**浙江中医药大学附属第三医院**

竞争性磋商文件

招标编号：**ZSYYCGZX20250903**

 招标项目：数据中心和网络安全维保服务项目

投标单位：

 投标日期：

**第一章 投标概况**

 根据浙中医大三院医院采购管理文件的要求,对**数据中心和网络安全维保服务项目**进行竞争性磋商。投标单位在投标之前必须认真阅读本磋商文件的说明、表格、条件及规范等所有内容，投标方因未能遵循此要求而造成的对本磋商文件所要求投标方提供的任何资料、信息、数据的遗漏或任何非针对磋商文件要求项目的报价，均须自担风险并承担可能导致其投标文件被招标方拒绝的后果。

1. 项目编号: **ZSYYCGZX20250903**
2. 采购方式：院内竞争性磋商
3. 采购内容：浙江中医药大学附属第三医院数据中心和网络安全维保服务项目项目预算：**预算17万元**
4. 投标单位的资格要求：见第二章
5. 投标时间和地点：

投标单位应于**2025年9月25日8：30**前将投标文件密封交到投标现场。

1. 投标地点：杭州市武林巷2号浙江中医药大学附属第三医院行政楼3楼会议室
2. 开标时间：**2025年9月25日9：00（周四上午）**
3. 开标地点：浙江中医药大学附属第三医院行政区三楼会议室（武林巷二号）
4. 联系地址和电话：

杭州市莫干山路219号浙江中医药大学附属第三医院采购中心

联系人:黄老师

联系电话：0571—88393587

**第二章 投标单位须知**

1. 符合《中华人民共和国政府采购法》第二十二条要求,能承担本项目的供应商。
2. 未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、税收违法黑名单、政府采购严重违法失信行为记录名单。
3. 本项目不接受联合体投标。
4. 该行业国家规定必备的资质、资格。

注：多家供应商参加本项目投标，如其中两家或两家以上供应商的法定代表为同一人或相互之间存在投资关系且达到控股，应当按一个供应商认定。

**五、响应情况**

采购文件中凡标注“▲”的条款均为实质性要求，不响应的投标文件将作无效标处理。

采购文件中凡标注“★”的条款为重要参数要求，根据响应情况进行评分处理。

**第三章 采购内容及需求**

**一、采购清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 采购项 | 描述 | 数量 | 金额 |
| 1 | 网络及安全运维项目 | 鉴于医院网络系统与数据信息的高安全性、高稳定性要求，本次项目涵盖机房运维服务、安全运营服务及数据安全服务。 | 1年 | 17万元 |

**二、详细服务清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务项** | **服务内容** | **服务频次** |
| 1 | 机房运维服务 | 设备维保服务 | 1年 |
| 资产梳理服务 | 1年 |
| 备品备件服务 | 按需提供 |
| 应急故障处理服务 | 按需提供 |
| 定期巡检服务 | 4次/年 |
| 虚拟化平台维护服务 | 1年 |
| 2 | 安全运营服务 | 安全日志分析与响应服务 | 12次/年 |
| 漏洞扫描服务 | 4次/年 |
| 基线核查服务 | 按需提供 |
| 渗透测试服务 | 4次/年 |
| 漏洞攻击防护服务 | 1年 |
| 主动安全防护服务 | 1年 |
| 安全威胁分析联动服务 | 1年 |
| 新系统上线评估服务 | 按需提供 |
| 应急演练服务 | 按需提供 |
| 重保值守响应服务 | 按需提供 |
| 应急响应服务 | 按需提供 |
| 安全培训服务 | 1次/年 |
| 3 | 数据安全服务 | 管理制度建设服务 | 1次/年 |
| 数据安全巡检服务 | 4次/年 |
| 数据安全自检服务 | 1次/年 |
| 测评审查支撑（迎检）服务 | 1次/年 |
| 数据安全培训 | 1次/年 |

**三、服务要求**

**（一）机房运维服务**

**（1）设备维保服务**

**服务器设备维保清单：**

服务器20台，具体清单请现场调研。

**存储设备维保清单：**

存储设备8台，具体清单请现场调研。

**（2）资产梳理服务**

梳理医院现有资产，协助落实设备资产管理，监督并保证设备使用记录完整准确，协助资产使用情况登记并进行拓扑展示。为后续简化运维、缩短运维响应时间，提供运维效率提供帮助，主要内如包括：

告警分析与通知：结合专业运维人员的经验及多种排查工具智能分析关联设备告警信息，缩小故障根源范围，帮助快速定位故障根源，并提供可行的故障解决方案，帮助用户快速解决异常，维护业务平稳运行。

配置文件管理：运维人员通过配置对比、合规性检查记录设备全量配置操作日志，实现对全网设备配置文件的统一管理和备份，全面提升配置效率、质量和安全性。

机房及布线管理：提供机房、弱电井综合布线理线服务，同时协助实现横纵向布线信息的统一有序管理，查询更便捷；联动IT资源监控数据，帮助用户全面掌握机房、管井、布线等哑资源的使用情况。

**（3）备品备件服务**

服务期间，若服务范围内核心物理设备出现故障且短时间内时间无法恢复的情况，及时提供备品备件优先恢复业务运行，将损失降到最低，直至设备修复完成。

**（4）应急故障处理服务**

接到用户方故障呼叫后，及时派相关认证工程师做现场服务，现场服务次数和时间不限。

1.对于严重故障(影响用户方业务正常运作的故障)，派遣工程师到现场做技术支持。响应时间:15分钟以内；到场时间:接到故障通知后，2小时内到达现场；修复时间:到达用户现场后，4小时内恢复。

2.对于一般性故障(不影响用户方业务正常运作的故障)，派遣工程师到现场做技术支持。响应时间:15分钟以内；到场时间:接到故障通知后，4小时内到达现场；修复时间:到达用户现场后，8小时内恢复。

**（5）定期巡检服务**

**网络及安全设备巡检维护**

服务期限内，每季度对数据中心机房核心网络设备包括交换机、路由器等设备进行巡检，根据巡检结果中发现的不合理或异常情况进行优化。

网络/安全设备主要涉及部件：

系统主板

接口卡和模块

电源和电源线

所有连接设备的LED指示灯和各种连接线缆等。

数通/安全设备维护主要巡检维护内容：

1、检查主机运行状态：对系统I/O状态、设置、日志文件、ErrorReport进行检查分析，清理系统中多余的垃圾文件；

2、检查设备端口的可用性：对以太网接口、光纤接口及光电转、FC光纤模块等进行重点检查；检查设备LED状态灯；

3、检查所有设备的连接件，包括CABLE、电源插座、模块等可能容易导致设备连接出现问题的敏感部件是否处于Available状态；

4、环境检查优化，包括电源电压、接地和室内温度、湿度、空气洁净度，及零地电压、零火电压等等；

5、核心设备性能测试：①功能测试：接口/设备/管理/业务/设备可靠性/设备功率/后台管理/系统恢复时间；②二层性能测试：吞吐量/突发长度/过负荷/转发速率/地址缓存能力/时延/时延抖动/丢包率；③三层性能测试：吞吐量/突发长度/过负荷/转发速率/时延/时延抖动/丢包率/QOS/路由表容量/协议性能/转发附加；④其他。

**服务器存储设备巡检维护**

服务期限内，每季度对数据中心机房核心IT业务资产包括服务器、存储、备份一体机等设备进行巡检，根据巡检结果中发现的不合理或异常情况进行优化。

服务器/存储/备份主要涉及部件：

主机的系统主板

CPU(含CPU板）

内存条或内存板

内置磁盘和外置移动硬盘

各种适配器卡和模块（包括以太网卡、HBA卡、光纤模块）

显示器或终端

各种内置与外置存储设备，包括磁盘阵列、磁带库、光盘库等

磁盘阵列控制器

磁盘阵列硬盘

SAN交换机和SFP短波模块

服务器/存储的电源和电源线

所有连接设备的LED指示灯和各种连接线缆等。

服务器/存储/备份设备维护主要巡检维护内容：

1、检查服务器主机运行状态：对系统CPU、内存、I/O状态、进程等检查；对系统设置、日志文件、ErrorReport进行检查分析，清理系统中过时的日志文件和垃圾文件；磁盘空间使用情况检查，要求已经使用空间在80%以下，并且至少有12MB以上的剩余空间；

2、检查服务器和存储等外部设备可用性：对磁盘阵列、磁带机、外置光驱、维护终端等的状态、设置进行检查；对风扇、后备电池、磁盘、磁带、键盘等敏感部件进行重点检查；检查设备LED状态灯；查看SAN交换机的ZONE配置信息/交换机状态/风扇状态/电源状态/温度状态/级联状况；

3、检查所有服务器、存储和SAN交换机的连接件，包括接口、CABLE、电源插座等可能容易导致设备连接出现问题的敏感部件；检查连接适配卡状态（包括SCSI卡、网卡、HBA卡以及光纤模块等）是否处于Available状态；

4、环境检查，包括电源电压、接地和室内温度、湿度、空气洁净度，及零地电压、零火电压等等；

5、服务器性能测试：功能测试：可扩展性（硬盘、PCI槽以及内存等扩展能力）/可用性（对热插拔及硬盘、电源、风扇、网卡等冗余设备的支持）/可管理性（随机所带管理软件）；

6、磁盘阵列安全性测试：安全性测试：电源/风扇/硬盘热插拨/硬盘故障；数据备份与恢复测试；

7、备份一体机性能测试：测试同步数据变化；测试数据增量变化；测试实际环境异常情况。

8、检查系统ERRORLOG并进行记录、分析，实施故障诊断：是否存在永久性不可恢复的硬件错误；读取root邮件等,检查是否有需要处理的部件故障；

9、检查数据备份情况，分析备份策略实用性；

10、存储间同步镜像数据的检查、数据同步情况分析；

11、硬件健康状态检查；

12、协助用户机房管理人员分析和日常设备运行中出现的未解决问题并提供建议。

**（6）虚拟化平台维护服务**

提供虚拟机的日常管理工作，包括虚拟机模板安装、虚拟机配置修改、虚拟机故障处理对于服务范围内的系统软件、应用软件提供版本管理和升级服务。对于发布的相关软件最新版本，与医院信息中心一起做好升级工作。若原厂商发布新的系统软件版本或补丁升级程序，提供系统软件版本和补丁测试，以及软件版本和补丁的升级实施服务。

**虚拟化平台日常运维：**

1、服务包括7×24电话服务和现场技术支持服务。

2、对虚拟化平台进行定期日志巡检、资源分配巡检、配置检查。针对不合理配置项提出调整建议，尽可能避免因配置不当造成的系统宕机及数据丢失风险。

3、虚拟化升级服务：按照用户要求对虚拟化系统进行升级（包括补丁安装及软件版本升级），升级前提供完整的升级计划及方案，说明需要停机的时间等，并配合用户进行系统升级完成后的测试、提交系统升级实施报告和测试报告等。

4、虚拟化调优服务：对运行的虚拟机进行整体分析，对占用资源较多的虚拟机进行优化，对长期不使用的虚拟机镜像资源重组再利用，对使用频繁的虚拟机进行合理化的调整。

5、虚拟化架构调整服务：分析虚拟化的整体架构，对于单链路、单主机等情况的架构部署为冗余配置，对于虚拟化后端存储配置不合理的，进行适当调整，提出建议及整改措施。

6、将院区内所有服务器及虚拟化、超融合平台进行资产梳理，并配合完成虚拟化平台新增扩容的安装部署和定期的虚拟机备份工作。

**虚拟机迁移及维护：**

特殊时期如业务系统迁移、硬件故障、机房搬迁等，提供虚拟机的迁移服务，包括虚拟机迁移至虚拟机、物理机迁移至虚拟机等，迁移前提供详细的迁移步骤、方案、应急处置措施和回退机制，保证用户数据不丢失和数据完整可用。

**日常故障处理：**

硬件维护：服务器随着业务的不断增长，对硬件资源不足问题或者出现存储硬件告警需要停机维护。首先做好虚拟机的备份工作：

在有条件的情况下可以将业务虚机迁移到集群中其他服务器主机上，再将故障服务器切换至维护模式并从HA集群中移除再进行更换操作。

软件维护：虚拟机定期快照和备份，一旦系统崩溃，则立即恢复虚拟机。

**（二）安全运营服务**

**（1）安全日志分析与响应服务**

**期限频率：**12次/年。

**服务范围：**全部网络安全管控设备，包括信息系统相关威胁感知设备、防火墙设备、应用安全设备等。

**服务内容：**提供高级安全专家服务，按季度为用户提供：

在现有信息化安全设备大量异构的情况下，梳理安全资产、收集安全设备日志、审查安全策略、评估外部威胁、精准入侵检查、事件溯源分析，通过部署统一安全威胁可视化系统，联动各安全设备，实现封禁和溯源威胁面的目标，同时提供高级安全专家进行事件处置、调优策略，并出具安全加固建议。

（一）安全威胁分析：结合安全感知日志和威胁情报进行深度分析，研判网络中存在的威胁和攻击行为，明确对业务的影响和危害

1.外部威胁评估：综合分析数据，发现攻击威胁、持续性攻击和高级黑客等安全事件；

2.精准入侵检查：webshell检查、恶意文件查杀、web日志分析、系统状态分析，发现已经被入侵或感染的主机；

3.位置威胁发现：及时对未公开威胁进行评估、针对高危威胁风险进行通告。未知威胁快速规避措施：通过安全策略的运营（例：自定义策略临时防护）临时应对、规避最新爆发的风险。安全功能迭代升级（例：更新规则库、升级安全组件）将防护能力整合到安全设备。

（二）安全事件处置：对安全事件进行处置，清除恶意文件、快速恢复业务；

1.策略管理：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新。策略冲突、策略有效性调优服务。

2.攻击对抗：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。通过全网大数据分析，发现有境外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为。

3.事件分析与处置：对用户上报的安全事件进行及时响应。实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助客户快速恢复业务，消除或减轻影响。

（三）事件溯源分析：深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径；

1.入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。

2.入侵威胁清除：排查攻击路径，恶意文件清除。

3.入侵原因分析：还原攻击路径，分析入侵事件原因。

（四）安全加固建议：根据事件发生的根因、影响范围，针对性给出安全加固建议。

**输出物：**《安全日志分析与响应报告》。

**（2）漏洞扫描服务**

数据库、操作系统及中间件作为信息系统的核心组件，其安全性直接关系到整个系统的稳定运行和数据安全。因此，本服务旨在通过专业的安全服务工程师对数据库、操作系统及中间件进行漏洞、端口、弱口令检测，发现潜在的安全风险，并提出整改建议，协助开发人员整改，以提高网络安全性。

**服务频次：**4次/年

**服务内容：**（一）漏洞扫描与检测

使用系统漏洞扫描工具对数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描。

利用专业级WEB应用扫描工具对被评估对象进行应用检测，以发现网站应用层面可能存在的技术漏洞；包括WEB容器识别，如：Apache、tomcat、Weblogic、WebSphere和Ngix等；支持多种服务端语言探测，如：PHP、JSP、ASP、ASPX和.NET等；支持WEB前端框架探测，如：jQuery、Bootstrap、HTML5等；支持WEB后端开发框架探测，如：Django、Rails、ThinkPHP、Struts等； 支持WEB业务应用探测，如：BBS、CMS和BLOG等（备注：逻辑类漏洞主要通过人工渗透测试完成）支持扫描对象包括：B/S架构类应用漏洞，主要包括：SQL注入、XSS跨站脚本攻击、应用系统弱口令、敏感文件下载、后台用户枚举等。

（二）漏洞确认与风险评估

对扫描发现的漏洞进行确认，排除误报和无效漏洞。对确认的漏洞进行风险评估，确定其潜在的安全威胁和影响范围。

（三）整改建议与协助

根据漏洞的风险评估结果，提出具体的整改建议和改进措施。协助开发人员理解漏洞原理和影响，提供技术支持和整改指导。最后跟踪整改过程，确保漏洞得到及时修复和加固。

（四）漏洞闭环

在协助漏洞修复后，我司会进行一次漏洞复测，验证修复措施是否有效，以及是否还有任何残留的安全风险。通过复测，确保漏洞已经被完全解决，从而保障系统的安全性，最后达到漏洞闭环效果。若复测出漏洞没有被修复完成，继续协助开发人员提供技术支持和整改指导，直至漏洞修复完成。

**输出物：**收集漏洞扫描工具输出的结果和数据。整理和分类扫描到的安全漏洞，包括漏洞类型、等级、位置等详细信息。编制漏洞扫描台账，记录扫描的日期、目标系统、扫描工具、发现的漏洞及其修复建议等。最后分析扫描结果，识别关键漏洞和潜在风险，输出《漏洞扫描报告》、《漏洞复测报告》，为安全团队提供决策支持。

**（3）基线核查服务**

**期限频率：**按需提供。

**服务范围：**核心网络设备、安全设备、服务器主机系统等。

**服务内容：**针对漏洞扫描工具不能有效发现的方面（网络设备的安全策略弱点和部分主机的安全配置错误等）进行安全辅助的一种有效评估手段。服务范围包括各种网络设备、安全设备、主机操作系统、数据库、常见中间件及网络服务应用等。基线核查的服务内容主要集中在设备的账号管理、口令管理、认证授权、日志配置、进程服务、外部端口等几个方面，覆盖与安全问题相关的各个层面。

**输出物：**《基线核查报告》。

**（4）渗透测试服务**

**期限频率：**4次/年。

**服务范围：**对外业务系统，用户指定业务系统、门户网站等。

**服务内容：**通过模拟黑客可能使用的工具、分析方法来对信息系统进行模拟攻击，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误等以及其他专项内容测试与分析，重点发现信息系统应用层业务流程和逻辑上的安全漏洞和敏感信息泄露的风险。渗透测试主要内容包括：

1、主机操作系统渗透：包括WINDOWS、SOLARIS、AIX、LINUX、SCO、SGI等。

2、数据库系统渗透：包括MS-SQL、ORACLE、MYSQL、INFORMIX、SYBASE、DB2等。

3、应用系统渗透：对各种应用系统进行渗透测试，如WWW、E-mail、DNS、FTP等。

**输出物**《渗透测试报告》。

**（5）漏洞攻击防护服务**

**服务内容：**部署入侵检测防护系统（漏洞防护），通过开展漏洞攻击防护服务，实现对漏洞利用攻击的防护方案。对漏洞利用攻击行为的风险IP发现、处置，保障整体网络安全，保护网络和系统整体安全。

**服务期限、频率：**一年。

**服务工具要求：**1、采用旁路部署的模式接入网络，不改变组网结构，通过镜像流量智能分析，不对正常业务造成干扰。

2、采用先进的SSL证书认证技术，构筑坚实可靠的HTTPS安全链接，确保数据传输的完整性与机密性，深度加密防护。

3、支持给予新用户系统操作步骤引导，帮助用户更好地理解和使用产品中的特定功能或完成特定任务。

4、利用网络安全技术和算法，对设备的网络和流量进行实时探测和分析，及时发现对设备的攻击或扫描行为。

5、支持主动屏蔽。采用大流量分析技术，对含有漏洞探测行为的流量进行针对性屏蔽，使其无法获取到目的资产的漏洞信息。

6、基于高频触发、部分爬虫行为的风险分析。采用流量分析手段匹配系统底层内置规则，识别恶意工具的访问、扫描、攻击行为。

7、基于规则库的攻击行为分析，库内支持30w+规则，采用漏洞规则比对手段检测中间件、系统框架、数据库、病毒木马等恶意攻击行为。

8、首页全视角呈现风险情况，包括但不限于发现风险、阻断风险、网卡状态及流量情况、已拦截风险IP信息、已识别风险ip信息、高中低危风险数统计等。

9、支持对攻击行为准确判断，根据预设警报规则对异常情况进行记录，并提供系统捕捉到的相关异常信息，包括风险IP、风险等级、告警次数、预警时间等。

10、具备风险IP自处理能力。支持批量对风险IP执行阻断/告警两种应对模式，提供通道能够人工对风险IP进行风险等级划分

11、★支持在IP路由协议(RIP、IGRP、OSPF、IS-IS、BGP、MPLS-VPN）下实现漏洞自动屏蔽。（需提供软件截图证明）

12、★双向阻断：同步监听东西向与南北向环境中的多重风险，监听从任意一端发起的攻击、访问、扫描行为及是否存在被攻击的风险，并对其行为采取预警/阻断处理。（需提供软件截图证明）

13、二次扫描：具备二次扫描能力。在初次扫描并过滤流量信息后，触发二次扫描机制，对已经过滤的流量数据进行更为深入和详尽的再次审查，提升安全检测的精准度，降低误报漏报情况。

14、登录安全：支持验证码的开启与关闭功能，以增强用户登录过程的安全性和灵活性。

15、未授权访问：新用户首次登录强制修改初始密码。具备密码到期提前提醒的功能，促使用户在密码即将过期之前及时更新密码。

16、支持对内网重要网段进行批量上传防护，对导入的数据进行解析、验证，结合安全策略和规则。支持对防护网段划分“隔离”和“放行”操作。

17、支持内网防护配置列表，对列表内IP开启漏洞防护功能，对蜜罐、诱饵、仿真类主机不加入防护列表。

18、支持通过端口设置扫描范围，支持根据源目端口及端口协议类型进行设置

19、★支持手动录入或自动发现风险IP信息，能够更好地进行风险管理和决策制定。（需提供软件截图证明）

20、★支持配置风险白名单，允许部分IP进入内网扫描。应用于内网自查漏洞风险、内网存在探测设备等场景。（需提供软件截图证明）

**（6）主动安全防护服务**

**服务要求：**部署漏洞仿真系统，通过漏洞仿真服务的建设，模拟各种业务和漏洞信息，隐匿真实资产信息和弱点漏洞，诱捕攻击者信息，发现潜在的安全威胁，并及时进行处置，从而提高系统的安全性和可靠性。

**服务期限、频率：**一年。

服务工具要求：1、采用旁路部署模式接入网络，无需对原始的网络架构和业务流程进行任何修改，不干扰正常业务运行对网络流量进行捕获和分析。

2、在攻击者入侵的关键路径上部署诱饵和节点，不占用业务环境内实际资源，诱导攻击者转移攻击目标进入与真实网络隔离的蜜网。

3、首页采用图表、图形、仪表盘等可视化元素，将训节点情况、攻击事件统计、攻击源IP、攻击趋势等以直观易懂的方式展现。

4、不改变本地现有资源情况下，利用空闲IP虚拟出泛漏洞信息散布，扩散业务量将真实业务藏身于虚拟环境内。

5、虚拟泛业务的漏洞依附场景，扩大虚拟业务场景数据量弱化真实业务的存在。

6、虚拟出泛漏洞信息，支持选择系统模板内的漏洞信息，支持自定义新增端口开放型风险，支持对风险进行威胁程度设定，扩大漏洞散布范围。

7、系统内置41条漏洞服务且不含敏感信息，便于用户部署诱饵系统，通过主动暴露非关键漏洞，诱捕并分析黑客攻击行为，增强安全防护的主动性与智能性。

8、该功能支持对当前部署的漏洞服务进行运行状态监测与评估，提供详尽的漏洞信息查询接口，并允许用户将特定漏洞与主机节点进行关联绑定，实现漏洞管理的精细化。

9、★通过虚拟引流技术识别具有异常的行为特征的流量，引导流量优先走向虚拟业务、仿真漏洞内。（需提供软件截图证明）

10、★实时监听诱饵、沙箱以及各个节点的失陷状态，即是否被未经授权的第三方入侵或控制。（需提供软件截图证明）

11、★发现攻击者触发仿真系统节点，其所有操作都会被详细记录，包括源目IP、源目端口、路径、请求包以及攻击行为记录等。

12、支持对少量触发漏洞服务的行为判断为疑似攻击，根据内置策略达到一定程度的攻击次数后判断为风险并记录在系统内，疑似攻击获取信息包括但不限于漏洞信息、攻击目标、威胁等级、攻击次数、开始/结束时间

13、支持对风险事件的时间序列数据进行综合分析并产生总结报告。允许总结报告存放在系统内，便于后续下载与查阅，确保风险管理流程的高效性与数据的安全性。

14、将恶意程序与命令、文本、工具等正常程序捆绑成一个文件，并通过伪装漏洞、虚拟业务等方式发送给攻击者。

15、攻击者执行被伪装的木马程序后，管理设备支持通过木马程序远程控制用户计算机，并在后台建立与服务器的连接。反制手段包括文件操作、进程管理、键盘记录、屏幕监控、摄像头控制、权限访问等。

16、支持获取目标计算机上的敏感信息，包括但不限于账号密码、文件资料、设备指纹信息、网址信息、手机号、社交账号等。

**（7）安全威胁分析联动服务**

**服务要求：**部署安全威胁统一管理系统及工具，通过安全威胁检测服务，及时发现并应对各种安全威胁。实现对网络流量、系统日志、应用程序事件等数据的实时监测和分析，发现潜在的恶意行为、漏洞利用和攻击行为，并联动防火墙和漏洞防护设备进行自动阻断。

**服务期限、频率：**一年。

**服务工具要求：**1、★支持主流厂商的态势感知、防火墙、入侵检测、蜜罐等安全设备对接并收集互联网风险告警信息。（需提供软件截图证明）

2、系统区分“监测类型设备”和“处理类型设备”，对接入设备进行类型和功能区分。

3、支持对第三方接入设备进行动态连接测试，保障第三方信息的持续收集，快速发现单位网络环境内的异常行为。

4、提供定制化设备对接服务，配合客户单位拓宽产品联动领域，对产品新版本或是其他厂商或类型的安全产品进行对接开发。

5、首页采用图表、图形、仪表盘等可视化元素，将第三方设备联动情况、攻击情况、攻击事件统计和详情、风险处置统计等以直观易懂的方式展现。

6、支持对接入信息进行数据识别分析，列举展示攻击名称、源/目地址、源/目端口、协议、威胁级别、数据来源、开始/结束时间等。

7、支持对异常告警信息的内容进行判断，通过内部核心动态数据分析技术实现数据来源定位，危险等级判断。

8、通过第三方对接收集到的数据包，对多条数据包进行大规模数据处理、数据清洗和数据分析，比较字段值的相似度和重复性，经过拆分、搭建、选择、重组、整合流程，将多条有效信息组合成一条新的风险告警数据信息进行展示。

9、支持大屏对各类安全设备关键数据的集中可视化展示，支持展示内容包括但不限于：

10、蜜罐相关指标：蜜罐被攻击漏洞TOP5、攻击源IP TOP5、蜜罐部署及沙箱节点情况。

11、外联检测指标：违规外联行为预警统计。

12、威胁入侵指标：威胁入侵事件预警以及风险分布，包括已处置风险IP、新增风险IP处置情况以及各类风险分布情况。

13、联动处置指标：威胁处置中心联动设备情况、事件处置进展及攻击事件统计情况。

14、★支持运营中心大屏与AI数字人联动，具备可视化数据分析与智能交互能力。AI数字人可基于大屏展示的安全数据，进行自动分析与辅助解读，支持快捷提问与自然语言交互，实现对系统功能、日志查询、威胁处理、策略配置等内容的快速响应与智能问答，提升安全运营智能化与便捷性。（需提供软件截图证明）

15、支持调动处置设备，自动对已发现的异常风险进行快速处置，并在风险处置页面记录相关风险信息，包括风险IP、风险类型、风险来源、处置设备、处置结果等信息。

16、支持自主新增风险IP进行提前预防，增加客户对网络环境的把控和灵活应对的手段。

17、★横向处置：自定义处置范围，开启横向处置则对内外网所有存在攻击行为的风险IP均进行阻断处置，关闭则对保护网段外的风险进行处置。（需提供软件截图证明）

18、支持配置内网地址白名单，允许任何IP与白名单内地址进行访问和通信(包括本身);支持配置事件白名单，自动根据规则放行白名单中的事件。

19、支持对系统的用户、机构、角色、岗位等参数进行适当调整，支持对系统的使用者进行权限划分和管理。

20、具备溯源功能，可追踪登录和操作日志，确保用户身份可信，并提供详细的操作记录，以实现对系统安全性和合规性的监控和审计。

**（8）新系统上线评估服务**

**期限频率：**按需提供。

**服务范围：**新上线业务系统。

**服务内容：**在新系统上线前，进行全面的安全脆弱性检查，从源头上减少信息系统存在的安全风险，包括新系统代码审计、渗透测试、安全配置检查、安全功能审核等内容，全面评估系统面临的威胁、弱点、影响和风险，以确定可能的安全问题。同时，针对这些安全问题，提供相应的解决建议，确保系统在面对潜在威胁时能够有效地应对。

**输出物：**《系统安全评估报告》。

**（9）应急演练服务**

**期限频率：**按需提供

**服务范围：**用户指定1个信息系统或网站

**服务内容：**在服务期内，为应对信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决的情况，提前针对此类事件进行应急方案的编制和演练，提高应对安全事件的处置能力，预防和减少安全事件造成的危害和损失

通过应急演练预案，并协助各级单位开展预案演练，提高应对安全事件的处置能力，预防和减少安全事件造成的危害和损失。应急演练是应急响应事件发生的场景模拟，通过对事件频发、危害性高、影响范围大的特定信息安全事件进行演练，以期在遇到此类信息安全事件应急响应处置过程中，发现问题，及时响应，快速处置的目的

**服务要求：**可选演练场景应包括但不限于：

入侵系统攻击安全事件

拒绝服务攻击安全事件

病毒与木马攻击安全事件

网站页面篡改安全事件

数据库内部误操作

可选演练内容应包括但不限于：

信息篡改：模拟针对网站首页篡改事件的监控和处理（利用上传漏洞或者弱口令实施攻击）。

拒绝服务：模拟从外部发起的针对网站的拒绝服务攻击事件的监控和处理（UD\CC等DDOS攻击工具）。

恶意代码：模拟某恶意攻击者，利用系统的弱口令，利用windows共享管理服务（tcp/445），获得对服务器的控制权限。

DNS劫持：模拟由于网站的域名解析管理账号存在弱口令，域名权威解析被篡改事件。

**输出物：**《应急演练总结报告》

**（10）重保值守响应服务**

**期限频率：**按需提供。

**服务范围：**涵盖医院信息系统网络。

**服务内容：**提供高级安全专家、安全服务工程师特殊时期提供人员保障服务。

特殊时刻人员值守：重大节日、活动、会议期间，提供人员值守服务对安全事件进行预防、监测、处置及溯源，保障信息系统安全稳定运行，及时封堵已知、未知攻击行为，确保重保期间不发生网络安全事件，对于发现的网络威胁情况能够紧急处理。

**服务要求：**1.重保前检查：针对信息资产及系统现状进行详细调研，并根据调研信息开展安全自查和整改工作，做好充分的准备工作。

2.重保中响应：安排专业值守人员和在线工程师做好安全防护和保障工作，第一时间发现并处理威胁流量，做好应急响应处置工作，避免安全事件带来的不良影响。

3.重保后总结：对重保期间的工作内容和威胁处置情况进行复盘总结和汇报，为下一步的安全建设和策略制定提供方向和建议。

**输出物：**《重保值守日报》《重保值守总结报告》等。

**（11）应急响应服务**

**期限频率：**按需提供。

**服务范围：**用户信息系统资产。

**服务内容：**当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助用户快速止损，最大化降低安全事件带来的影响。

**服务要求：**7\*24小时突发安全事件应急响应，在优先恢复业务运行的前提下，提供安全事件的溯源、分析、处置、加固协助的完整闭环支撑服务。

**输出物：**《应急响应报告》。

**（12）安全培训**

**期限频率：**1次/年。

**服务范围：**用户指定。

**服务内容：**根据用户要求对业务人员、安全管理人员、技术人员开展针对性网络与信息安全培训，提高受众个人隐私保护、技术防护、信息安全管理等能力，增强个人网络安全防护意识，规避网络攻击风险。

**服务要求：**对安全管理人员的培训，讲解国家相关部门对系统信息安全管理和建设的相关标准，研讨建立具有针对性和适用性的安全管理办法。

对技术人员的培训，使他们了解信息系统所面临的严峻安全威胁和挑战，以及如何进行全面有效的安全防护措施。

全员培训主要包括：安全意识培训等。

对普通用户的培训，让大家对信息安全的有初步的认识和逐步提高安全意识，让安全事故可以得到有效的避免。

**输出物：**《网络安全培训课件》。

**（三）数据安全服务**

**（1）管理制度建设服务**

**服务频次：**1次/年。

**服务内容：**配合医院从组织、制度、人员等管理维度，开展调研工作，按实际管理要求定制化输出数据安全相关制度、流程和规范文件，以满足安全管理要求及实质合规要求。制度上满足用户要求。如数据安全、网络安全（包括但不限于信息安全等级保护2.0二级、三级认证的要求，监管单位对应的制度要求）。

数据安全与网络安全紧密相连，两者互为支撑，共同构成了信息安全的基础。网络安全是数据安全的基础保障，只有确保网络系统的安全性，才能有效防止外部攻击和内部泄露对数据的威胁；数据安全也是网络安全的重要组成部分，通过对数据的严格保护和管理，可以降低网络安全事件的风险和损失。通过管理制度建设服务中，将数据安全与网络安全紧密结合，形成一套完整的安全管理体系。

通过将制度方针、管理制度与流程规范、实施细则与指南、审批表单与日志四个方面进行分层，建立单位自有制度体系，并通过单位层面整体考虑和设计形成制度体系框架，并构建制度流程。

横向参考ISO框架，纵向参考DSMM模型，与现有制度体系进行融合，建立数据安全管理规范；涵盖从风险评估到策略制定、从组织架构优化到流程规范、从技术防护到应急响应的全生命周期管理制度建设。由数据和网络利益相关者和专业人员分别组成领导小组、管理小组、运营小组，实现从审批、监督、治理、制度建设、平台建设等全流程建设服务。并从统筹管理能力、运营能力、技术能力三个方面帮助用户单位，根据不同的分工，培训并建立起与各安全岗位人员适配的安全能力。

**服务范围：**数据安全、网络安全【包括但不限于信息安全等级保护2.0三级认证、监管单位对应的制度建设要求】

**输出物：**包括但不限于如下:

* 《网络数据安全制度管理映射清单》
* 《数据安全管理办法》
* 《数据安全领导小组发文》
* 《数据安全工作方案》
* 《数据安全应急响应制度》
* 《数据合作方管理制度》
* 《数据生命周期安全管理制度》
* 《存储介质安全管理规范》
* 《数据安全分类分级管理制度》
* 《数据资产管理制度》
* 《数据安全人员管理制度》
* 《数据公开管理制度》
* 《数据安全与新应用开发评估制度》
* 《个人信息保护内部管理制度和操作规程》
* 《数据安全领导小组发文》
* 《大数据平台安全管理制度》
* 《云数据安全责任说明书》
* 《数据公开安全操作规程》
* 《数据提供安全策略与操作规程》
* 《数据脱敏管理制度》
* 《数据加密防泄漏管理制度》
* 《数据安全审计与日志管理制度》
* 《数据导入导出管理规范》
* 《数据安全评估管理制度》
* 《网络安全管理办法》
* 《网络安全领导小组发文》
* 《网络安全工作方案》
* 《网络安全应急响应制度》

**（2）数据安全巡检服务**

**服务频次：**4次/年。

**服务内容：**日常运维和安全加固

设备巡检：定期对数据安全设备、数据库服务器、进行安全巡检，包括设备硬件状态巡检、性能巡检、日志和备份检查、规则库、授权等基础信息巡检。

补丁升级：为提高数据库的稳定性，规避风险，定期分析业务系统数据库隐患，结合客户的业务需求的具体情况，提出补丁预警方案，并制定完善的升级计划，对任何可能存在的风险进行规避，同时可借助其他工具进行虚拟补丁升级。

策略优化:根据数据全生命周期各项管理要求，制定通用安全策略，并结合各业务场景安全需求，制定针对性的安全策略。其中基于安全基线评估及日常业务流程过程中，对前期制定的安全策略进行优化调整，对访问控制进行优化增强访问控制杜绝越权访问带来的威胁，对行为审计进行优化实现全面审计无“死角”实现安全策略优化效果，最终通过通用策略和针对性策略结合部署，最终实现对数据流转过程的安全防护。

数据安全设备统一纳管

由于在数据安全生命周期内，各种数据安全设备种类繁多、异构性强，导致安全管理工作面临巨大挑战。本服务旨在通过梳理安全设备、纳管各安全设备，实现统一日志收集、分析、安全策略统一运营、数据安全态势展示、风险事件处置、知识库维护等。

**输出物：**《管控中心巡检报告》、《数据安全风险事件统一处置报告》

**（3）数据安全自检服务**

**服务频次：**1次/年

**服务内容：**通过数据检查工具箱为企业提供一套全面、高效的数据安全自我检测与评估工具，帮助企业快速识别、评估并管理数据安全风险。通过综合运用数据资产全面测绘、敏感数据识别与保护、配置信息采集与核查、网络流量检测与弱口令扫描、网络脆弱性扫描与数据安全评估等功能。实现数据安全问题自我闭环。

**服务要求：**数据资产全面测绘：快速发现存活主机、网络设备、数据库，并准确识别其属性。支持可视化地图展现，从不同维度直观展示数据库数据信息、敏感数据信息。为企业提供全面的数据资产清单，为后续的安全评估与防护提供基础。

敏感数据识别与保护：深度发现隐藏于数据库、文本、图片中的敏感信息，并统计敏感数据量。采用抽样扫描匹配加人工核实校正的方式，形成敏感数据分布清单。建立负面清单敏感词库，提高敏感数据的识别精度与保护效率。

配置信息采集与核查：检查数据库、操作系统、应用程序、网络设备的配置项。获得合规和不合规项信息，以及高危、中危和低危的配置项信息。为企业提供详细的配置信息报告，帮助发现潜在的安全隐患。

网络流量检测与弱口令扫描：实时检测网络中的恶意攻击、违规行为、非法设备接入以及蠕虫、病毒等恶意软件的传播。支持检测系统、数据库、应用程序等中的弱口令。通过识别和修复弱口令，加固数据安全防线，提高系统的整体安全性。

网络脆弱性扫描与数据安全评估：对数据库、操作系统、应用软件、虚拟化平台、工业控制系统等网络资产进行漏洞扫描。及时发现漏洞并采取相应的防御措施，降低系统被攻击的风险。提供数据安全评估功能，帮助企业全面了解数据资产，识别敏感数据，确保数据处理符合法规和政策。

风险识别与管理：通过全面测绘数据资产、识别敏感数据、检测数据库漏洞、监测网络流量等功能，帮助企业发现潜在的安全风险。提供风险分析报告，指导企业及时采取措施，降低数据泄露和攻击的风险。

快速响应与整改：一旦发现数据安全问题，为企业提供详细的修复建议。助力企业迅速采取行动，缩短漏洞暴露时间，降低潜在损失。提供持续的跟进与技术支持，确保整改措施的有效实施。

**输出物：**《数据安全检查报告》

**（4）测评审查支撑(迎检)服务**

**服务频次：**1次/年

**服务内容：**在客户单位迎接上级对其数据安全的通过性审查时，为客户提供全面测评的技术支撑，将测评对应项进行罗列整理并提供相应的解决方案，协助客户通过数据安全审查，并确保测评分数处于高位水平。

同时，我们将协助客户准备审查所需的文档资料，包括但不限于数据安全管理政策、操作流程、技术防护措施等，确保所有材料齐全、规范，符合审查要求。此外，我们还将提供模拟审查服务，通过模拟上级审查流程，帮助客户提前发现并整改潜在的问题，进一步提升迎检准备工作的针对性和实效性。

（一）测评对应项罗列与解决方案提供

1. 全面梳理测评项

组织专业的数据安全团队，依据上级审查的标准和要求，对医院数据安全涉及的各个方面进行全面梳理。涵盖数据的收集、存储、传输、使用、共享和销毁等全生命周期环节，以及数据安全管理体系、技术防护措施、人员安全意识等多个维度。

2. 深入分析与风险评估

对梳理出的测评项进行深入分析，结合医院的实际业务情况和数据安全现状，评估每个测评项可能存在的风险和问题。采用先进的评估工具和方法，如漏洞扫描、渗透测试等，全面检测医院信息系统的安全性。

3. 定制化解决方案

针对每个测评项的风险和问题，制定个性化的解决方案。对于技术层面的问题，如系统漏洞、数据加密不足等，提供专业的技术修复建议和实施计划；对于管理层面的问题，如制度不完善、人员操作不规范等，协助医院完善相关管理制度和操作流程。

（二）审查文档资料协助准备

1. 资料清单制定

根据上级审查的要求，结合医院的实际情况，制定详细的审查文档资料清单。清单包括但不限于数据安全管理政策、操作流程、技术防护措施、应急响应预案、人员培训记录等。

2. 资料编写与完善

协助医院编写和完善审查所需的文档资料。对于已有的文档，进行审核和修订，确保内容完整、规范、符合审查要求；对于缺失的文档，根据医院的实际情况和相关标准要求进行编写。

3. 资料审核与优化

对编写和完善后的文档资料进行审核，确保所有资料的准确性、一致性和合规性。同时，根据审核结果对资料进行优化，提高资料的质量和可读性。

（三）模拟审查服务

1. 模拟审查流程设计

参照上级审查的实际流程和标准，设计详细的模拟审查流程。模拟审查流程包括审查准备、现场检查、文档审核、问题反馈等环节，确保模拟审查的真实性和有效性。

2. 模拟审查实施

按照设计好的模拟审查流程，组织专业的审查团队对医院进行模拟审查。审查团队由具有丰富数据安全审查经验的专家组成，采用多种审查方法，如文件审查、现场访谈、系统测试等，全面检查医院的数据安全状况。

3. 问题整改与跟踪

模拟审查结束后，及时向医院反馈审查结果，列出发现的问题和潜在风险。协助医院制定问题整改计划，明确整改责任人和整改期限。对整改情况进行跟踪和监督，确保问题得到及时、有效的解决。

**（5）数据安全培训**

**服务频次：**1次/年。

**服务内容：**数据安全与网络安全紧密相连，两者互为支撑，共同构成了信息安全的基础。通过分层培训体系，对管理人员、技术人员和全体员工开展数据安全与网络安全培训，提升单位信息安全防护能力，保障信息安全合规。

针对本次项目投标产品及服务，提供原厂培训，培训讲师深耕数据安全领域，提供更加深层次且全面的数据安全培训。

根据数据安全产品和运行维护进行针对性的培训。全面提升单位相关管理人员及技术人员对数据安全的认识与理解，掌握数据分类、敏感信息识别、数据安全法律法规、数据加密技术、数据备份与恢复以及数据安全管理制度等关键知识点。通过系统的培训，增强单位的数据安全防护能力，确保数据资产的安全与合规。

通过线上课程、线下讲座等多种方式，全面提升相关管理人员及技术人员对数据安全的认识与理解，掌握数据分类、敏感信息识别、数据安全法律法规、数据加密技术、数据备份与恢复以及数据安全管理制度等关键知识点。通过系统的培训，增强院内的数据安全防护能力，确保数据资产的安全与合规。

**四、商务要求**

1、付款方式：合同签订正式生效后7个工作日内支付40％合同款；服务期满一年后15个工作日内支付60%的合同款。

2、服务期：本次服务时间1年，具体日期以合同签订时间为准。

4、售后服务：如有技术疑难问题，须半小时内响应；如需到达现场处置，须2小时内到达。在服务期内，提供信息安全的咨询服务，能够协助用户进行安全整改、制度建设等工作。

3、▲其他要求：为了提高服务质量，并对整个项目的服务周期有迹可循，项目维保周期内，要求中标供货商对供货、规划、调试、割接、集成、巡检、运维的服务记录，提供跨网传输系统并实时上传服务记录文档，涉及数据安全问题，系统需部署在甲方本地机房内，跨网传输系统要求如下：

1）支持在不同网络之间的文件传输，包括内网和外网。用户通过平台将文件从一个网络环境传输到另一个网络环境，实现文件的同步和共享。系统同时支持实时同步功能，确保文件在不同网络环境下的实时更新和一致性。（需提供软件截图证明）

2）群组成员角色包括管理员(即为创建者)、子管理员(代管人)、普通成员。管理员拥有所有权限。子管理员权限包括文件版本管理、编辑文件权限、增删回收站、增删成员、成员权限编辑。（需提供软件截图证明）

3）支持批量文件压缩下载；支持文件夹压缩下载。（需提供软件截图证明）

4）采用图文形式直观展示重要数据。支持在管理端查看CPU、内存、存储资源使用情况；支持查看在线、离线人数；支持查看当天、当月、总上传文件数量；支持查个人/群组总存储资源利用率，根据Top10排列；支持查看个人、群组空间饱和程度，便于管理员分配。（需提供软件截图证明）

5）审批流程：接收用户传输文件的申请，可对内容进行预览（支持预览基础文件格式），处理结果为通过或驳回。

6）审批记录：审批员可查看文件审批的历史记录，必要时进行追溯。

7）审批消息：通知审批员来自用户传输文件等待审批的消息。

8）系统支持通过文件上传格式限制进行安全管控，可自定义策略进行安全管理，默认不限制文件上传格式。（需提供软件截图证明）

9）所有文件上传均会进行文件格式及内容的病毒扫描，支持双重扫描过程。第一阶段包括对文件的轻量级基础扫描，能够保证文件快速上传的同时同步进行文件简单病毒扫描；第二阶段包括已存在的文件进行深度病毒扫描，会根据扫描结果进行文件区分和展示。（需提供软件截图证明）

**第四章 报价要求**

**一、报价方式：本次报价方式为总价包干。投标总价应包括本项目整个服务期所需的一切软件、配套硬件、人工、工具、保险、交通、利润、税金、售后服务、保修（包含须由投标人承担的各种税费）、其它需投标人承担的费用及潜在可能涉及的一切费用。未计入报价而应该发生的费用的，视为已含在其他分项投标报价中。投标人应认真计算可能发生的各相关费用并计入投标报价内，在项目实施过程中不得借此要求增加任何费用。报价单需盖公章。**

二、为防止出现恶意扰乱招标程序的报价，投标人报价明显高于市场价或明显低于成本价的，视为无效投标处理。

三、投标单位如违反上述条款，将被取消投标资格或终止合同（协议）。

**第五章 投标文件格式要求**

1.1报价文件

初始报价一览表(按照报价格式要求)

1.2商务技术文件

（1）资格证明文件：

 1）投标人营业执照副本（复印件）；

 2）有效期内的组织机构代码证（复印件）（多证合一的，只需提供营业执照复印件）；

 3）有效的税务登记证或当地税务部门开具的依法纳税的缴税（费）证明（复印件）（多证合一的，只需提供营业执照复印件）；

 4）有效期内的社会保险登记证或社保缴纳证明（复印件）（多证合一的，只需提供营业执照复印件）；

5）投标人近三年在经营活动中没有重大违法记录的书面声明（格式参考）；

（2）投标函；

（3）投标项目浙江省内企事业单位用户名单（类似项目相关业绩）；

（4）法定代表人资格证明书；

（5）法定代表人授权委托书（法定代表人签署不需提供此书）；

（6）法定代表人及授权代表身份证正反面复印件；

（7）供货或服务清单；

（8）随机标准附件、备品备件、另配件、专用工具清单表（如适用）；

（9）产品性能说明或服务内容详细说明；

（10）技术规格明细表（如适用）；

（11）产品的合格证书复印件（如3C证书等）（如适用）；

（12）投标机型的样本或彩页（如适用）；

（13）投标人认为有必要提供的其它文件；

（14）按照项目具体要求响应(可标注页码)，同时提供所需文件证明。

1.3 投标文件的编制

1.3.1 投标文件应按照本章1.2款中规定的顺序及采用“投标文件格式”中提供的格式进行编制。

1.3.2投标文件的正本需打印或用不退色的墨水填写，并注明“正本”字样。副本可以复印，并注明“副本”字样。当副本和正本不一致时，以正本为准。

1.3.3投标文件由投标人的法定代表人或其委托代理人签字（或盖章）、盖单位公章。投标文件应尽量避免涂改、行间插字或删除，如果出现上述情况，改动之处应加盖单位公章或由投标文件签署人签字（或盖章）确认。签字或盖章的具体要求见“投标人须知前附表”。

1.3.4由于字迹模糊或表达不清引起的后果由投标人负责。

1.4 投标报价

▲1.4.1本次投标报价为含税人民币价。

1.4.2投标报价包括完成所有产品供货及履行所有规定服务所产生的全部费用。产品及服务须达到采购文件规定的质量标准及使用要求。

1.4.3报价应按不同费用构成分开填写，具体详见“投标文件格式”。

▲1.4.4 本次投标报价采用二次报价方式，以磋商谈判后的二次承诺报价为最终报价。

2、投标

2.1 投标文件的密封及标记

2.1.1投标文件应按以下方法密封

投标文件密封要求在密封袋封皮上写明招标项目编号、项目名称、投标人名称、所投标项名称、投标文件名称（”报价文件”或“商务技术文件”）、“在投标截止时间（ 年 月 日 时 分）前不得启封”。封口处应有盖单位公章或投标授权代表签字（或盖章）。

2.1.2如果投标人未按上述要求加写标记，采购人对投标文件的误拆和提前启封不负责任。

2.1.3投标文件份数： 提供一式三份，其中报价文件正本一份，副本二份；商务技术文件正本一份，副本二份。

2.1.4投标文件装订要求： 报价文件和商务技术文件须分别装订成册，采用胶装（粘贴方式装订），不得采用活页夹等可随时拆换的方式装订。

2.2 投标人不足三家情况处理

投标截止时间结束后参加标项投标的供应商不足三家的，除采购任务取消情形外，采购人可选择以下方式之一处理：

1）可将本标项作废标处理，重新组织采购；

2）符合医院内控要求的其他采购方式组织采购；

**承诺函**

浙江中医药大学附属第三医院：

我方（供应商）近三年内，具有良好的商业信誉，依法缴纳税收和社会保障资金，未被列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，在经营活动中没有重大违法记录（没有因违法经营受到刑事处罚，没有被责令停产停业、被吊销许可证或者执照、被处以较大数额罚款等行政处罚，没有因违法经营被禁止参加政府采购活动的期限未满情形）。如有虚假，采购人可取消我方任何资格（投标/中标/签订合同），我方对此无任何异议。

特此承诺！

投标人全称（盖单位公章）：

投标文件签署人（签字或盖章）：

日期： 年 月 日

**投标函**

浙江中医药大学附属第三医院：

（投标人全称）参加贵方组织的（项目名称）（招标项目编号）招标的有关活动，并对（项目名称）进行投标。为此我方：

1、承诺在投标人须知规定的投标截止日起遵守本投标文件中的承诺，且在投标有效期满之前均具有约束力。本投标文件的有效期为自投标截止时间起 天。

2、承诺已经具备采购人规定的特定条件。

3、已详细审核全部采购文件，包括采购文件补充（如果有）、参考资料及有关附件，确认无误。

4、提供投标人须知规定的全部投标文件，包括投标文件正本 1 份，副本 2份。 招标文件装订成册（胶装）密封

5、投标报价详见《开标一览表》。

6、保证遵守采购文件中的其他有关规定。

7、完全理解不一定接受最低价中标。

8、我公司自愿参加本项目的投标，并保证投标文件中所列举的投标报价文件及相关资料和公司基本情况资料是真实的、合法的。愿意向贵方提供任何与该项目投标有关的数据、情况和技术资料。若贵方需要，愿意提供我方做出的一切承诺的证明材料。

9、保证忠实地执行双方所签订的合同，并承担合同规定的责任和义务。

10、我方承诺不存在以下情况：

a）提供虚假材料谋取中标、成交的；

b）采取不正当手段诋毁、排挤其他供应商的；

c）与采购人、其它供应商或者采购代理机构恶意串通的；

d）向采购人行贿或者提供其他不正当利益的；

投标人全称（盖单位公章）：

投标文件签署人（签字或盖章）：

日期： 年 月 日

单位地址：

邮编：

电话：

传真：

**法定代表人资格证明书**

投标人名称：

法定地址：

姓名：

性别：

年龄：

职务：

身份证号码：

该同志系公司法定代表人。

特此证明！

投标人：（盖章）

日期： 年 月 日

附：

|  |  |  |
| --- | --- | --- |
| 法定代表人身份证复印件正面 |  | 法定代表人身份证复印件 反面 |

**法定代表人授权委托书**

（法定代表人签署不需提供此书）

致浙江中医药大学附属第三医院：

我 \_（姓名）系 \_\_（投标人名称）的法定代表人，现授权委托本单位在职职工 （姓名）以我方的名义参加 （项目名称） 项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。

我方对被授权人的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤销而失效。

被授权人无转委托权，特此委托。

被授权人签名：

职 务：

被授权人身份证号码：

法定代表人签名：

职 务：

身份证号码：

投标人公章：

签署时间： 年 月 日

附：

|  |  |  |
| --- | --- | --- |
| 被授权人身份证复印件正面 |  | 被授权人身份证复印件反面 |