中山大学附属第六医院粤西医院信宜市人民医院

网络安全加固建设院内调研文件

中山大学附属第六医院粤西医院/信宜市人民医院

2024 年 8 月

目　录

第一章　报名须知

一、报名注意事项

1．报名截止时间一到，我院不接收报名人的任何报名文件及相关资料。为此，请适当提前报名。

2．报名人请注意我院采购需求和报名提交资料的具体要求，不按照要求提交，报名作废处理。

3．请仔细检查报名文件要求盖公章、签名、签署日期之处。

4．如所投项目属于许可证管理范围内的，须提交相应的许可证复印件。

5．如报名人以非独立法人注册的分公司名义代表总公司盖章和签署文件的，须提供总公司的营业执照副本复印件及总公司针对本项目报名的授权书原件。

6．加★号的条款必须一一响应。

7．报名文件应按顺序编制页码。

8．因场地有限，我院无法提供停车位，不便之处敬请谅解。如有需要，请到周边的停车场停车，建议改乘公共汽车或出租车等交通工具。

9．为提高采购效率，已提交了报名文件而决定不参加本次采购项目询价的报名人，按《采购需求书》中的联系方式，以文字形式及时告知我院（否则纳入我院供应商评价管理-影响今后的采购项目）；对您的支持与配合，谨此致谢。

（本提示内容非采购文件的组成部分，仅为善意提醒。如有不一致，以采购文件为准。）

二、报名文件的递交

1. 报名文件的密封和标记

报名人应将报名文件正本和所有的副本密封包装，并在外包装上清晰标明“正本”、“副本”字样。

2. 对报名文件投递的要求

2.1 所有报名文件应于采购公告中规定的递交文件截止时间前递交到我院指定地点。

2.2 所有报名文件必须成册整理。报名文件的正本和副本应分别标注，并在包装的封面上写明：

报名文件（正/副本）

项目名称：填写采购公告中写明的项目名称

报名人名称（盖章）：

报名人地址：

联 系 人：

联系电话：

3. 报名文件的修改和撤回

3.1 报名人在递交文件截止时间前，可以对所递交的报名文件进行补充、修改或者撤回，并文字通知采购人。补充、修改的内容应当按采购/调研文件要求签署、盖章，并作为报名文件的组成部分。

3.2 在递交文件截止时间之后，报名人不得对其报名文件做任何修改和补充。

3.3 不接受电报、电话、电传、传真等形式的报名。

3.4 报名人在递交报名文件后，可以撤回其报名，但报名人必须在规定的递交文件截止时间前以书面形式/报名邮件告知采购人本项目指定联系人，否则将列为采购人黑名单供应商。

3.5 报名人所提交的报名文件在竞争性磋商结束后，无论采购结果与否概不退还。

3.6 采购人对不可抗力事件所造成报名文件的损坏、丢失不承担任何责任。

4. 报名样品

4.1 本项目如要求提交报名样品的，采购人在收取样品时没有对样品外观进行验收及性能测试，对样品的破损或质量概不负责。

4.2 由于采购人存放样品的空间有限，如采购人无需留存样品的情况下，请各有关报名人在参与采购项目竞争性磋商结束后当日内主动取回，否则视同报名人不再认领，采购人有权进行处理。

5、 报名文件的拒收：在超过递交资料截止时间送达的或未送达指定地点的，采购人有权利拒绝收取报名文件；

三、询价原则

1.评审小组随机确定供应商的询价次序。

2.评审小组首先审查供应商的资格，然后按询价次序与合格供应商分别进行询价。

3.评审标准：对通过初步评审的报名文件进行商务、技术和价格的评审（可依据报名情况适时调整）。

4.分值（权重）分配

评分总值最高为 100 分，商务、服务及最终报价得分分值（权重）、分值设置如下：

分值比例（100%）	商务评分（25%）	技术评分（45%）	报价得分（30%）
总分 100	35 分	35 分	30 分

1．商务评分（35 分）

序号	评审项目	评审细则	分值
1	一般商务条款响应情况	根据报价文件的一般商务条款响应情况进行评审，完全响应（无偏离或正偏离）的**得 7 分，每负偏离一个扣 1 分**，扣完即止。	7
2	重要商务条款响应情况	根据报价文件的重要商务条款响（标▲）应情况进行评审，完全响应（无偏离或正偏离）的**得 4 分，每负偏离一个扣 2 分**，扣完即止。	4
3	管理体系认证	报名人具备有效的质量管理体系认证证书，到达年度审查时间的须同时提供有效的最新年度审查证明文件。**满分 2 分**； 无提供或其他，得 0 分。	2
4	供应综合实力	报名人综合实力强，达到国家标准 GB/T23793-2017、ISO37001-2016 及 CTSSES1001-2019 的要求，并获得相对应的“供应商综合实力评价体系认证证书”，有得 2 分，没有不得分，且提供证书复印件并加盖报名人公章。 备注：证书有效性在国家认证认可监督管理委员会官网（http://www.cnca.gov.cn/)可查。	2
5	售后服务能力	报名人具备完善的售后服务体系，符合《商品售后服务评价体系》规定的五星级要求，并获得相关证书，有得 2 分，没有不得分，且提供证书复印件并加盖报名人公章。 备注：证书有效性在国家认证认可监督管理委员会官网（http://www.cnca.gov.cn/)可查。	2
6	投标人信息安全保障能力	报名人具备软件开发信息安全保障的能力，信息安全管理体系需符合 GB/T22080-2016/ISO/IEC 27001:2013 标准，并获得相关证书，有得 2 分，没有不得分，且提供证书复印件并加盖报名人公章。 备注：证书有效性在国家认证认可监督管理委员会官网（http://www.cnca.gov.cn/)可查。	2

7	同类项目业绩	报名人 2020 年 1 月 1 日至今同类项目业绩，**每提供一项合同得 2 分，最高得 8 分**。 注：提供合同关键页复印件，合同价格、服务内容清晰可见，以合同签订时间为准，不提供，得 0 分。	8
8	项目人员配备情况	对项目人员配备情况进行评审： 1、项目经理（最高得 4 分） 具备高级信息系统项目管理师证书得 4 分； 具备中级系统集成项目管理工程师证书得 2 分； 2、项目其他成员（最高得 4 分） 具备高级信息系统项目管理师证书或具备中级系统集成项目管理工程师证书得 2 分；	8

2．服务评分（35 分）

序号	评分项目	评分细则	分值
1	一般技术条款响应情况	根据报名人对一般技术内容的响应情况进行评审，完全响应（无偏离或正偏离）的**得 10 分，每有一条不满足（负偏离）扣 0.5 分**，扣完为止。	10
2	重要技术条款响应情况	根据报名人对重要技术内容（标▲）的响应情况进行评审，完全响应（无偏离或正偏离）的**得 15 分，每有一条不满足（负偏离）扣 1 分**，扣完为止。	15
3	实施服务方案	根据现场询价及项目实施服务方案进行评审： 1. 对项目需求理解透彻、实施方案具体、详细、可行，有利于项目实施的，**得 5 分；** 2. 对项目需求理解较好、实施方案较具体、较详细、可行，较有利于项目实施的，**得 3 分；** 3. 对项目需求理解一般、实施方案方案一般、较详细、可行性一般的，**得 1 分**； 4. 对项目需求理解较差、不提供实施方案，**得 0 分**。	5
4	售后服务方案	对项目的售后服务方案进行评审： 1. 有具体完善的售后服务方案，包括维修服务和技术支持，各阶段服务计划详尽，质保期、维护期内服务承诺可靠、具体，**得 5 分**； 2. 有较完善的售后服务方案，未完全包括维修服务和技术支持，质保期、维护期内服务承诺可靠、具体，**得 3 分**； 3. 有售后服务方案，服务计划、质保期、维护期内服务承诺一般、简单，**得 1 分**； 4. 未提供售后服务方案，**得 0 分**。	5

3．价格评分

评审项目	分值	评分细则

价格	30	价格得分采用低价优先法计算，即以满足竞争性磋商文件要求且有效报价的最低价为评审基准价，价格得分为 30 分，其他报名人的价格得分按如下公式计算(小数点后保存二位有效数，四舍五入)： 价格分＝（评审基准价/报名报价）×30。

第二章　用户需求书

序号	货物名称	政府采购品目分类编码	计量单位	数量

一、总体要求说明

1.1．标有“★”的条款为必须完全满足的实质性要求，报名人如有一项带“★”的条款未响应或负偏离，将按无效报名处理。

1.2．标有“▲”的条款为重要性要求，报名人如有带“▲”的条款未响应或负偏离的将被严重扣分。

1.3．报名人在响应详细内容中必须列出具体数值或作出具体承诺。如果报名人只注明“正偏离”或“无偏离”，将可能被视为“负偏离”，从而可能导致严重影响评分结果。

二、报价说明

报价要求说明：报名价格为包干价。报名人按采购文件的要求内容整体报价，报价应包含：实施服务费、人员劳务费、税费、交通费等在项目实施过程中的全部费用。报名人报价中漏报、少报的费用，视为此项费用已隐含在报名报价中，确定采购结果后不得再向采购人收取任何费用。最终报价以现场询价为准。

三、技术要求

（一）主要功能用途：主要功能用途：

为了我院信息网络的安全稳定运行，确保医院信息系统安全，根据我院目前的计算机信息网网络特点及安全需求，本着切合实际、保护投资、着眼未来的原则，提出本技术方案。

需求参数：

1	防火墙(政务网，医保网，互联网出口）	A02010301防火墙	台	3
2	行为审计	A02010311网上行为管理设备	台	1
3	防火墙（外网服务器区）	A02010301防火墙	台	1
4	防火墙（数据中心）	A02010301防火墙	台	1
5	终端安全管理系统	A02010309计算机终端安全设备	套	230
6	运维审计	A02010307审计类设备	台	1
7	网闸	A02010310网闸	台	1
8	零信任综合网关	A02010313虚拟专用网（VPN）设备	台	1
9	安全托管服务	C16010500 信息安全软件开发服务	套	1

备注：硬/软件产品及定制开发内容均需提供 3 年免费维保服务以及病毒库升级维护服务。

信息系统采购需求书

采购项目名称	信宜市人民医院网络安全加固建设项目		
采购品目分类	硬件类		
采购数量	1 项		
是否允许进口产品	是✪　否☼	**是否需要进口论证**	是✪请附论证材料 否☼
是否专门面向中小企业	是☼　否✪（中小企业特指制造商，如“否”需说明原因）		
是否开展需求调查	是✪　否☼（如“是”需附调查相关资料）		
	法定条件	供应商应当满足政府采购法规定的下列条件： （1）具有独立承担民事责任的能力； （2）具有良好的商业信誉和健全的财务会计制度； （3）具有履行合同所必需的设备和专业技术能力；	

<table>
<tr><td rowspan="3">供应商资格条件</td><td></td><td>（4）有依法缴纳税收和社会保障资金的良好记录；
（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录。</td></tr>
<tr><td>信用条件</td><td>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、重大税收违法失信主体或政府采购严重违法失信行为记录名单。</td></tr>
<tr><td>特定条件</td><td>依据信息系统特定的行业项目需求进行填写</td></tr>
<tr><td>项目背景和目标</td><td colspan="2">（描述项目背景和目标，包括为什么需要采购贵司软件以及期望实现甲方需求的目标）

（一）项目背景

医院是一个信息和技术密集型的行业，其计算机网络是一个完善的办公网络系统，作为一个现代化的医疗机构网络,除了要满足高效的内部自动化办公需求以外,还应对外界的通讯保证畅通。结合医院复杂的 HIsS、LIS、PACS 等应用系统，要求网络必须能够满足数据、语音、图像等综合业务的传输要求，所以在这样的网络上应运用多种高性能设备和先进技术来保证系统的正常运作和稳定的效率。同时医院的网络系统连接着 Internet、医保局和卫健委等，访问人员比较复杂，所以如何保证医院网络系统中的数据安全问题尤为重要。
在医院行业的信息化建设过程中，信息安全的建设虽然只是一个很小的部分，但其重要性不容忽视。便捷、开放的网络环境，是医院信息化建设的基础，在数据传递和共享的过程当中，数据的安全性要切实地得到保障，才能保障医院信息化业务的正常运行。然而，我们的数据却面临着越来越多的安全风险，时刻对业务的正常运行带来威胁。
为此， 2011 年 12 月，卫生部发布《卫生部办公厅关于全面开展卫生行业信息安全等级保护工作的通知》，要求卫生行业“全面开展信息安全等级保护工作”，《中华人民共和国网络安全法》（以下简称《网络安全法》）自 2017 年 6 月 1 日开始施行。其中，《网络安全法》第 21 条明确规定了“国家实行网络安全等级保护制度”。《网络安全法》是从国家层面对等级保护工作的法律认可，简单点就是单位不做等级保护工作就是违法。医院信息系统的安全性直接关系到医院医疗工作的正常运行，一旦网络瘫痪或数据丢失，将会给医院和病人带来巨大的灾难和难以弥补的损失。同时，医院信息系统涉及大量医院经营和患者医疗等私密信息，信息的泄露和传播将会给医院、社会和患者带来安全风险。</td></tr>
</table>

所以在信宜市人民医院的信息化建设过程中，我们应当正视可能面临的各种安全风险，对网络威胁给予充分的重视。为了我院信息网络的安全稳定运行，确保医院信息系统安全，根据我院目前的计算机信息网网络特点及安全需求，本着切合实际、保护投资、着眼未来的原则，提出本技术方案。

（二）项目目标

依照《卫生部办公厅关于全面开展卫生行业信息安全等级保护工作的通知》、《中华人民共和国网络安全法》、《网络安全等级保护基本要求》等标准，以及医院对信息系统等级保护工作的有关规定和要求，对医院的网络和信息系统进行等级保护定级，通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使得系统具有在统一安全策略管控下，保护敏感资源的能力。

通过技术体系和管理体系建设，使得信宜市人民医院网络系统的等级保护建设既可以满足等级保护的相关要求，又能够全方面为医院的业务系统提供持续的安全保护。

本项目建设将完成以下目标：

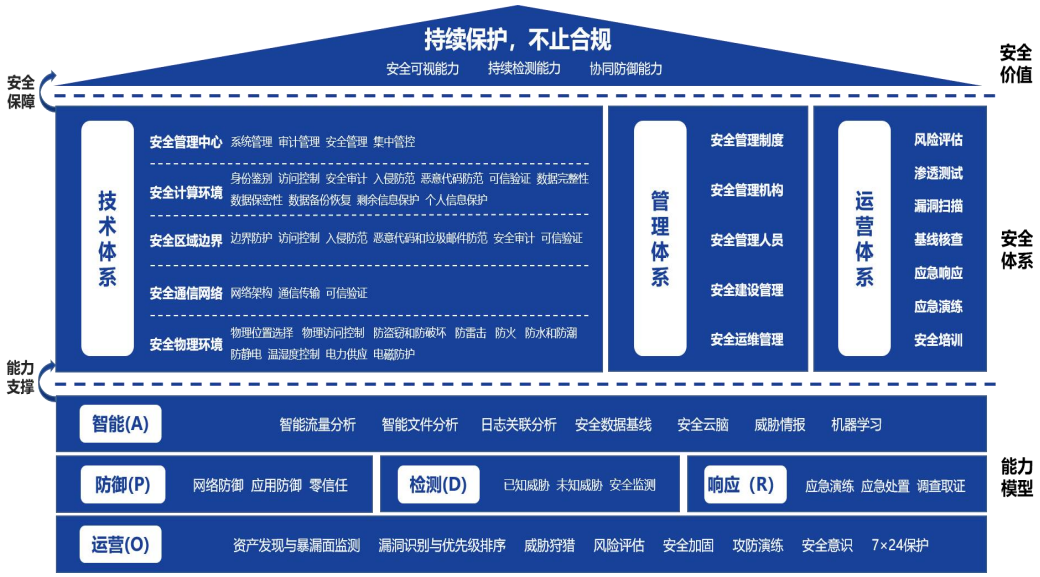
1、建立完善的安全技术防护体系。根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的有关规定要求，建立满足等级保护要求的安全技术防护体系，在满足安全合规基础上实现信宜市人民医院网络安全持续保护。

2、建立符合医院实际的安全管理组织机构，健全信息系统安全管理制度。根据网络安全等级保护的要求，制定各项信息系统安全管理制度，对安全管理人员或操作人员执行的重要管理操作建立操作规程和执行记录文档。

3、制定医院网络安全应急预案。应急预案是网络安全等级保护的重要组成部分，按可能出现问题的不同情形制定相应的应急措施，在系统出现故障和意外且无法短时间恢复的情况下能确保生产活动持续进行。

4、安全培训：为医院信息化技术人员提供信息安全相关专业技术知识培训和全员安全意识培训。

5、 完善信宜市人民医院整体安全规划，建立服务+技术+管理的整体安全体系，让医院安全规划更全面，安全更持续有效。

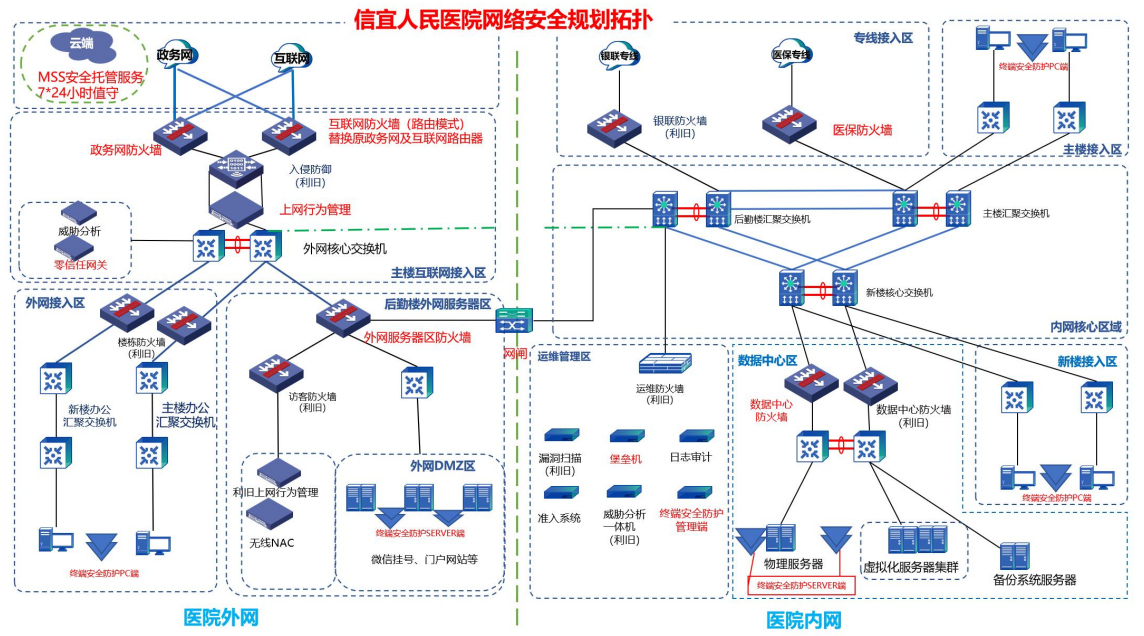


技术要求

（*内容多请另附页）

（一）主要功能用途：

基于我院现有的网络拓扑结构和业务发展规划，根据业务保障原则，按照业务系统工作职能、重要性的不同将网络划分为不同的安全区域。按照“一个中心、三重防护”的设计思路，对整体拓扑规划如下：



网络安全等级保护建设将从安全技术体系、安全管理体系、安全运营体系三个方面进行建设：

安全技术体系设计按照“一个中心”管理下的“三重防护”体系框架，构建安全机制和策略，形成网络安全综合技术防护体系。该安全保护环境主要分为安全计算环境、安全区域边界、安全通信网络和安全管理中心四个部分，最后结合安全的

物理环境构建体系化安全技术保障体系。

安全计算环境层面，通过加强用户身份鉴别、自主访问控制，强化系统自身的权限管控，通过运维审计、主机审计、数据库审计、应用审计等手段加强系统安全审计、保障事后追溯和分析能力，通过在所有主机和终端安全网络版防病毒软件，对各类病毒进行彻底查杀，建立恶意代码防范机制。

安全区域边界层面，通过下一代防火墙、全流量威胁分析系统、潜伏威胁探针和安全感知平台等边界检测和防护类设备，加强对关键网络区域边界访问控制、完整性保护、入侵防范和恶意代码防范，并通过全网行为管理、零信任等加强对非法内外联、互联网访问行为、远程接入行为的审计和管控。

安全通信网络层面，通过合理的分区分域降低系统性安全风险，针对关键通信线路、网络设备和计算设备采用冗余设计，保证系统高可用、网络设备的业务处理能力满足业务高峰期需要，并通过支持国产密码算法的 VPN 技术对广域网通信链路中的信息传输进行加密保护和完整性校验，确保通信链路的保密性和完整性。

安全管理中心层面，针对系统管理、安全管理、审计管理采取“三权分立”设计，保障系统、安全、审计管理员各司其职，通过独立的管理界面做好系统的管理工作。构建集中的管控中心，划分特定的安全运维区域、建立加密的安全运维管理链路，对全网系统和设备进行集中的状态检测、日志审计和分析，建立网络安全通报预警体系，对网络中发生的各类安全事件进行识别、报警和分析。

安全物理环境层面，对系统所涉及到的主机房、辅助机房和异地备份机房等进行物理安全设计，设计内容包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应及电磁防护等方面。

安全管理体系从安全管理制度、安全管理机构、安全管理人员、安全建设管理及安全运维管理等方面进行系统规划设计，加强网络安全管理，建立完善人员管理、教育培训、系统安全建设和运维等管理制度，加强机房、设备和介质安全管理，强化重要数据和个人信息保护，制定操作规范和工作流程，加强日常监督和考核，确保各项管理措施有效落实，最终做到整体防御、分区隔离；积极防护、内外兼防；自身防御、主动免疫；纵深防御、技管并重。

安全运营体系以漏洞和威胁作为要素，发挥技术体系安全效果、帮助管理体系更好落地，通过漏洞管理、安全评估、渗透测试、应急响应、应急演练、威胁检测与主动响应、网络安全培训和托管服务等运营机制为用户构建持续运营、安全闭环、

主动防御的安全运营体系。

（二）需求参数要求：（含软件和配套硬件等）

1. 国产防火墙（政务网，医保网，互联网出口）：

硬件要求：规格≥1U，内存大小≥8G，硬盘容量≥128G SSD，电源：单电源，接口≥6 千兆电口
性能要求：网络层吞吐量≥4G，应用层吞吐量≥2G，防病毒吞吐量≥600M，IPS 吞吐量≥600M，全威胁吞吐量≥400M，并发连接数≥200W，HTTP 新建连接数≥4.5W，IPSec VPN 最大接入数≥800，IPSec VPN 吞吐量≥500M
▲产品支持对不少于 9000 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制 （需提供产品功能截图证明，并加盖原厂公章）
▲产品支持 ftp 协议命令控制功能，至少包含 delete、rmdir、mkdir、rename、mget、dir、mput、get、put 等，保护对外服务不被恶意篡改（需提供产品功能截图证明，并加盖原厂公章）
▲产品内置不低于 10000 种漏洞规则，同时支持在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则 （需提供产品功能截图证明，并加盖原厂公章）
产品支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性
产品支持静态路由、策略路由和多播路由协议，并支持 BGP、RIP、OSPF 等动态路由协议
产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护
产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议
产品支持 Web 管理、串口管理、SSH 管理等多种不同方式
产品支持多种安全日志存储方式，至少包括防火墙本机、日志服务器等不同方式
软件升级≥3 年，产品质保≥3 年

2. 国产互联网行为审计：

硬件要求：规格≥1U，内存大小≥8G，硬盘容量≥128G SSD，电源：单电源，接口≥6 千兆电口
性能要求：网络层吞吐量（大包）≥3Gb，应用层吞吐量≥300Mb，带宽性能≥200Mb，IPSEC VPN 加密性能（最高性能）≥50Mb，支持用户数≥1000，包转发率≥27Kpps，每秒新建连接数≥2400，最大并发连接数≥120000
支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；（需提供产品功能截图证明，并加盖原厂公章）
支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况（需提供产品功能截图证明，并加盖原厂公章）

支持通过 OAuth 认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证
▲设备内置海量预分类的 URL 地址库，能够针对各种 URL 类型做识别和分类，同时所有 URL 类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制（需提供产品功能截图证明，并加盖原厂公章）
URL 数量在 3000 万以上，包含分类数量 150 个以上
▲设备内置应用识别规则库,支持超过 9000 种以上应用规则数、支持超过 6000 种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制；（需提供产品功能截图证明，并加盖原厂公章）
▲支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义（需提供产品功能截图证明，并加盖原厂公章）
▲支持通过抑制 P2P 的下行丢包，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题（需提供产品功能截图证明，并加盖原厂公章）
支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为（包括包括钓鱼及恶意网站、漏洞利用、挖矿页面、恶意跳转、跨站脚本攻击和病毒文件等），避免用户网页资源被滥用；支持实时阻断和告警
软件升级≥3 年，产品质保≥3 年

3. 国产防火墙（外网服务器区）：

硬件要求：规格≥1U，内存大小≥16G，硬盘容量≥128G SSD，电源：冗余电源，接口≥6 千兆电口
性能要求：网络层吞吐量≥20G，应用层吞吐量≥15G，防病毒吞吐量≥2G，IPS 吞吐量≥2G，全威胁吞吐量≥1.5G，并发连接数≥800 万，HTTP 新建连接数≥16 万，IPSec VPN 最大接入数≥1500，IPSec VPN 吞吐量≥1G
产品支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御
产品支持勒索病毒检测与防御功能，需提供产品功能截图证明，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“勒索病毒”的证书或检测报告证明功能有效性。
▲产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 120 万种，可识别主机的异常外联行为 （需提供产品功能截图证明，并加盖原厂公章）
▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生 （需提供产品功能截图证明，并加盖原厂公章）
产品支持 3 种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证
产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求

产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护、Smurf 攻击防护、Land 攻击防护、WinNuke 攻击防护等攻击类型
产品支持基于文件传输方式、文件类型等维度的管控策略配置
产品支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间
软件升级≥3 年，产品质保≥3 年

4. 国产防火墙（数据中心）：

硬件要求：规格≥2U，内存大小≥16G，硬盘容量≥128G SSD，电源：冗余电源，≥6 千兆电口，≥2 万兆光口 SFP+
性能要求：网络层吞吐量≥20G，应用层吞吐量≥18G，防病毒吞吐量≥4G，IPS 吞吐量≥4G，全威胁吞吐量≥2G，并发连接数≥800 万，HTTP 新建连接数≥16 万，IPSec VPN 最大接入数≥1500，IPSec VPN 吞吐量≥1G
产品支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上
产品支持杀毒白名单设置，可以例外排除特定 MD5 和 URL 的病毒文件，针对特定文件不进行查杀
▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理 （需提供产品功能截图证明，并加盖原厂公章）
产品支持基于 IP 对象的会话控制策略，实现并发连接数的合理限制
产品支持基于网络区域、网络对象、MAC 地址、服务、应用等维度进行访问控制策略设置
产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护
产品支持三权分立功能，根据管理员权限分为安全管理员、审计员、系统管理员三种角色
产品支持 SNMP V1/V2/V3/Trap 等标准网络管理协议
软件升级≥3 年，产品质保≥3 年

5. 国产终端安全管理系统：

≥230 套终端安全管理系统（服务器端+PC 端）
▲提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数 （需提供产品功能截图证明，并加盖原厂公章）
具备终端侧系统层、应用层行为数据采集能力，数据采集面覆盖 ATT&CK 技术面 160 项
▲支持以可视化形式展现攻击故事，提供可视化的进程树溯源，可直观看出攻击入口、相关操作行为、高危实体文件等信息，协助客户进行事件攻击溯源和研判分析（需提供产品功能截图证明，并加盖原厂公章）
支持对攻击事件深度分析，展示每步关键进程相关的文件行为、域名访问行为、进程操作行为、命令行参数等攻击相关的关键行为，帮助用户快速

了解攻击者操作，洞悉目的和危害面
支持基于终端侧采集记录的行为数据，对文件变更、进程变更、网络连接、DNS 查询等多种行为，在全网中搜索命中指定条件的端点和行为，进行高级威胁的狩猎对全网终端发起威胁狩猎，挖掘潜伏攻击
支持主流国产化操作系统，如中标麒麟、银河麒麟、统信等
采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能
支持收集并展示单个终端的基本信息，包括：主机名、在线/离线状态、IPv4 地址、MAC 地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新
支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户
支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴
通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整 EDR 的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务零摩擦
构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置
支持在管理平台下发终端漏洞扫描任务，并针对已发现的漏洞提供相应的修复建议
软件升级≥3 年

6. 运维审计：

硬件要求：规格≥1U，内存大小≥16G，硬盘容量≥64GB SSD+1TB SATA，电源：单电源，≥6 千兆电口，≥4 千兆光口 SFP
性能要求：授权资源数≥50 点授权（最高支持 150），并发数字符≥100 / 图形 50
▲支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（需提供产品功能截图证明，并加盖原厂公章）
支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批（需提供产品功能截图证明，并加盖原厂公章）
支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作
全面支持 IPV6，设备自身可以配置 IPV6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登陆和审计
支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人（需提供产品功能截图证明，并加盖原厂公章）

支持从 windows AD 域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式
支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断
支持对常见设备运维操作进行记录（至少包括 windows 主机、linux/unix 主机、网络设备等），审计信息至少包括以下内容：用户账户、起止时间、登陆 IP、设备 IP、设备名称、设备类型、访问账号、访问协议等信息
支持日志数据的外置存储，支持 FTP、SFTP 和 NAS 文件共享协议
软件升级≥3 年，产品质保≥3 年

7. 国产网闸：

硬件要求：规格≥2U，≥8 个千兆电口，≥4 个千兆光口
性能要求：CPU≥8 核 2.3GHz*2，内存≥18G，硬盘企业级≥2TB，≥500 个并发文件交换请求，≥10GB 的文件交换

8. 国产零信任综合网关：

硬件要求：规格≥1U，内存大小≥16G，硬盘容量≥128G SSD，电源：单电源，≥6 千兆电口，≥4 千兆光口 SFP
性能要求：最大理论加密流量（Mbps）≥300Mbps，最大理论并发用户数≥600
▲支持配置点击工作台的业务应用即可直接拉起对应的 CS 程序进行访问，包括但不限于浏览器、远程桌面或其他指定程序，支持 Windows、macOS、统信 UOS、麒麟 kylin、Ubuntu 等主流操作系统；针对 Windows 系统，还应支持拉起 CS 应用时携带启动参数，自动访问管理员设定的地址（需提供产品功能截图证明，并加盖原厂公章）
1、为提升在弱网环境下访问体验，应支持优化 TCP 协议，增强隧道抗丢包、抗抖动特性，实现弱网环境的访问加速 2、为降低业务访问时延，提升访问体验，应支持将短隧道资源新建连接耗时优化至 0RTT，大幅降低业务访问的网络时延，实现同等网络环境下访问速度达到直连访问
1、为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告 2、支持在设备上查看及下载巡检报告 3、报告应至少包含检测项、检查状态、存在的问题描述、建议改进措施等
▲为提升 WEB 业务的数据安全性，应支持禁止对 WEB 应用禁止复制、禁止打印、禁止下载、禁止鼠标右键、禁止浏览器调试，以保护应用的数据安全也应用安全（需提供产品功能截图证明，并加盖原厂公章）
对于一些主要在主站点中点击使用的子站点 WEB 业务系统，且子站点跟主站点业务系统权限一致的场景，为简化管理员配置，零信任系统应支持开启依赖站点功能 为方便业务快速上线，还应支持自动采集站点功能对

依赖站点进行梳理
1、为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持 UDP+TCP 组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞 2、PC 端和移动端均支持通过安全码激活客户端为授权客户端，从而可进行 SPA 敲门和连接，安全码支持共享码和一人一码两种模式，支持短信分发安全码，保障业务的安全性 3、一人一码模式下，当实际登录用户跟分发 SPA 安全码绑定的用户不一致时，零信任系统可以产生安全告警，帮助管理员溯源，进一步提升系统安全性
为了使系统资源利用最大化，本地集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和
为方便维护人员管理应用权限，支持直接在应用授权界面为单一应用或某个应用分类分配用户授权，授权方式支持直接授权给用户所在的组织架构、用户关联的角色或用户本身，并展示应用直接授权的组织架构、授权角色或用户数量
为了进一步保障用户身份安全，需支持多因素认证，支持管理员结合已对接的主认证和辅认证类型进行设置，可自由选择采用首次认证+二次认证+终端认证+增强认证等方式
软件升级≥3 年，产品质保≥3 年

9. 安全托管服务：

安全运营服务以保障网络安全“持续有效”为目标，围绕资产、漏洞、威胁、事件四个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式 7*24H 持续性开展网络安全保障工作，与用户一同构建持续（7*24 小时）、主动、闭环的安全运营体系
暴露面梳理：投标方应使用安全工具对招标方服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险 投标方应具备互联网暴露面梳理的服务工具，该工具应当支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP 地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标方举证，及对应暴露资产存在的漏洞需提供服务工具具备以上暴露面梳理能力的证明截图
高危可利用漏洞防护：针对服务范围内资产扫描到的高危可利用漏洞，投标方应当为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失；需提供服务平台具备高危可利用漏洞防护规则的证明，并且支持对扫描到的高危可利用漏洞能够自动匹配漏洞防护规则； 服务承诺：要求招标方可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到 99%
7*24 小时威胁鉴定：投标方应当具备云端检测和分析平台，通过采集招标方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术

		手段，为招标方提供 7*24 小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；分析研判包括但不限于对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，支持将同一资产的多个告警进行聚合分析发现各类安全事件并生成工单，并在告警详情中展示告警的基本信息，涉及的业务信息、攻击趋势、威胁详情、攻击原理、处置建议等内容，并支持根据客户情况提供备注；需提供云端服务平台告警审核功能界面截图，举证一个告警聚合分析的例子和一个告警详情展示具备上述能力；
		个性化的检测规则定制：为了保证安全监测的准确率和服务质量，投标方应当支持为招标方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求；需提供投标方服务平台支持为用户自定义配置安全规则的截图； 服务承诺：为了应对日益严峻的安全风险，要求投标方承诺支持为用户服务范围内资产定制不少于 3 个的个性化安全检测规则
		受影响资产排查与加固：安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固 提供一个威胁情报的安全通报工单的截图证明，工单内容包含威胁情报的基本信息和推送信息以及跟进记录，要求明确说明关联资产信息的排查情况
		安全策略检查：投标方安全专家每月对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果 投标方云端服务平台应当具备丰富的策略检查工具（要求不少于 40 种策略检查的工具），支持排查安全设备防护策略配置的合理性 提供投标方云端服务平台策略检查工具的截图证明
		为了保障服务质量和加强投标方与招标方的沟通，投标方应当承诺为招标方配置一名经验丰富的安全专家作为专属服务经理，并且实时响应投标方咨询的网络安全相关问题；
		投标方应当为招标方提供 7*24 小时的安全守护，不论是白天、黑夜、节假日投标方都应该能做到 7*24H 在线服务，并且在节假日期间应当每日为招标方提供《节假日值守总结》 服务承诺：投标方应当向招标方承诺，不论白天、黑夜、节假日投标方都能为招标方提供 7*24H 在线服务，并且在节假日期间能为招标方提供每日的《节假日值守报告》
		为了降低招标方因网络安全事件造成的损失和影响，投标方应当按照以下服务指标和要求为招标方提供服务：
		（1）从安全日志产生到事件通告给招标方的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于 30 分钟，一般事件的通告时间少于 1 小时
		（2）在配备投标方的边界防护服务组件和终端防护服务组件的情况下，高级威胁的处置完成时间少于 1 小时，一般威胁的处置完成时间少于 4 小时
		（3）安全事件经过服务人员的确认后，通告给招标方的各类安全事件的准确率不低于 99%（即误报不能超过 1%）
		（4）投标方应当承诺，服务范围内的所有安全事件的闭环处置比例达到 100%
		（5）投标方应当满足重大事故应启动应急响应机制，工作时间 15 分钟之内云端专家进行响应，非工作时间 30 分钟之内云端专家进行响应，省会 2 小时上门处置，省内 8 小时上门处置 投标方对标该服务指标进行应答，需提供服务承诺函

		（6）在具备投标方的边界防护组件的情况下，要求招标方可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到 99%，投标方对标该服务指标进行应答，需提供服务承诺函
		服务质量监控： 投标方需为招标方提供的服务成果展示门户（或用户 Portal）应具备服务质量可视化展示，投标方能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，以验证投标方所承诺的服务指标（或称为服务 SLA） 提供服务成果展示门户中服务质量监控相关的截图证明
		服务交付物管理： 投标方需为招标方提供的服务成果展示门户（或用户 Portal），可以直观的管理服务过程中生产的服务报告和交付物，包括但不限于《准备阶段文件》、《特殊时期值守报告》、《运营周报》、《运营月报》、《运营季报》、《威胁情报》、《年度汇报》、《事件总结报告》 提供服务成果展示门户中支持下载和管理上述交付物的相关截图证明
		投标方云端服务平台应当支持对接招标方网络中已部署的主要安全设备，如下一代防火墙、安全态势感知、终端检测与响应等，支持实时接收安全设备检测到的安全事件信息、安全日志数据提供 7*24 小时的安全托管服务；提供云端服务平台支持对接的上述安全设备的能力证明截图，展示详细的对接步骤
		投标方应当基于最小原则详细说明云端服务需要采集的数据类型和内容，并说明其用途和信息存储方案及保护方案；要求投标方提供上述内容的详细说明，以服务承诺函的形式提供相关证明材料
		投标方云端服务平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务平台至少通过等级保护三级测评；投标方应当提供云端服务平台等级保护三级测评通过证明，提供报告首页、基本信息表、等级测评结论首页，以上内容中必须明确指出该平台用于为用户提供 7*24 小时的安全托管服务；（敏感内容投标方可脱敏展示） 投标方云端服务平台应通过国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部四部委联合组织的云计算服务安全评估，入选“通过云计算服务安全评估的云平台”名单，以确保平台的安全性和可控水平；提供中央网络安全和信息化委员会办公室、国家互联网信息办公室官方网站发布的《通过云计算服务安全评估的云平台》入选名单作为证明（名单截图），需明确写明为安全托管服务运营平台
		了保障服务效率和质量，投标方的云端服务平台应当具备一套完善的流程编排引擎，能够为客户灵活编排、定义服务流程，并且定义服务的 SLA，将服务过程中的各个关键环节按照一定的顺序和规则进行组织和安排，以达到高效、优质的服务目标；投标方应当提供云端服务平台具备上述流程编排能力的证明
		投标方的安全运营平台的平台能力和人员服务能力需要符合《面向云计算的安全运营中心能力要求》标准，获得云计算开源产业联盟和中国信息通信研究院的认证
		投标方的安全运营服务平台应当通过国家互联网信息办公室、国家发展和改

革委员会、工业和信息化部、财政部四部委联合组织的云计算服务安全评估，入选“通过云计算服务安全评估的云平台”名单

（五）配置清单：（包括各种配件写明规格和数量，电脑要列明详细的配置，无此项内容则写“无”。）

*配置清单（外置或特殊要求）				
序号	名称	单位	数量	备注
1	防火墙(政务，互联网，医保)	台	3	
2	互联网行为审计	台	1	
3	防火墙（外网服务器区）	台	1	
4	防火墙（数据中心）	台	1	
5	国产化非涉密 aES	套	230	
6	运维审计	台	1	
7	网闸	台	1	
8	零信任综合网关	台	1	
9	安全托管服务	套	1	

(一)其它技术指标要求：

★本项目包含网络安全加固建设项目与医院各个系统的的网络安全等级保护测评整改项目内容，在医院每年度的网络安全等级保护测评中，等保测评公司检测出的整改问题供应商在硬件维保期限内需按照差距评估报告对本次采购设备进行协助整改。

四、商务要求

(一)实施开发人员服务要求：

1. 项目经理的要求

在医疗行业具有 3 年以上同类项目实施经验；担任项目经理两年或以上；

2. 实施人员的要求

应具有两年或以上同类项目实施经验；

3. 其它

最终成交人应保证项目成员的稳定，如确因工作安排或其他原因需更换时，须事先征得采购人同意，

否则不能擅自更换。更换工作组成员时，应至少提前 5 个工作日以书面形式通知采购人，并取得采购人同意方可更换工作组成员。如采购人要求更换不称职的项目代表时，最终成交人保证全力在采购人指定的时间内更换同等或更高资历的人员。

(二)培训

1.培训采购人工程师，主要内容为系统的开发、实施、运营等，培训地点主要按招标方安排，需使采购人人员能熟练操作及应用全部系统。确保采购人系统管理员能够熟练地对系统进行运行、诊断、维护和管理。

2.确保本项目相关业务人员能熟练使用应用系统。

3.培训内容：

1）系统使用维护培训：要求对所有相关人员进行现场系统使用、维护培训，时间不少于 2 周；

2）从现场调试开始，对操作管理人员进行现场培训，并提供不少于 2 次的全院使用培训，指导业务部门用户培训熟悉掌握平台所有操作，提供相关操作文档和 PPT，直到系统操作人员能使系统正常运行为止；

(三)售后服务

1.本项目要求自到货签收之日起提供三年的免费售后服务，提供 7*24 小时免费售后服务。

2.▲签收使用后三年内免费维护（包含一名工程师 1 名，按需到场，负责沟通需求、更新维护、系统巡检等），在工程实施及售后服务期间维持医院系统的良好运行，该驻场工程师有相关实施经验，接受医院统一管理，若不符合医院要求，医院有权要求更换现场维护人员。

3.医院工作日白天(6:30-18:00)故障响应时间不超过 30 分钟，非工作日及夜间故障响应时间不超过 60 分钟。出现故障后，故障在 1 小时内排除（可以使用远程维护、远程指导等手段），2 小时内排除重要故障（包括因系统原因、外界原因引起的故障）。现场人员不能排除故障时，通过电话线或 VPN 方式远程登陆到院方网络系统进行免费的故障诊断和故障排除。如在规定时间内无法有效处理，则采取应急措施解决，不影响采购人的正常工作业务。

4.免费维护期内，最终成交人提供软件升级服务。

(四)验收要求

1.设备到货签收后 1 周内无质量问题反馈可发起验收申请，以双方签字的验收报告作为付款依据。

2.验收按国家有关的规定、规范进行。验收时如发现所交付的设备有不符合招标方需求之情形者，最终成交人应作出详尽的说明，并由采购人签署同意需求迁改方可进行验收。由此产生的有关费用由最终成交人承担。

3.最终成交人保证本项目提供的设备不侵犯任何第三方的专利、商标或版权。否则，最终成交人须承担对第三方的专利或版权的侵权责任并承担因此而发生的所有费用。

4.▲验收前，最终成交人必须完成采购人信息数据处工程师的培训，最终成交人不得以任何理由拒

绝或延迟完成采购人提出的合理需求。

（五）付款方式

1. 合同签订生效后 10 个工作日内，采购人支付合同总价的 30%款项；

2. 设备到货签收后 10 个工作日内，采购人支付合同总价的 30%款项；

3. 设备上架运行 1 个月后，采购人支付合同总价的 35%款项；

4. 维保期满三年后 10 个工作日内，采购人支付合同总价的 5%款项。

第三章　报名文件格式

（请报名人按照以下文件的要求格式、内容、顺序制作报名文件，并请编制目录及页码，否则可能将影响对报名文件的评价。）

报 名 文 件

（正本/副本）

项目名称：_____

报名人名称（盖章）：_____

报名人地址：_____

联 系 人：_____

联系电话：_____

报名文件目录

备注：

1. 根据报名文件资料由办公软件自动更新页码，请仔细查验是否添加页码；

2、本模板提供参考格式的参考格式，如没有可自拟格式；

3、按《报名文件目录》的顺序装订成册。

初步评审自查表

序号	审查内容	自查结论	证明资料
1	报名函（参考格式 1）	通过或不通过	见报名文件第（）页
2	资格声明函（参考格式 2）	通过或不通过	见报名文件第（）页
3	报名人基本情况表（参考格式 3）		见报名文件第（）页
4	法定代表人（负责人）证明书（参考格式 4）	通过或不通过	见报名文件第（）页
5	法定代表人（负责人）授权委托书（参考格式 5）	通过或不通过	见报名文件第（）页
6	法人或其他组织的营业执照等证明文件（具有独立承担民事责任能力的在中华人民共和国境内注册的法人或其它组织）	通过或不通过	见报名文件第（）页
7	本项目不接受联合体报名。	通过或不通过	//
8	报价有效期：90 日	通过或不通过	//
9	报价一览表（参考格 6）	通过或不通过	见报名文件第（）页
10	能满足用户需求的主要参数（带“★”号条款）	通过或不通过	见报名文件第（）页
11	报名文件按照规定要求签署、盖章	通过或不通过	见报名文件第（）页
12	报名人满足采购文件的要求	通过或不通过	见报名文件第（）页
13	未出现恶意竞争低于成本价的情形	通过或不通过	见报名文件第（）页
14	无采购文件中规定的被视为无效报名的其它条款的	通过或不通过	见报名文件第（）页
15	未出现法律、法规、规章规定属于报名无效的其他情形	通过或不通过	

备注：

1、以上材料将作为报名人合格性和有效性审核的重要内容之一，报名人必须严格按照其内容及序列要求在报名文件中对应如实提供，对缺漏和不符合项将会直接导致无效报名。

2、报名人须在“自查结论”栏填写通过或不通过，在“证明资料”栏填写页码。

商务评审自查表

《商务评审表》响应情况：

序号	评审分项	内容	证明文件（如有）
1			见报名文件（　）页
2			见报名文件（　）页
3			见报名文件（　）页
4			见报名文件（　）页
5			见报名文件（　）页
…			

注：报名人应根据**第一章第三条询价原则** 中的《商务评分》的各项内容填写此表。

技术评审自查表

《技术评审表》响应情况

序号	评审分项	内容	证明文件（如有）
1			见报名文件（　）页
2			见报名文件（　）页
3			见报名文件（　）页
4			见报名文件（　）页
5			见报名文件（　）页

注：报名人应根据**第一章第三条 询价原则** 《技术评审表》的各项内容填写此表。

其他商务及技术响应情况表

序号	内容	证明文件（如有）
1		见报名文件（ ）页
2		见报名文件（ ）页
3		见报名文件（ ）页
4		见报名文件（ ）页
5		见报名文件（ ）页
…		

注：本表用于填写**非**《商务评审表》和**非**《技术评审表》清单内的其他响应情况。

本表内容不作为评分项，但是有利于更好展示公司实力、设备性能优势、服务实力等方面。

格式 1：报名函

报名函

致：中山大学附属第六医院粤西医院/信宜市人民医院

根据贵院采购项目名称：中山大学附属第六医院粤西医院信宜市人民医院******采购项目的采购公告、采购文件要求，我方签字代表_____(全名及职衔)经正式授权并以报名人(报名人名称、地址)的名义报名，并提交报名文件。

在此，我方声明如下：

1. 我方同意并接受采购文件的各项要求，遵守采购文件中的各项规定，按采购文件的要求提供报价。

2. 我方同意报名有效期为报名截止日起 90 日。如果我方报名的项目确定成交，报名有效期延长至合同验收之日。

3. 我方已经详细地阅读并完全明白了全部采购文件及附件，包括澄清、修改（如有）和所有已提供的参考资料以及有关附件，我方完全明白并认为此采购文件没有倾向性，也不存在排斥潜在报名人的内容，我方同意采购文件的相关条款，放弃对采购文件提出误解和质疑的一切权力。

4. 我方已毫无保留地向贵方提供一切所需的证明材料。

5. 我方完全服从和尊重评委会所作的评定结果，同时清楚理解到报价最低并非意味着必定获得成交资格。

6. 完全理解医院拒绝迟到的任何报名和最低报名报价不是被授予成交的唯一条件。

7. 如果我方未对采购文件要求作实质性响应，则完全同意并接受按无效报名处理。

8. 我们证明提交的一切文件，无论是原件还是复印件均为准确、真实、有效、完整的，绝无任何虚假、伪造或者夸大。我们在此郑重承诺：在本次采购活动中，如有违法、违规、弄虚作假行为，采购人有权取消我方的报名及成交资格，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

（注：本报名函内容不得擅自删改，否则视为无效报名）

报名人名称（盖公章）：_____

报名人授权代表（签字或盖章）：_____

联系方式：_____

日期：_____年_____月_____日

格式 2：资格声明函

资格声明函

致：中山大学附属第六医院粤西医院/信宜市人民医院

关于贵方采购项目名称：中山大学附属第六医院粤西医院/信宜市人民医院******项目报名邀请，参与报名，提供用户需求书中规定内容，并按采购文件要求提交所附资格文件且声明和保证如下：

1．我方为本次报名所提交的所有证明其合格和资格的文件是真实的和正确的，并愿为其真实性和正确性承担法律责任。

2．我方是依法注册的法人，在法律上、财务上和运作上完全独立于中山大学附属第六医院粤西医院/信宜市人民医院。

3．我方具备《政府采购法》第二十二条规定的条件：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中无重大违法记录；

（6）法律、行政法规规定的其他条件。

4．单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参与本项目报名（响应）。

5．我方未被列入“信用中国”网站(www.creditchina.gov.cn)“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单。

特此声明！

报名人名称（盖公章）：_____

报名人授权代表（签字或盖章）：_____

日　　期：_____年_____月_____日

格式 3：报名人基本情况表

报名人基本情况表

<table>
<tr><td>单位名称</td><td colspan="7"></td></tr>
<tr><td>营业执照号</td><td colspan="7"></td></tr>
<tr><td>地址</td><td colspan="7"></td></tr>
<tr><td>法人代表</td><td colspan="2"></td><td>职务</td><td colspan="3"></td></tr>
<tr><td>授权代表</td><td colspan="2"></td><td>职务</td><td colspan="3"></td></tr>
<tr><td>邮编</td><td></td><td>电话</td><td></td><td>传真</td><td colspan="3"></td></tr>
<tr><td rowspan="4">单位概况</td><td>注册资本</td><td>万元</td><td colspan="2">占地面积</td><td colspan="3">m^2</td></tr>
<tr><td>职工总数</td><td>人</td><td colspan="2">建筑面积</td><td colspan="3">m^2</td></tr>
<tr><td rowspan="2">资产情况</td><td>净资产</td><td colspan="2">万元</td><td colspan="3">固定资产原值 万元</td></tr>
<tr><td>负债</td><td colspan="2">万元</td><td colspan="3">固定资产净值 万元</td></tr>
<tr><td colspan="2">公司开户银行名称及账号</td><td colspan="6"></td></tr>
<tr><td rowspan="2">财务状况</td><td>年度</td><td>营业收入（万元）</td><td>资产总额（万元）</td><td>利润总额（万元）</td><td>净利润（万元）</td><td>资产负债率</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">证书情况</td><td>证书名称</td><td>证书等级</td><td colspan="2">发证单位</td><td colspan="3">证书有效期</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="4">企业规模
（根据行业划型标准，填入“大型企业”、“中型企业”、“小型企业”或“微型企业”</td><td colspan="4"></td></tr>
<tr><td>公司简介</td><td colspan="7"></td></tr>
</table>

注：1．文字描述：企业性质、发展历程、经营规模及服务理念、主营产品、技术力量等；

2．图片描述：经营场所、主要经营项目等；

3．如报名此表数据有虚假，一经查实，自行承担相关责任。

格式 4：法定代表人（负责人）资格证明书

法定代表人（负责人）资格证明书

_____现任我单位_____ 职务，为法定代表人（负责人），特此证明。

有效期限与本公司所提交的报名文件标注的报名有效期一致。签发日期：_____年_____月____日

附：

代表人性别：_____年龄：_____身份证号码：_____

营业执照注册号：_____ 企业类型：_____

经营范围：_____

_____

_____。

法定代表人（负责人） 居民身份证**正反面**复印件粘贴处

报名人名称（盖公章）：_____

地　　址：_____

日　　期：_____

注：法定代表人是指营业执照中注明的“法定代表人”

负责人是指营业执照中注明的“负责人”

格式 5：法定代表人（负责人）授权委托书

法定代表人（负责人）授权委托书

本授权书声明：注册于（公司地址）的（报名人名称）在下面签字的[法定代表人（或负责人）姓名、职务]代表本公司授权（单位名称）的（授权代表姓名、职务）为本公司的合法代理人，就中山大学附属第六医院粤西医院/信宜市人民医院*********项目活动，提交报名文件及采购合同的签订、执行、完成和售后服务，作为报名人代表以本公司的名义处理一切与之有关的事宜。

被授权人（报名企业授权代表）无转委托权限。

本授权书于_____年_____月_____日签字之日起生效，特此声明。

附：

报名人名称（盖公章）：_____

地址：_____

法定代表人（或负责人）签字或盖章：_____

报名人代表（授权代表）签字或盖章：_____

职务：_____

注：法定代表人是指营业执照中注明的“法定代表人”

负责人是指营业执照中注明的“负责人”

报名人代表（授权代表） 居民身份证**正反面**复印件粘贴处

格式 6：报价一览表

项目名称：_____

报价公司：_____ 报价日期：_____

联系人：_____ 联系电话：_____

序号	主要功能模块名称及（或）设备名称	品牌型号	数量	单位	分项单价（元）	分项总价（元）
1						
2						
…						
总价： （小写）人民币_____元，（大写）人民币_____元整						
供应商确认	1. 企业规模： ☐大型企业 ☐中型企业 ☐小型企业 ☐微型企业 ☐其他 ； 2. 报价包括货物费用及安装调试、验收、培训、税费、服务期限内的一切技术和售后服务、管理费、人工费、服务人员费用、各项税费及合同实施过程中一切可见及不可预见费用。 3. 其它说明： 签名确认： （单位公章） 年 月 日					

注：1.报名人须按要求填写所有信息，不得随意更改本表格式。

2.报价包含的内容及要求见第二章用户需求书的“**报价说明**”。

3.以人民币报价。

格式 7：★实质性要求响应表

序号	★实质性要求内容	报价响应详细内容	正/负/无偏离	偏离说明	报名文件响应页码
…					

报名人必须将对采购文件**第二章 用户需求书 中的“三、技术要求”、“四、商务要求”**有关“★”号的实质性要求进行响应，响应详细内容和页码填写此表。

备注：

1、采购文件用户需求成交有“★”的指标均被视为实质性响应指标，报名人如有一项带“★”的指标未响应或不满足，将按无效报价处理。

2、如采购文件用户需求书上无标有“★”实质性响应指标的，无需填写该表格。

3、承诺以上响应情况属实，如有虚假响应同意本项目一票否决，并列入采购人黑名单供应商。

格式 8：▲重要性技术要求响应表

序号	▲重要性技术要求内容	报价响应详细内容	正/负/无偏离	偏离说明	报名文件响应页码
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
..					

报名人须对采购文件**第二章 用户需求书 中的“三、技术要求”**中有关“▲”号的重要性要求进行响应，响应详细内容和页码填写此表。

备注：

1、采购文件用户需求成交有“▲”的指标均被视为重要性要求，报名人如有一项带“▲”的指标未响应或不满足，将可能导致严重扣分。

2、如采购文件用户需求书中无标有“▲”重要性指标，请在表格上填写“无”。

3、承诺以上响应情况属实，如有虚假响应同意本项目一票否决，并列入采购人黑名单供应商。

格式 9：▲重要性商务要求响应表

序号	▲重要性商务要求内容	报价响应详细内容	正/负/无偏离	偏离说明	报名文件响应页码
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
..					

报名人须对采购文件**第二章 用户需求书 中的 “四、商务要求”**中有关“▲”号的重要性要求进行响应，响应详细内容和页码填写此表。

备注：

1、采购文件用户需求成交有“▲”的指标均被视为重要性要求，报名人如有一项带“▲”的指标未响应或不满足，将可能导致严重扣分。

2、如采购文件用户需求书中无标有“▲”重要性指标，请在表格上填写“无”。

3、承诺以上响应情况属实，如有虚假响应同意本项目一票否决，并列入采购人黑名单供应商。

格式 10：一般技术要求响应表

序号	一般技术要求内容	报名人响应详细内容	正/负/无偏离	偏离说明	报名文件响应页码
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

备注：

1、本表根据采购文件**第二章 用户需求书 中的“三、技术要求”**除带“★”和“▲”条款之外，报名人须逐条详细响应并作出标注**“正偏离/负偏离/无偏离”**，“**正/负偏离**”的请在偏离说明栏目中具体说明及填写页码；

2、承诺以上响应情况属实，如有虚假响应同意本项目一票否决，并列入采购人黑名单供应商。

格式 11：一般商务要求响应表

序号	商务要求内容	报名人响应详细内容	正/负/无偏离	偏离说明	报名文件响应页码
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

备注：

1、本表根据采购文件**第二章 用户需求书 中的“四、商务要求”**，除带“★”和“▲”条款之外，报名人须逐条详细响应并作出标注**“正偏离/负偏离/无偏离”**，“**正/负偏离**”的请在偏离说明栏目中具体说明及填写页码；

2、如需求书未明确区分服务和商务条款，本表可略过，全部需求在服务条款响应表进行响应；

3、承诺以上响应情况属实，如有虚假响应同意本项目一票否决，并列入采购人黑名单供应商。

格式 12：管理体系认证

管理体系认证

（格式可自拟）

格式 13： 2020 年至今同类项目业绩一览表

同类项目业绩一览表

序号	客户名称	项目名称	合同金额（万元）	签约日期及完成时间	联系人及电话
1					
2					
3					
…					

备注：

1、**须提供合同关键页复印件**，要求能清晰看出项目内容等，否则视为无效业绩。

2、承诺以上提供信息属实，如有虚假同意本项目一票否决，并列入采购人黑名单供应商。

格式 14：项目人员配备情况

项目人员配备情况

（格式可自定）

格式 15：实施服务方案

实施服务方案

（格式可自定）

格式 16：售后服务方案

售后服务方案

（格式可自定）

格式 17：项目文档移交方案

项目文档移交方案

（格式可自定）

格式 18：其他

（标题）

（格式可自定，标题需清晰，并在目录页体现）