接老化时间；

6.支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备；

7.支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的CPU和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙；

8.支持MPLS；

9.为保证业务连通性，设备支持CPU利用率过高时，自动停用部分应用层攻击防护功能；

10.支持配置回滚，并可对比回滚前后配置文件中的不同；

11.支持对安全策略进行冗余分析，并支持按不同时间段筛选未匹配的策略功能，且可以对其进行禁/启用或者删除操作；

12.设备应具备中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书EAL4证书》。

#### 内网端点安全管理软件

1.支持按攻击面维度统计并展示已知资产、互联网暴露面资产的攻击点，攻击点包括：未安装的高危补丁、开放的高危端口、存在的弱口令账号、连接的外设资产

2.支持以推荐措施的维度，展示针对系统内所有风险的推荐措施，措施信息包括：风险描述、处置措施步骤、受影响终端的统计与信息展示、受影响策略、推荐时间、所属类别

3.能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁；

4.对于恶意文件处理措施至少支持三种以上，包括厂家推荐措施、统一处理措施、以及针对不同类型病毒/恶意软件提供不同处理措施，同时不同病毒/恶意软件类型不少于5种分类，提供产品证明截图并加盖厂商公章；

5.为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时CPU占用比例，分高、中、低三个级别；

6.支持终端防火墙功能，可依据以下标准设定规则：远程IP、方向（出站\入站），协议（所有协议\ICMP\TCP\UDP\TCP+UDP）、端口；

7.具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新，提供产品证明截图并加盖厂商公章；

8.具备预测机器学习技术，可检测可疑进程中或来自可移动存储、Web邮件等各渠道的文件中的新兴未知安全风险威胁；

9.支持检测全局可疑站点（C&C)识别，监控可疑站点的连接，并提供记录或者阻止的处理措施；

10.本项目提供600点PC端授权

11.为方便统一运维管控、快速响应，平台保留扩展能力，可基于数据和日志接口，可根据需求开放能力接口与第三方平台系统联动对接，如终端软件安装资产数据信息的对接，安全日志、告警信息的对接，提供产品证明截图并加盖厂商公章

#### 内网云主机安全产品

1.系统控制台支持横向扩容，支持多节点集群化部署，保证系统高可用性。控制台离线，客户端仍可进行安全防护

2.支持本地扫描和云扫描，支持实时扫描（文件落地即扫描）、预设扫描、手动扫描和快速扫描；如发现特殊情况 （如业务高峰期），可支持终止操作

3.支持扫描办公文件、压缩文件、Office宏病毒、文本文件等各种类型文件，支持配置扫描类型、文件大小、压缩层级、数量等参数

4.支持通过行为监控的方式，如检测可疑活动和未经授权的更改，防止勒索软件感染，并提供针对勒索软件事件专有历史纪录和勒索软件统计的监控组件

5.提供多种病毒的处理措施：包括不限于清除、删除、拒绝访问、隔离、不处理等，并针对不同的恶意软件类型，定制处理措施

6.支持和外部沙箱实现集成，同步沙箱的检测结果，检测未知威胁并处理，提供产品证明截图并加盖厂商公章

7.支持网络入侵攻击的防护，包含支持防护SQL注入,Cookie 注入，命令注入，跨站脚本(XSS)，跨站请求伪造(CSRF)，WebShell攻击防护等

8.通过流量检测技术，实现漏洞利用的攻击防护，支持操作系统、数据库、邮件服务、办公软件、中间件、Web应用、应用等类型的漏洞

9.支持0Day漏洞暴露后，快速定制入侵防御规则，包括不限于签名、特征码、XML等方式，进行0day的快速防护，同时可支持配置优先级、检测或阻止模式、严重性等，提供产品证明截图并加盖厂商公章；

10.支持虚拟补丁规则自定义，需显示补丁实际功能描述，提供产品证明截图并加盖厂商公章；

11.内网云主机安全防护应支持弹性授权本项目提供内网40个CPU虚拟化的安全防护，提供不少于1000个虚拟机的安全防护能力，提供厂家声明函并加盖厂商公章；

#### 内网准入控制系统

1.产品架构：软硬一体化1U标准机架式设备；业务接口≥8个千兆电口，≥12个万兆光口；支持管理的最大设备数量≥1000个；

2.设备本身不能出现对视频业务产生如视频抖动、卡顿等现象，基于SIP的视/音频传输时延＜20微秒;

3.支持与GB 35114 C级平台互联，通过公安部安全与警用电子产品质量检测中心的委托测试;

4.设备满足GA/T 1788.3要求，达到视频接入安全防护系统增强II级防护要求，和设备准入控制系统防护要求，提供检测报告复印件并加盖原厂公章。

5.支持MAC认证功能，MAC地址在白名单中的终端能够通过设备进行正常访问，MAC地址不在设备白名单中的终端通讯会被阻断；支持IP认证功能，IP地址在白名单中的终端能够通过设备进行正常访问，IP地址不在设备白名单中的终端通讯会被阻断。

6.支持符合GB/T 28181标准协议接入网络的终端进行通信，采用非GB/T 28181标准协议接入网络进行通信的终端会被系统阻断并产生告警日志。

7.支持基于Portal认证的实名制违规外联检测机制，基于portal认证入网的设备，存在违规外联行为的终端，通讯会被阻断；支持无感知方式的违规外联检测机制，存在违规外联行为的终端，通讯会被阻断；

8.支持DDoS攻击防护功能，提供权威机构检测报告复印件并加盖原厂公章证明；

9.支持基于终端和服务器的双向认证功能，提供权威机构检测报告复印件并加盖原厂公章证明；

10.支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断。

#### 日志审计

1.产品架构：软硬一体化1U标准机架式设备；内存≥8G，硬盘≥2T，接口数量：≥6个千兆电口，单电源，配置55个日志源；平均处理能力（每秒日志解析能力EPS）≥2000 EPS

2.支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等

3.支持监测目标主机的CPU利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息。

4.根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义；基于角色的权限管理机制，通过角色定义支持多用户访问

#### 堡垒机

1.产品架构：软硬一体化1U标准机架式设备，接口数量：千兆业务电口≥6个；最大并发：最大字符连接≥110个，最大图型连接≥25个，授权资产数同时并发量≥100个；CPU≥4核；内存≥8G；硬盘容量≥2T；单电源；配置三年硬件维保和软件升级

2.部署方式：支持逻辑串联、物理旁路部署模式，对现有网络架构无影响，支持多网卡绑定冗余，增强网络连通健壮性

3.支持主机类型：支持Windows主机、Unix主机、Linux主机、网络设备、安全设备

4.支持数据库类型：支持Oracle、SQL Server、MySQL、DB2、Sybase、Informix、达梦数据库

5.支持同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。（需提供相关截图或检测报告或证书等相关证明材料）

6.会话协同功能支持在运维界面实时查看协同人员，可由会话发起人在线进行操控权分配，可实时踢出会话协同人员；会话协同人员可主动申请当前会话操控权，待会话发起者同意后可拥有会话操作权。（需提供相关截图或检测报告或证书等相关证明材料）

#### 漏洞扫描系统

1.产品架构：软硬一体化标准机架式设备，配置三年硬件维保和软件升级

2. 资产类别包括：操作系统、网站、数据库、中间件、网络设备、安全设备、网络打印机、虚拟化设备等

3. 支持空间资产探测、系统漏洞扫描、等保合规评估等

4、检测信息系统中存在的各种脆弱性问题

#### 移动终端安全检测系统

1、支持对安卓系统、鸿蒙系统手机、pad等移动终端系统安全检测：检测内容至少包括是否被ROOT，以及手机、pad等移动终端设备的基本信息。

2、支持对安卓、鸿蒙手机、pad等移动终端进行恶意样本检测，可以对手机、pad等移动终端上已安装应用、未安装应用进行恶意性检测，精准识别各类木马、蠕虫以及恶意仿冒样本；

3、支持对安卓、鸿蒙手机、pad等移动终端进行可疑应用检测，可以结合高级威胁特征有效检出针对性植入应用，避免被监听和隐私窃取；

4、支持对安卓、鸿蒙手机、pad等移动终端进行敏感应用检测，发现已安装应用中是否存在翻墙、反动、工具、通讯、涉黄、涉赌、涉贷、诈骗、交友、虚拟货币、摄像监控、境外党政类应用；

5、支持对安卓、鸿蒙手机、pad等移动终端进行违规应用检测，发现已安装应用是否为违规收集使用个人信息的应用；

6、支持对安卓、鸿蒙手机、pad等移动终端进行黑名单应用检测，检测装机列表中是否存在用户定义的黑名单应用；

7、支持对安卓、鸿蒙手机、pad等移动终端进行已卸载应用检测，发现手机、pad等移动终端安装过但已卸载的应用信息；

8、支持对安卓、鸿蒙手机、pad等移动终端已安装应用进行供应链威胁分析，列出存在威胁SDK的风险应用；

9、支持检测敏感字配置：系统基于实际检测场景提供多种检测类型模板，包括涉军、涉赌、涉黄、涉贷、涉邪教、心理异常等，同时支持自主设置敏感字进行检测，可以根据需要启用相关模板或者敏感字进行敏感内容检测；

10、支持安卓、鸿蒙、苹果手机、pad等移动终端敏感聊天内容检测，通过配置的敏感字对手机、pad等移动终端QQ\微信聊天内容进行扫描匹配，可以获取敏感内容的来源账号、实际内容、发送方、接收方、发送时间等；

11、支持安卓、鸿蒙、苹果手机、pad等移动终端敏感文件检测，可以通过自定义敏感词及类型，对手机、pad等移动终端内的Word、Excel、PDF、TXT、PPT、Zip、RAR、7-Zip格式文档进行全盘扫描，扫描范围涵盖文件名和文件内容，支持提取出文档的路径、文件名等信息；

12、支持安卓、鸿蒙、苹果手机、pad等移动终端敏感图片检测，支持带有敏感词的截图、拍照、系统图片识别和检出，支持可疑图片、红头文件等敏感图片识别检测；可以识别相关图片路径以及匹配识别项；

13、支持安卓、鸿蒙、苹果手机、pad等移动终端敏感微信群、QQ群检测，可以针对群名称进行扫描检测，发现涉敏聊天群，并在检测结果中展示；

14、支持敏感内容清理，系统检测出的敏感聊天内容、敏感文件以及敏感图片，支持路径定位，用户可以删除所有相关敏感内容，保障信息安全；

15、支持检测记录及相关信息清理，针对设备的检测记录以及检测结果，用户可以进行彻底删除，实现无痕检测；

16、对于检出的恶意样本，能够进行导出和一键卸载；

17、具备检测数据统计能力：至少包括检测设备连接的总体统计，以及每条手机、pad等移动终端安全检测的详细内容；

18、支持自动生成检查报告，可以导出为PDF格式或者excel检测报告。

19、支持检测设备及系统恢复出厂设置；

20、支持离线或者在线更新知识库版本、病毒库版本以及系统版本；

21、对接入终端数量无限制。

#### 数据库安全审计系统

1.基础配置：标准机架设备，16G内存，1T硬盘，板载6G电口，具备1扩展槽，扩展槽扩展接口可选，最大吞吐量3000条SQL/秒，默认支持10个数据库实例审计。

2.部署方式：支持不改变原有网络结构的旁路镜像部署；支持探针部署，采集服务器和虚拟环境下流量；支持丰富的探针参数，包括IP地址过滤、服务器和探针的CPU占用率、内存占用率、本地缓存大小等灵活配置。

3.兼容性：支持国际主流数据库；支持国产数据库；非关系型数据库；支持主流的数据库工具。

4.数据库自动发现：支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址等信息，并且自动添加到审计范围，无需用户提供网段、数据库地址等信息。

6.漏洞攻击审计：支持对利用数据库漏洞实现攻击的行为进行审计。支持数据库漏洞攻击行为监听，内置数据库漏洞规则库，覆盖Oracle、SQLServer、Mysql、DB2、Sybase、DM等多种数据库类型；漏洞规则应显示漏洞名称、漏洞类型、CVE标示、CNNVD标示、漏洞影响范围，提供界面截图并加盖厂商公章。

7.支持告警与规则关联，实现不同规则的告警发送给不同收件人，方便进行风险的排查。

8.报表与告警：提供自定义报表功能；告警方式告警方式包括：邮件、短信、SYSLOG、SNMP等，提供界面截图并加盖厂商公章。

11.数据备份：日志备份与恢复管理，支持审计日志数据的备份与恢复，支持自动备份，支持的备份服务器类型至少包含FTP、SFTP方式，备份记录可以查询。

#### 数据脱敏系统

1.基本配置：专用机架设备，2GE板载管理口，4GE板载接口。16GB内存，2TB硬盘。

2.支持对Excel、CSV、DEL、TXT文件脱敏：支持无中间数据库情况下脱敏dmp文件：支持对DICOM(医学影像)文件脱敏；提供界面截图并加盖厂商公章。

3.脱敏方式：系统支持自定义、图形化操作的脱敏规则和脱敏方式，支持UNICODE标准、中文等字符编码。支持数据库到数据库、数据库到文件、文件到文件、文件到数据库等多种脱敏方式。系统支持异构脱敏，提供界面截图并加盖厂商公章。

4.敏感数据发现：系统应支持敏感信息的自动发现能力，系统具有内置敏感数据特征库，能对身份证、通用证件号、银行卡号、电话号码（手机、座机）、中文姓名、中文地址、企业名称、日期、email地址、金额、ip地址、mac地址、车牌号、车架号、军官证、港澳通行证、回乡证敏感信息自动识别。系统能读取数据库或txt、csv等文件内容，根据内容和内置敏感数据特征规则发现敏感数据；提供界面截图并加盖厂商公章。

5.数据脱敏功能：使用相同含义的数据替换原有的敏感数据，如姓名脱敏后仍然为有意义的姓名，住址脱敏后仍然为住址。将原数据中部分或全部内容，用“\*”或“#”等字符进行替换，遮盖部分或全部原文。

6.至少支持一种国密算法，可以对字段进行加密处理，提供界面截图并加盖厂商公章。

7.数据管理；系统不允许真实生产数据落地，不能存储生产数据；并提供审计报告，包括用户信息、脱敏配置信息、任务信息等。

#### 整体配置清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **单位** |
| 1 | 防火墙 | 2 | 台 |
| 2 | Web应用防火墙 | 1 | 台 |
| 3 | 外网端点安全管理软件 | 1 | 套 |
| 4 | 外网云主机安全产品 | 1 | 套 |
| 5 | 网闸 | 1 | 台 |
| 6 | 内网外联防火墙 | 2 | 台 |
| 7 | 安全管理区接入防火墙 | 2 | 台 |
| 8 | 数据中心防火墙 | 2 | 台 |
| 9 | 内网端点安全管理软件 | 1 | 套 |
| 10 | 内网云主机安全产品 | 1 | 套 |
| 11 | 内网准入控制系统 | 1 | 台 |
| 12 | 日志审计 | 1 | 台 |
| 13 | 堡垒机 | 1 | 台 |
| 14 | 漏洞扫描系统 | 1 | 台 |
| 15 | 移动终端安全检测系统 | 1 | 台 |
| 16 | 数据库安全审计系统 | 1 | 台 |
| 17 | 数据脱敏系统 | 1 | 台 |
| 18 | 辅材 | 1 | 宗 |
| 19 | 施工费 | 1 | 项 |

### 商务要求

#### 培训要求

采购人认为培训是保证项目成功的一个重要手段，因此为了保证系统顺利完成，投标人需要准备一份完整的培训计划，对采购人各类人员进行相关的培训，包括现场培训和集中培训等多种方式，培训的内容、次数和方式由采购人提出，采购人仅负责提供培训场地、培训电脑和培训人员的召集，培训环境的搭建、培训文档的准备、培训的实施、培训人员的考核等由投标人负责。对与本项目的相关技术，投标人也需要提供必要的手段保证能够将其传授与采购人。与培训相关的费用，投标人应当一并计算在投标报价中。

投标人派出的培训教员应具备丰富的相同课程教学经验，所有的培训教员必须中文授课，供应商必须为所有被培训人员免费提供培训用文字资料和讲义（电子版和纸张版）等相关用品。提供下列几个方面的培训：

（1）硬件、软件的用户使用培训，应用软件操作培训；

（2）系统管理培训、甲方技术人员维护排错培训；

（3）系统疑难问题解答；

投标人应按采购人约定合理地安排培训时间。

培训对象包括初级技术人员培训、高级技术人员培训和甲方推荐的医护人员操作培训。初级培训可使得系统维护人员能够顺利地完成日常的维护工作，保证系统的正常运行。高级培训应使得高级技术人员对本业务支撑系统的运行机制有着清晰明确的认识，并能够高效及时地解决系统突发运行故障。

#### 项目实施

模块的上线可根据医院具体部门的需求、按照整体规划，分步实施的原则上线，投标方案中所描述的功能和实施方案是在充分了解银丰（济南）医院整体信息化建设情况后给出的方案说明，除特别说明外所报价格应包含了所有投标方案中描述的功能，且产品支持无限量并发用户数。

（1）项目工期、实施要求

合同签订后立即组织驻场施工，投标人需结合我院2024年9月1日开业的要求，拟定详细的系统实施计划，含客户化修改、测试、试运行、培训及上线计划，保证在合同规定时间内上线及上线系统的基本平稳。

（2）人员要求

在项目实施阶段应保证至少3个工程师到医院现场实施；医院开业后一个月内，应保证至少2个工程师在医院现场实施；项目负责人一经确定，未经院方同意不得更换。项目负责人需通过医院相关主管的考核。实施人员需提供简历并通过甲方面试。

（3）建设范围

自建医院以及若干签约入驻医院。

#### 项目验收

硬件系统正式投入运行3个月后进行系统验收，验收人员由我院相关人员与投标人相关人员共同组成，验收结果双方主管人员签字认可。

项目验收需满足如下条件：

（1）满足招标文件及合同签订的相关要求；

（2）保障上线产品（软件、硬件）的质量及技术参数要求；

（3）保障上线系统的基本平稳及正常运行；

#### 服务要求

投标人所提供技术支持方案及保证措施，包括本地化、售后服务、服务期限、响应时间、操作维护人员提供的培训计划的优劣。

质保期（保修期）：

自招标人整包最终验收合格之日起，项目整体原厂质保 3 年。签订合同后，提供针对本项目的原厂服务承诺函原件。

包装和运输要求：

投标人需针对不同的产品提出包装、运输和装卸方案，确保运输和装卸过程中产品质量完好。

安装调试要求：

（1）投标人需根据本项目特点，制定安装调试方案，详细描述安装人员配备、安装、调试时间及标准、注意事项等，确保安装调试顺利实施。

（2）投标人在货物运抵现场前，向招标人提供安装进度计划表及需招标人配合的事项。

（3）安装施工过程中，应事先通知招标人，经同意后再进行安装。

（4）投标人在制作、运输、安装、布线及调试过程中，应严格按照国家有关的操作规程和施工规范进行作业，确保安装牢固，安全可靠。

（5）投标人在制作运输安装过程中，应加强作业现场管理，保持整洁有序，不得破坏环境，否则由投标人负全责。

（6）投标人必须加强制作、运输及安装施工过程中的安全防护，在此过程中，如因投标人原因导致的双方及第三方的任何人身、设备安全事故及财产损失均由投标人负全责。

（7）投标人应送货上门、安装，并提供咨询服务，费用包含在报价中。

人员配置：

（1）安装阶段：项目经理需具有丰富的相关案例实施经验，项目实施期间及招标人后续各个业务系统上线调试期间，需在招标人指定地点配合其他软硬件设备测试及整体联调工作。其他人员请各投标人根据项目情况，自行配备。

（2）质保期（售后服务）服务阶段：投标人需免费配备至少一名经验丰富的专业技术人员（需经过甲方面试通过）进行医院驻场服务，负责所供产品的日常巡检、维护，处理日常问题，配合医院进行业务系统上线及其它相关工作。

质保期售后服务：

（1）服务期三年内提供 7\*24 小时响应，服务热线电话响应时间为立即响应，电话中可以解决的问题通过电话咨询即可解决，如不能通过电话方式解决的，须提供现场支持。服务费综合考虑到报价中，质保期外上门服务仅收取更换零部件的成本费。

（2）驻场技术人员不能解决的问题，可解决问题的厂家技术人员应在 4 个小时内到达现场处理。

（3）投标人需在质保期内，配合甲方完成等保测评相关工作。

#### 报价要求

项目报价中，投标人需针对 “自建医院”作为主体项目进行产品与服务报价。

## 附件二 项目招标评价表

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **评分内容** | **评分标准** | **分值范围** |
| 价格分  （90分） | 项目报价 | 价格分统一采用所有合格投标人的最低价格作为基准价，其价格分为满分90分。投标人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）×90％×100（如投标报价低于基准价，则为满分） | 0-90分 |
| 技术分  （10分） | 产品参数响应 | 由评委根据各投标产品的整体性能、功能、配置情况、技术性能及经济性、先进性，对于招标参数中的技术参数不满足项每项扣1分，最多扣7分。（本标书所有参数需求方保留投标后测试的权力，如需求方认为投标人及投标产品有虚假应答的嫌疑，则需求方有权力要求投标人及投标产品厂商提供相应的设备进行测试，如测试不通过，则判定为投标人及投标产品厂商虚假应答，没收投标保证金） | 0-7分 |
| 实施方案 | 根据投标人提供针对本项目的项目管理方案、实施计划、质量保障措施合理、完善得1分；针对本项目的项目管理方案、实施计划、质量保障措施较合理、较完善0.5分；内容与采购要求不符或未提供的不得分。 | 0-1分 |
| 售后方案 | 投标人对具体售后服务方案完整明确、维护响应时间快速及时、服务承诺有效到位以及技术人员安排科学合理得1分，对具体售后服务方案较明确、维护响应时间较长、服务承诺比较到位以及技术人员安排比较合理得0.5分；内容与采购要求不符或未提供的不得分。 | 0-1分 |
| 本地化服务能力 | 由于医院业务的特殊性，要求投标人在山东省具备一定的服务能力：  具备15人或以上的服务团队，得1分。  具备5-15人的服务团队，得0.5分。  无服务团队得0分。  评审说明:提供本单位服务团队在山东省缴纳社保的证明材料（前六个月任意2个月的社保缴纳记录与凭证）。 | 0-1分 |