赣榆区政府采购

招标文件

标段名称：赣榆区中医院信息安全建设项目

标段编号：320721-J-GYJZ2023G020-1

采购人：连云港市赣榆区中医院

采购代理机构：赣榆区公共资源交易中心

2023 年 10 月

目录

目录 2
第一部分投标邀请 3
第二部分投标人须知 8
第三部分评标办法 18
第四部分项目需求 20
第五部分合同 27
第六部分投标文件格式 2726

新点网上招投标系统

第一部分　投标邀请

项目概况

赣榆区中医院信息安全建设项目招标项目的潜在投标人应在连云港市公共资源电子交易系统获取招标文件，并于 2023 年 10 月 31 日 9 点 00 分 00 秒（北京时间）前**上传电子投标文件**。

一、项目基本情况

标段编号：　320721-J-GYJZ2023G020-1

标段名称：赣榆区中医院信息安全建设项目

预算金额：104 万元。

最高限价：104 万元。

采购需求：为了满足医院信息系统可以稳健、高效、安全的运行，同时为了满足医院等保安全建设需要，参考三甲医院信息化建设方案，按照医院机房设计规划，根据“覆盖全院、数据共享、应用优先、资源共享”的原则，拟在现有的信息化系统基础上，完善信息化安全建设。

对项目采购需求、特定资格要求的询问、质疑请与采购人联系，由采购人负责答复。

本项目（是/否 √）接受联合体投标。

二、申请人的资格要求

1.满足《中华人民共和国政府采购法》第二十二条规定，提供下列材料：

（1）法人或者其他组织的营业执照等证明文件，自然人的身份证明；

（2）2021 或 2022 度经审计的财务状况报告（成立不满一个年度的不需提供）；

（3）依法缴纳税收和社会保障资金的相关证明材料；

（4）具备履行合同所必需的设备和专业技术能力的声明及证明材料；

（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的书面声明。

根据连财购〔2023〕4号文件精神，第（2）、（3）项可以提供《财务状况报

告及税收、社会保障资金缴纳情况承诺函》，详见招标文件第六部分格式。

2.落实政府采购政策需满足的资格要求：无。

4.本项目的其他资格要求：

响应文件递交截止前，被信用中国、中国政府采购网列入失信被执行人、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的供应商，拒绝其参与政府采购活动。

备注：采购人或采购代理机构通过信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），对供应商信用记录情况进行查询，查询结果页面打印留存。

5.法律、法规规定的其他条件。

6. 本项目执行《关于印发环境标志产品政府采购品目清单的通知》（财库〔2019〕18 号）、
《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19 号）等有关规定，采购人
拟采购的产品属于品目清单范围的，采购人及其委托的集采机构将依据国家确定的认证机构
出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府
优先采购或强制采购。投标人须按招标文件要求提供相关产品认证证书。

7.为助力打好污染防治攻坚战，推广使用绿色包装，政府采购货物、工程和服务项目中涉及商品包装和快递包装的，投标人提供产品及相关快递服务的具体包装要求要参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》。

三、获取招标文件

时间：2023 年 10 月 11 日至 2023 年 10 月 21 日 18：00 止（北京时间）

地点：连云港市公共资源电子交易系统

网址：http://218.92.36.85:8186/PSPBidder/memberLogin

方式：在线获取

售价：0 元

四、提交投标文件截止时间、开标时间和地点

1.投标文件接收时间与地点

投标文件接收截止时间：2023 年 10 月 31 日上午 9：00（北京时间）

电子投标文件上传地址：http://218.92.36.85:8186/PSPBidder/memberLogin

2.开标时间与地点

开标时间：2023 年 10 月 31 日上午 9：00（北京时间）

开标地点：连云港市公共资源不见面开标大厅

开标大厅网址：

http://218.92.36.85:8186/BidOpening/bidopeninghallaction/hall/login

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

1.本次公开招标不收取投标保证金。

2.本招标文件中标注★的款项为实质性响应要求和条件，如不满足将按无效响应处理。

3.无论出于何种原因，采购人在采购活动开始前可对采购文件进行修改、补充或变更，其内容作为采购文件的重要组成部分，请各供应商关注连云港市政府采购交易平台网站。若因供应商自身原因未及时关注本项目有关修改、补充或变更信息，导致投标文件编制或提交失误，由此造成的一切损失由供应商自行承担。

七、对本次招标提出询问，请按以下方式联系

1.采购人信息

名　　称：赣榆区中医院

地　　址：连云港市赣榆区青口镇文化东路 1 号

联 系 人：董自军

联系方式：051886212169

2.采购代理机构信息

名　　称：赣榆区政府采购中心

地　　址：赣榆区青口镇文化路东路 300 号行政中心东辅楼公共资源交易中心 207 房间

联系方式：刘工 0518-86260257

八、电子招投标说明

1.本项目采用电子招标投标，请供应商严格按照招标文件的规定编制、提交投标文件，否则所造成的一切不利后果由供应商自行承担。

2.供应商进入“连云港市公共资源电子交易系统”，完成注册、CA 办理、激活、诚信库信息完善等流程，选择需要获取的文件，信息录入后下载交易文件即可参加该项目采购活动。其他途径获取的招标文件无效，投标时投标文件将拒收，由此造成的不利后果由供应商自行承担。**系统操作流程详见连云港市政府采购交易平台-下载中心-供应商操作手册[网]。**

系统操作咨询：400-998-0000；0518-85861319。

特别说明：依法获取采购文件的供应商，不能参加本项目采购活动的，应当在递交投标文件截止前，通过连云港市公共资源电子交易系统“放弃投标”模块，提交放弃说明（流程详见下载中心-供应商操作手册[网]）。对于未参加本项目采购活动，也未在递交投标文件截止前提交放弃说明的供应商，将按照《江苏省政府采购信用管理暂行办法》等有关文件规定，视为一般失信行为，给予信用评价扣分。

九、不见面交易，供应商注意事项

本项目采用远程不见面交易方式，通过不见面交易系统及配套硬件设备（摄像头、话筒、音响等）完成远程解密、现场疑义及回复、开标唱标（开启）等交互环节。注意事项说明如下：

1.不见面交易项目的时间均以国家授时中心发布的时间为准。

2.开标当日，供应商可在任意地点通过连云港市公共资源不见面开标大厅参加开标会议，如自主决定抵达开标现场，请自备笔记本电脑、热点网络等（现场不提供），并提前做好调试，赣榆区公共资源交易中心（赣榆区公共资源交易中心)不承担因供应商自身准备原因造成的损失。

3.投标（响应）文件递交截止时间前，工作人员提前进入开标大厅，播放测

试音频，请各供应商法定代表人或委托代理人**提前登录不见面开标大厅并在投标文件递交截止时间之前完成签到（参加多个标段投标的须分别完成）**，收听观看实时音视频交互效果并及时在讨论组中反馈。**未按时加入开标会议并完成登录、签到操作的或未能在开标会议区内全程参与交互的，供应商将无法收到解密指令、疑义回复等实时内容，视为放弃投标（响应）和放弃对开标（开启）全过程提出疑义的权利，并承担由此导致的一切后果。**

注：供应商在签到时，须填写法定代表人或委托代理人姓名，手机号码（在整个招标采购过程中，该手机号码务必保持畅通，否则澄清、说明、答疑等联系不到产生的一切后果由供应商自行承担）。相关操作详见供应商操作手册[网]。

4.投标（响应）文件接收截止时间后，工作人员将在不见面开标大厅发出投标（响应）文件解密指令，供应商在各自地点按规定时间自行实施远程解密，解密限定在发出指令后30分钟内完成。

因供应商网络与电源不稳定、配置的软硬件环境无法满足系统正常使用、CA数字证书发生故障或错用等自身原因，导致投标（响应）文件在规定时间内未能解密、解密失败或解密超时，视为供应商投标（响应）文件递交无效，系统内投标（响应）文件将被退回；因网上开评标系统发生故障，导致无法按时完成投标（响应）文件解密或开评标工作无法正常进行的，可根据实际情况相应延迟解密时间或调整开评标时间。本项目在限定的解密时间内，只要有一家供应商解密成功，即视为不见面开标大厅运行无故障。

5.为保证交互效果，建议供应商配置的硬件环境有：高配置电脑、高速稳定的网络、电源（不间断）、CA数字证书、音视频设备（耳麦、高清摄像头）等；软件环境有：IE 浏览器（版本必须为 11），江苏省互联互通驱动。建议选择封闭安静的地点参与远程交互。因供应商自身硬件、软件配备不齐全或发生故障等问题导致在交互过程中出现不稳定或中断等情形的，由供应商自身承担一切后果。

赣榆区公共资源交易中心

2023年10月10日

第二部分　投标人须知

一、说明

一、适用范围：

本招标文件仅适用于本次公开招标中所叙述项目的采购，招标需求详见第四部分“项目需求”。本次招标、投标、开标、评标和中标结果发布全程电子化。

投标人的投标文件以及投标人与集采机构就有关投标的所有来往函电统一使用中文（特别规定除外），既有中文也有外文的，以中文意义为准。

二、定义：

“招标人”（采购人）系指组织本次招标的招标机构；“投标人”系指向招标人提交投标文件的制造（研发）商或供应商；“投标人代表”系指投标人的法定代表人或者获其授权的代理人。

三、投标费用：

无论投标过程中的作法和结果如何，投标人自行承担所有与参加投标有关的全部费用。

二、招标文件说明

四、招标文件的构成：

招标文件用以阐明所需服务、招标投标程序等，具体由下述部分组成：

第一部分 投标邀请

第二部分 投标人须知

第三部分 评标办法

第四部分 项目需求

第五部分 合同

第六部分 投标文件格式

五、招标文件的修改：

招标文件的修改书（若有）将构成招标文件的一部分，对投标人有约束力。

三、投标文件的编制

六、编制要求：

投标人应仔细阅读招标文件的所有内容，应当按照招标文件的要求编制电子

投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应，并保证所提供的全部资料的真实性，**否则作无效响应处理**。

七、投标报价：

本项目投标报价最高不得超过预算价（最高限价），否则**作无效响应处理。**

投标人应根据投标报价要求在详细报价书上列明各项投标单价、总价等，未全部列示的**作无效响应处理**。

八、投标人资格的证明文件：

投标人必须提交证明其有资格进行投标的文件，作为投标文件的一部分。银行、保险、石油石化、电力、电信等特殊行业法人的分支机构（不具有独立的法人资格）参加本项目政府采购活动的，应当提供总公司出具的愿为其参与本项目政府采购活动以及履约行为承担民事责任的承诺书（或授权书）。

投标人委托代理时还应提交法定代表人授权委托书，请按第六部分“投标文件格式”填写并附法定代表人与委托代理人身份证明电子件。

九、投标有效期：

投标文件接收截止时间结束后 60 天内。

十、投标文件制作工具：

投标人必须使用连云港市公共资源电子交易系统可接受的投标文件制作工具编制投标文件，系统操作流程详见连云港市政府采购交易平台-下载中心-供应商操作手册[网]，请及时关注版本更新。

十一、电子投标文件编制要求：

投标人编制的投标文件应包括**商务文件、技术文件、评审因素所需材料和其他材料**等内容，相关文件的提交如未特别注明可提供扫描件。

1、投标文件格式：

填写投标人名称、投标人地址、法定代表人、委托代理人、日期等内容。

2、商务文件：（政府采购政策有关材料可选提交；委托代理时必须提交法定代表人授权委托书，否则投标无效；其他文件必须提交，否则投标无效）

（1）响应函：请按给定格式及要求填写。

（2）开标一览表：请按给定格式及要求填写。

（3）报价明细表：请按第六部分“投标文件格式”提供的“报价明细表”格式及要求填写。

（4）政府采购政策：中小企业声明函、残疾人福利性单位声明函及省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（5）资格审查材料：

投标单位基本信息、财务状况报告可以通过同步诚信库后挑选上传；税收证明、社保证明请上传依法缴纳税收和社会保障资金的相关材料；具备履行合同所必需的设备和专业技术能力的证明材料、参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明，请按给定的格式填写；具备法律、行政法规规定的其他条件的证明材料，如有请提供；其他资格审查材料要求，详见本招标文件第一部分“投标邀请”“二、申请人的资格要求”。

（6）法定代表人授权委托书：请按给定格式及要求填写。

（7）商务条款偏离表：请按给定格式及要求，并根据投标人投标承诺的商务条件与“合同条款”“项目需求”等的差异填写。

（8）售后服务承诺书：请按给定格式及要求填写。

3、技术文件：（以下文件必须提交，否则该投标人投标无效）

（1）技术标：可以但不限于技术方案、招标文件规定的其他材料等，格式自定。

（2）项目需求响应：格式自定。

4、评审因素所需材料：

如有，请按招标文件要求提供。

5、其他材料：

如有，请按招标文件要求提供。

十二、生成投标文件：

投标文件应由**法定代表人或其委托代理人在凡规定签章处逐一签字或盖章并加盖投标人公章（相关内容可以打印、签字、盖章后扫描电子件）或使用电子签章**，本招标文件所表述的公章是指刻有投标人法定名称的印章，不包括合同、财务、税务、发票等形式的业务专用章。

电子投标文件不得涂改、行间插字或删除，如出现上述情况应重新编制。

投标文件制作工具生成内容相同、加密与未加密两个版本电子投标文件，加密版本用于提交上传，未加密版本用于特殊情况处理。

四、投标文件的提交

十三、投标文件的上传、修改和撤回：

投标人应当使用投标文件制作工具，生成加密电子投标文件一份，在规定的截止时间前上传。

投标人在上传投标文件后可以对其修改或撤回，但这种修改或撤回，必须在规定的投标截止时间前。

对电子投标文件的修改，投标人可以在投标截止时间前登录电子交易平台撤回文件，并上传新的投标文件，投标文件以最终完成上传的为准。

投标人不得在投标截止时间后修改投标文件，也不得在投标截止时间起至投标有效期满前撤回投标文件。

十四、递交投标文件的截止时间：

所有投标文件都必须在规定的接收截止时间之前上传，迟于截止时间的**不予接收。**

十五、电报、电话、传真以及纸质投标文件形式的投标概不接受。

五、开标和评标

十六、开标：

集采机构将在本招标文件第一部分“投标邀请”规定的时间和地点进行开标，投标人的法定代表人或其委托代理人应准备**身份证件和用于生成、加密和上传电子投标文件的 CA 数字证书参加开标会。**

线下开标的，供应商必须按规定时间递交 CA 数字证书，超过截止时间的集采机构有权拒收，视为放弃投标（响应）和放弃对开标（开启）全过程提出疑义的权利，并承担由此导致的一切后果。

不见面交易的，供应商必须提前登录不见面开标大厅并在投标文件递交截止时间之前完成签到，**如未按时加入开标会议并完成登录、签到操作的或未能在开标会议区内全程参与交互的，供应商将无法收到解密指令、疑义回复等实时内容，视为放弃投标（响应）和放弃对开标（开启）全过程提出疑义的权利，并承担由此导致的一切后果。**

供应商未参加开标会的，视同认可开标结果。

投标人使用 CA 数字证书解密投标文件后，集采机构当众宣读每份电子投标文件中“开标一览表”的各项内容以及集采机构认为有必要宣读的其他内容并记录，唱标顺序按开标系统投标人先后顺序进行。

十七、评标委员会：

评标委员会由采购人代表和评审专家组成，评标委员会按照招标文件中规定的评标方法和评标标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

评标期间，投标人的法定代表人或者获其授权的代理人必须候场，随时接受评委询问，并予以解答。

十八、对投标文件的审查和确定：

1、开标结束后，采购人依法对投标人的资格进行审查。

2、评标委员会负责具体评标事务，并独立履行下列职责：

（1）审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

（2）要求投标人对投标文件有关事项作出澄清或者说明；

（3）对投标文件进行比较和评价(对商务、技术及其他内容的比较和评价结束前，评标委员会不得比较和评价投标报价)；

（4）确定中标候选人名单，以及根据采购人授权直接确定中标人；

（5）向采购人、集采机构或者有关部门报告评标中发现的违法行为；

（6）编写评标报告。

3、评标委员会对符合资格的投标人的投标文件进行符合性检查，以确定其是否满足招标文件的实质性要求。

符合性检查：依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。

未实质性响应招标文件的投标文件按无效响应处理。

评标委员会首先审查每份投标文件是否实质性响应了招标文件的要求。实质性响应的投标文件是与招标文件要求的全部实质性条款、条件和规格相符且其余非实质性技术及商务条款没有重大偏离或保留。

所谓重大偏离或保留，是指与招标文件规定的主要技术指标或重要的商务条款或除上述以外的多项指标要求存在负偏离，或者在实质上与招标文件不一致，而且限制了合同中采购人和见证方的权利或供应商的义务，保留或给予纠正这些偏离的机会将会对其他实质性响应要求的供应商的竞争地位产生不公正的影响。重大偏离的认定需经过评标委员会 2/3 及以上成员的认定。

4、评标委员会决定投标文件的响应性仅基于投标文件本身的内容，而不寻

求外部证据。

5、评标委员会将拒绝被确定为非实质性响应的投标人，投标人不能通过修正或撤销不符之处而使其投标成为实质性响应的投标。

6、投标文件报价出现前后不一致的，按照下列规定修正：

（1）投标文件中“开标一览表”内容与投标文件中相应内容不一致的，以“开标一览表”为准；

（2）大写金额和小写金额不一致的，以大写金额为准；

（3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照政府采购有关规定经投标人确认后产生约束力，投标人不确认的，其投标无效。

十九、投标文件的澄清：

对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式（从评标系统发起）要求投标人作出必要的澄清、说明或者补正。

投标人的澄清、说明或者补正采用书面形式，通过连云港市公共资源电子交易系统作出，使用 CA 数字证书签章后提交，并不得超出投标文件的范围或者改变投标文件的实质性内容。投标人的澄清文件是投标文件的组成部分。

投标人有责任按照评标委员会通知的时间、方式进行答疑和澄清，如未按规定作出，其风险由投标人自行承担。

二十、评标原则、方法和现场开标特殊情况处理：

评标委员会应当公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与供应商接触。

评标时，评标委员会各成员应独立对每个投标人的投标文件进行评价，并汇总每个投标人得分，评标方法详见第三部分“评标办法”。

因“开评标系统”自身故障，开标活动无法正常进行时，将使用投标文件备份 U 盘继续进行开标活动（采用不见面交易方式招标的本条款不适用）；“开评标系统”自身故障是指非投标人原因造成所有投标人电子投标文件均无法解密的情

形，部分投标文件无法解密的，不适用该条款；对于不同载体的投标文件，开标、评标及认定顺序为电子投标文件、投标备份 U 盘，前项不能读取的可按后项评审。

二十一、投标人存在下列情况之一的，投标无效：

1、投标人未按照招标文件的规定提交投标保证金的；

2、投标文件未按招标文件要求编制、签署、盖章的；

3、不具备招标文件中规定的资格要求的；

4、报价超过招标文件中规定的预算金额或者最高限价的；

5、投标文件含有采购人不能接受的附加条件的；

6、未按招标文件要求提供电子投标文件或者电子投标文件未能解密（指投标人自身原因）且按照招标文件明确的投标文件解密失败后补救方案（仅现场开标适用）补救不成功的；

7、投标人提交的电子投标文件、投标文件备份 U 盘（仅现场开标适用）均因其自身原因出现问题导致无法电子评标的；

8、法律、法规和招标文件规定的其他无效情形。

有下列情形之一的，视为投标人串通投标，其投标无效：

1、不同投标人的投标文件由同一单位或者个人编制；

2、不同投标人委托同一单位或者个人办理投标事宜；

3、不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

4、不同投标人的投标文件异常一致或者投标报价呈规律性差异；

5、不同投标人的投标文件相互混装；

6、不同投标人的投标保证金从同一单位或者个人的账户转出。

二十二、在招标采购中，出现下列情行之一的，应予废标：

1、符合专业条件的供应商或者对招标文件作实质性响应的供应商不足三家的；

2、出现影响采购公正的违法、违规行为的；

3、投标人的报价均超过了采购预算（最高限价），采购人不能支付的；

4、因重大变故，采购任务取消的。

六、中标结果

二十三、中标人的确定

评标委员会按照评审得分由高到低顺序推荐 3 名中标候选人，并根据采购人的授权，直接确定排名第一的中标候选人为中标人。

二十四、中标通知书

中标人确定后，中标结果由集采机构在连云港市政府采购交易平台公告，中标公告期限为 1 个工作日，同时由集采机构向中标人发出中标通知书。**中标供应商在领取中标通知书时，需提供一份与电子投标文件一致的纸质打印投标文件，须封面、骑缝加盖公章。**

集采机构无义务向未中标人解释未中标原因和退回投标文件。

七、合同

二十五、签订合同

采购人应当自中标通知书发出之日起 30 日内与中标人签订书面合同，并递交一份原件至政府采购中心备案。

招标文件、中标人的投标文件及其澄清文件(若有)等，均为签订合同的依据。

所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性的修改。

八、质疑、投诉

二十六、 质疑

1、质疑的提出

提出质疑的供应商应当是参与所质疑项目采购活动的供应商。

供应商认为招标文件、采购过程、中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日（获取招标文件之日、中标公告发布之日）起七个工作日内以书面形式向采购人、集采机构提出质疑。供应商应当在法定质疑期内一次性提出针对同一采购程序环节的质疑。**未依照采购公告要求获取招标文件的供应商，视为未参与该项目的采购活动，不具备对该招标文件提出质疑的法定权利。**

提出质疑时，必须坚持“谁主张，谁举证”“实事求是”的原则，不能臆测。属于须由法定部门调查、侦查或先行作出相关认定的事项，质疑供应商应当依法申请具有法定职权的部门查清、认定，并将相关结果提供给采购人、集采机构。采购人、集采机构不具有法定调查、认定权限。

质疑函的接收方式为供应商书面原件提交。联系部门、联系电话和通讯地址详见本招标文件第一部分“投标邀请”。质疑实行实名制，不得进行虚假、恶意质疑。

质疑函应当使用范本（详见连云港市政府采购交易平台-监管信息-意见反馈）。

供应商提出质疑应当**提交质疑函和必要的证明材料**，应当包括下列内容：

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期；

（7）**必要的证明材料；**

（8）采购文件(交易文件)下载回执函；

（9）营业执照复印件及法定代表人授权委托书、法定代表人身份证复印件、委托代理人身份证复印件。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代理人签字或者盖章，并加盖单位公章。

2、质疑函的受理和答复

质疑供应商应当保证其提出的质疑事项及必要的证明材料的真实性及来源的合法性，并承担相应的法律责任。**对不能提供必要的证明材料的、涉及商业秘密的、非书面原件形式的、匿名的质疑函将不予受理**。必要的证明材料要具备客观性、关联性、合法性，无法查实的（如宣传册、媒体报道、猜测、推理等）不能作为证明材料。采购人、集采机构不负责搜集必要的证明材料等工作。

对符合质疑要求的，采购人、集采机构接收并登记《质疑函登记表》。在处理过程中，发现需要质疑供应商进一步补充必要的证明材料的，质疑供应商应在法定的时间内提供，质疑答复时间相应顺延。质疑供应商不能按时提供必要的证明材料的，视同放弃质疑。

对不符合质疑要求的，采购人、集采机构有权要求其补充必要的证明材料，质疑供应商未在法定的时间内提供补充必要的证明材料的，视同放弃质疑。

采购人、集采机构负责将质疑供应商提出的质疑函及相关材料提供给评审委员会协助答复，并将答复意见回复质疑供应商。必要时，可向被质疑供应商转发《质疑函》及相关材料。被质疑供应商应当在要求的时间内，以书面形式作出说明并提交相关材料。

3、质疑处理

质疑供应商未按照法定程序进行质疑投诉的，视为一般失信行为。

质疑供应商不配合或者采用不正当手段干扰政府采购质疑、投诉处理工作的，视为一般失信行为。

质疑供应商投诉受理期间，就同一事项多头举报，干扰财政部门投诉处理的，视为一般失信行为。

质疑供应商在全国范围 12 个月内三次以上质疑查无实据的，视为一般失信行为。

质疑供应商采用捏造事实、提供虚假材料或者以非法手段取得证明材料等方式进行虚假、恶意投诉的，视为严重失信行为。（证据来源的合法性存在明显疑问，投诉人无法证明其取得方式合法的，视为以非法手段取得证明材料）

质疑供应商在全国范围 12 个月内三次以上投诉查无实据的，视为严重失信行为。

未尽事宜，依照有关法律、法规执行。

二十七、投诉

投诉事项依照有关法律、法规执行。

第三部分　评标办法

一、评标方法：

本项目评标方法采用综合评分法。综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

二、评标原则：

评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与供应商接触。

三、评标标准：

1、评标时，评标委员会以招标文件为评标依据，评标委员会各成员独立对每个投标人的投标文件进行评价，并汇总每个投标人的得分。

2、本项目评分总分为 100 分，按四舍五入取至小数点后两位。

3、中标标准：评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

综合评分法

1.价格分（30 分）

采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他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）× 30 分。

评标过程中，不得去掉报价中的最高报价和最低报价。

2.商务技术分（70 分）

评分项目	评分内容	评分要求	备注
技　术部分	技术方案（26 分）	根据投标方案总体设计、建设方案、详细阐述医院系统的建设现状、问题分析、建设思路和关键技术，方案是否对医院现状及存在的问题分析透彻，建设思路是否科学合理、安全严密、具有一定的前瞻性，是否有独到的优势综合打分： 问题分析透彻、建设思路清晰、解决方案科学合理、项目规划设计优秀且合理的，得 6-8 分； 问题分析一般、建设思路模糊、解决方案合理性一般、项目规划	

		设计一般的，得 3-5 分； 问题分析较差、建设思路较差、解决方案合理性较差，项目设计规划较差的，得 0-2 分。 未阐述方案不得分。	
		根据投标方案中“关键数据容灾部分”的内容，考察投标人对采购人信息化建设现状熟悉程度和对数据容灾部分的理解程度，方案是否充分结合医院现有软硬件设备，是否充分兼容医院现有数据库和虚拟化平台等方面进行综合打分： 项目理解充分、数据容灾方案与医院现状结合充分、兼容度较高的，得 6-8 分； 项目理解一般、数据容灾方案与医院现状结合一般、兼容度一般的，得 3-5 分； 项目理解较差、数据容灾方案与医院现状结合较差、兼容度较差的，得 0-2 分； 未阐述方案或数据容灾方案与医院现状完全不结合、不兼容的，不得分。	
		投标人提供项目实施安装调试方案，内容包含但不限于总体实施安装方案、重点（关键）和难点的安装方案及处理措施、货物调试的软硬件配置等。 优：方案服务项目齐全、内容全面具体，措施完善：4-5 分； 良：方案内容较全面、较具体，措施较完善：2-3 分； 一般：售后服务承诺一般，服务保证措施一般：0-1 分。 未见阐述该项不得分。	
		投标人提供售后服务运维方案，内容包含但不限于售后期限、售后服务组织、服务方式、服务范围、服务内容、服务人员，响应时间、应急处理方案等。 优：售后服务体系非常完善，响应时间及时，应急方案处理到位；4-5 分 良：售后服务体系较完善，响应时间较及时，应急方案处理到位；2-3 分 一般：售后服务体系完善性一般，响应时间及时，应急方案处理一般；0-1 分 未见阐述该项不得分。	
	产品性能（25 分）	根据所投产品技术性能以及对招标文件各项基本技术参数要求的逐项响应情况： 1.标记★的项为必响应技术参数指标，不得负偏离,如带★项出现负偏离，将被视为无效投标。 2.标▲的功能及技术参数性能指标，有一项不满足扣 1 分； 3.未标记的功能及技术参数性能指标，有一项不满足扣 0.5 分。扣完 25 分为止。 功能及技术参数指标请投标人按照附表《技术规格偏离表》格式填写响应情况，并按招标文件要求提供相关证明材料（所有证明材料必须加盖投标人公章），未按格式响应、未按要求提供相关证明材料或提供材料与要求不符的视为负偏离。	

	所投产品质量（8分）	1、投标人所投外联单位和互联网边界安全防护设备产品同时具有防火墙密码检测证书和信息技术产品安全测评证书（EAL4+）（千兆）的得1分； 2、投标人所投远程安全访问控制设备产品同时符合国密局制定的《IPsec技术规范》和《SSL VPN技术规范》和IPv6 Ready认证的得1分； 3、投标人所投运维审计与风险控制设备产品符合测评标准：GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》（idt ISP/IEC 15408:2008），并获得由“中国信息安全测评中心信息安全实验室”颁发的《国家信息安全测评 信息技术产品安全测评证书》，级别应为EAL3+，满足的得2分，不满足不得分。 4、投标人所投数据库审计与风险控制设备具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级的得1分，其余不得分。 5、投标人所投日志审计分析设备具备中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，符合 GB/T 20945-2013 《信息安全技术 信息系统安全审计产品安全技术要求 和测试评价方法》（增强级）的得1分，其余不得分。 6、投标人所投虚拟化防病毒系统生产厂商同时具备CNNVD（国家信息安全漏洞库）技术支撑单位一级单位认证、ITSS云计算服务能力（SaaS服务）标准符合性证书以及中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类不低于三级）的得1分，其余不得分。 7. 投标人所投终端杀毒系统生产厂商具备网络安全应急服务支撑单位（国家级）证书的得0.5分，其余不得分。 8. 投标人所投终端杀毒系统生产厂商具备网络安全应急服务支撑单位证书（反网络诈骗领域）的得0.5分，其余不得分。	
	业绩（2分）	投标人自 2019年1月1日以来（时间以合同签订日期为准），每承担过类似项目业绩的，每个得1分，总分2分；（投标人须将中标（成交）通知书复印件、合同复印件，二者缺一不可）	
	项目技术人员（5分）	**1.项目经理：** 拟派项目经理同时具有高级项目经理认证及 Oracle OCP 认证及CISP认证证书的得1分；其余不得分。 **2.项目组人员：** （1）拟派项目组人员中具有高级网络工程师证书（如：CCIE、HCIE、H3CIE等，每有一个得0.5分，最高得0.5分； （2）拟派项目组人员中具有中级数据库工程师认证证书的（如：ORACLE OCP、达梦DCP、SQLserver MCSA等），每有一个得0.5分，最高得1分； （3）拟派项目组人员中具有IT服务项目经理资质证书的，每有一个得0.5分，最高得0.5分； （4）拟派项目组人员中具有注册信息安全专业人员认证证书的（如：CISP等），得0.5分； （5）拟派项目组人员中具有项目管理专业人士资格认证证书的（如：PMP等），得0.5分； **3.特情值班人员：**	

		拟派特情值班人员同时具有 RHCE 认证及 ORACLE OCM 认证及 CISP 认证证书的得 1 分，其余不得分。 注：投标文件里提供相关证书复印件及投标人为证书人员缴纳的 2023 年 1 月以来任意连续三个月的社保证明原件的扫描件，上述所有材料加盖投标人公章，否则不得分。	
投标人资质	投标人履约能力（4 分）	投标人具有 ISO9001 质量管理体系认证证书，得 1 分； 投标人具有 ISO14001 环境管理体系认证证书，得 1 分； 投标人具有 ISO45001 职业健康管理体系认证证书，得 1 分； 投标人具有 AAA 级企业资信等级证书的，得 1 分。 需提供证书复印件加盖投标人公章制作在投标文件中，否则不得分。	

3、总得分 = 价格分 + 商务技术分

4、中标标准：评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

第四章 项目需求

说明：1.本项目采购方式为公开招标，项目属性为货物，采购标的对应的中小企业划分标准所属行业为制造业。

2.本章中标注★的款项为实质性要求和条件（由采购人根据实际情况设置），投标人必须作出满足或者优于原要求和条件的响应，否则投标无效。

3、根据财政部令第 87 号第 31 条：供应商提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前两款规定处理。

本项目核心产品为：核心交换设备。

2.1.1 一项目需求概述

为了满足医院信息系统可以稳健、高效、安全的运行，同时为了满足医院等保安全建设需要，参考三甲医院信息化建设方案，按照医院机房设计规划，根据“覆盖全院、数据共享、应用优先、资源共享”的原则，拟在现有的信息化系统基础上，完善信息化安全建设。

赣榆区中医院医院属于二级甲等中医医院，医院信息化建设已运行多年。医院建设有医院信息管理系统（HIS）、医学影像存储与管理系统（PACS）、体检系统、手术麻醉信息系统、合理用药、供应中心追溯系统等数十个子系统。信息系统覆盖全院各个部门，涵盖患者就诊的各个环节。医院信息系统的安全性直接关系到医疗工作的正常运行，一旦网络瘫痪或数据丢失，将会给医院带来巨大的灾难和难以弥补的损失。因此，为保证医院信息系统安全正常工作，必须采用加强信息化数据容灾和信息化安全建设，采取必要的信息化安全管理措施，来保障医院信息网络系统持久、稳定、安全地运行。

2.1.2 项目建设目标

项目建设必须以公安部关于等级保护测评2.0第三等级的相关建设要求为依据，参考三级医院信息化安全建设要求，确保本项目建成后医院可以顺利通过等级保护测评。

2.1.3 产品清单及技术指标

下文所列技术指标要求中带★的项为必响应技术参数指标，不得负偏离。如带★项出现负偏离，将被视为无效投标。

★投标人中标后5日内，提供与投标产品相同品牌型号的测试产品，采购人将对中标人的应标参数进行逐一核对，如发现存在中标人实际供货产品参数与投标产品参数不一致的情况，则按照虚假应标处理，采购人将上报相关单位。并要求中标人更换与投标参数响应完全一致的产品，直至满足招投标参数为止（如招标与投标参数不一致以有利于采购人的参数为准）；由此带来的后果包括并不限于暂不签订合同、可能对中标人产生的信誉以及对医院运营影响产生的相关费用索赔由中标人全权负责。（投标文件中提供相应书面承诺函）

2.1.4 项目需求清单

序号	设备名称	配置需求	单位	数量
1	关键数据容灾系统	详见技术参数要求	套	1
2	核心交换设备	详见技术参数要求	台	2
3	网络隔离设备	详见技术参数要求	台	1
4	外联单位边界安全防护设备	详见技术参数要求	台	1
5	互联网边界安全防护设备	详见技术参数要求	台	1
6	远程安全访问控制设备	详见技术参数要求	台	1

7	运维审计与风险控制设备	详见技术参数要求	台	1
8	数据库审计与风险控制设备	详见技术参数要求	台	1
9	日志审计分析设备	详见技术参数要求	台	1
10	Web 应用安全防护设备	详见技术参数要求	台	1
11	防病毒系统	详见技术参数要求	套	1
12	IT 统一运维管理系统	详见技术参数要求	套	1
13	网络安全运维服务	详见技术参数要求	套	1
14	系统集成及运维服务	详见技术参数要求	套	1

新点网上招投标系统

2.1 技术参数要求

2.2.1 关键数据容灾系统

技术指标	技术要求
核心数据库容灾	**1. 常规备份：** 支持医院关键业务系统数据库定时自动化备份作业，并定期提供备份数据恢复演练服务，投标文件中提供详细的备份数据恢复演练方案。 ★要求配套的 IT 运维管理软件可以监控备份作业的执行结果，并及时发送结果通知管理员（提供承诺函加盖投标人公章）。 **2. 数据实时容灾：** 核心系统 HIS 数据库同时部署本地异机、异地异机两套实时容灾保护系统： 2.1 利旧医院现有设备，构建 HIS 系统数据库本地异机实时同步容灾保护系统； 2.2 利用异地云平台环境，构建 HIS 系统数据库异地异机实时同步容灾保护系统。 2.3 要求实时容灾系统必须完全兼容医院 HIS 数据库平台，为了避免数据同步对生产数据库带来性能影响，不接受在操作系统或数据库系统中安装第三方代理的方式实现数据同步。 2.4. ★要求本项目配套的 IT 运维管理软件，可以实时监控生产库与容灾库数据同步延迟时间，延迟大于 5 分钟触发告警机制，并及时发送告警消息通知管理员（提供承诺函加盖投标人公章）。 2.5 要求提供定期容灾恢复演练服务，投标文件中提供详细的数据容灾恢复演练方案。 3.连续性数据保护 利旧医院现有设备，为核心业务 HIS 系统数据库部署连续性数据保护机制。
虚拟化数据容灾	采用与医院现有虚拟化平台兼容的备份解决方案，定制虚拟化平台定时备份作业，为了避免备份作业对虚拟化平台带来性能影响，不接受在虚拟化平台安装代理的解决方案。 ★要求配套的 IT 运维管理软件可以监控备份作业的执行结果，并及时发送结果通知管理员（提供承诺函加盖投标人公章）。

2.2.2 核心交换设备

技术指标	技术要求
★交换容量	交换容量≥25Tbps
★包转发率	包转发率≥1600Mpps
★接口	支持万兆 SFP+端口≥48 个、40/100GE QSFP28 端口≥6 个
电源	支持可插拔双电源
风扇	独立可插拔风扇≥4 个
技术特性	支持 MAC 地址表≥128K、ARP 表≥128K、IPv4 路由表≥192K，IPv6 路由表≥64K；
	静态路由、RIP V1/2、RIPng、OSPF、OSPFv3、IS-IS、IS-ISv6、BGP、BGP4+、ECMP、路由策略；
	支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式，支持分组/分域/分时管理；
	支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN；
	支持 VXLAN 功能，支持 BGP-EVPN、分布式 Anycast 网关，IPv4 VXLAN 隧道≥16000，IPv6 VXLAN 隧道≥4000；
	支持安全启动，CPU 防攻击、加密通信分析、安全诱捕等安全特性；
	支持 NetStream、支持 Telemetry；
服务	提供原厂三年质保服务。
★本次配置	48 个万兆 SFP+端口、6 个 40GE QSFP28 端口，冗余电源；冗余风扇模块；24 个千兆 RJ45 电口模块；4 个 10Gb SFP+光模块多模模块；12 个 1Gb SFP 多模光模块；16 对 3M LC-LC OM3 多模光纤跳线。

2.2.3 网络隔离设备

技术指标		技术要求
产品架构	系统基本架构	“2+1”系统结构，内外端机为 TCP/IP 网络协议的终点，阻断 TCP/IP 协议的直接贯通； 内外端机之间采用专用硬件和专用协议进行连接，不可编程。网闸以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换。

	安全体系结构	仲裁审计系统部署于内端机上，通用协议无法通过外端机直接连接到仲裁系统； 只能通过内端机上的管理口对网闸进行配置，避免内外端机由于被黑客入侵，导致隔离网闸被黑客完全控制的现象。
	操作系统	▲采用多级安全多核多线程并行安全操作系统；（提供相关证明材料加盖原厂公章） ▲系统基于加固安全操作平台，为主机提供深度防御；（提供相关证明材料加盖原厂公章） 能够对两个主机系统提供多层次、高强度的安全防护，保护其重要进程、文件、数据不受黑客侵袭； 采用对象互斥和线程守护技术，保护主要进程的安全性和稳定性； 不采用通用的指令库和函数库，只提供有限的内部调试用指令函数。
功能要求	系统管理	三权分立：安全管理流程主要由安全管理员、系统管理员和安全审计员通过安全管理中心执行，分别实施系统维护、安全策略制定和部署、审计记录分析和结果响应等。 支持菜单级别和用户级别配置功能； ▲支持 UKEY 认证登录（提供界面截图加盖原厂公章） 支持管理端 IP 和 MAC 地址限制 支持负载均衡 支持所有配置导入导出 自带数据分析和网络诊断工具 支持日志详细查询、备份和回滚机制 支持邮件告警
	支持协议	TCP、UDP、HTTP、HTTP_PROXY、FTP、ORACLE、POP3、SMTP、OPC、MODBUS、GB_28181_UDP、GB_28181_TCP、SIP_DB33、RTSP、MAC、ICMP、SNMP、OPC_ICOMM、INTERCONN、IMAP、H323_Q931、ORACLE_RAC、MYSQL、ORACLE_SHARED、SIP_XICHAN、GAT_1400、H225_RAS 等；
	支持网络	支持 IPV4 与 IPV6
	安全上网功能	提供安全的上网访问，支持 HTTP 协议及代理等； 访问控制对象：源地址、目标地址、源端口、目的端目、域名、URL、访问方式等； 内容过滤：关键字过滤； 脚本过滤：javascript、Applet、ActiveX 等； ▲支持 HTTP 策略过滤包含 HTTP_URL、HTTP 响应内容类型、HTTP 响应内容敏感词、HTTP 请求方法、HTTP 请求内容正则过滤、HTTP 请求 Content-Length 最大值限制、HTTP 响应 Content-Length 最大值限制、HTTP 自定义头部域检查、HTTP 方法/URL 正则和请求体过滤（提供界面截图加盖原厂公章）。

	安全邮件功能	提供安全的邮件访问，支持 POP3、SMTP 协议； 支持发件地址、收件地址、邮件主题、邮件内容、邮件附件过滤。
	文件传输功能	提供安全的文件传输功能，支持 FTP、NFS、SAMBA 等文件传输协议； 支持 FTP 对传输文件的类型过滤； 支持 FTP 指令控制； 支持 FTP 文件名黑白名单控制； 支持 FTP 传输文件大小控制； 支持对特定文件内容进行过滤
	文件同步功能	▲可通过专用客户端和网闸主动获取两种方式提供安全的文件同步功能；（提供两种方式的界面配置截图加盖原厂公章） 支持 windows 平台和 linux 平台； 支持不同任务设置不同的扫描间隔和扫描的时间段； 支持任务优先级控制； 支持跨协议同步； 支持内容过滤； 支持实时扫描、多对一传输、增量传输； 支持目录内子目录同步，至多支持 32 级目录； 支持中文文件名或目录同步； 支持传输后删除源文件； 提供详细的日志审计； ▲支持对格式类型进行特征过滤，并允许用户通过样本文件自定义格式类型；支持文件在线编辑、在线预览等操作；支持文件分享功能，可设置到期时间和提取密码。（提供界面截图加盖原厂公章）
	数据库访问功能	提供对多种主流数据库（SQL、ORACLE、DB2、MYSQL 等）数据库系统的安全访问； 支持用户查询、修改、添加、删除等操作； 支持全表复制、增量更新、全表更新等； 支持各种实例访问。
	数据库同步功能	提供多种主流数据库（SQL、ORACLE、DB2、MYSQL 等）的单、双向数据交换； 支持同步表双向检索功能； 无需修改数据库表结构，不涉及到代码修改及二次开发； 同步粒度可以达到表内具体字段； 支持多种增量同步方式，可分别定义增加、删除、修改的传输方式； 支持数据一对一、一对多、多对多的单向或双向交换和同步。 支持实时交换或定时同步的策略定义；
	自定义功能	支持用户基于标准 TCP、UDP 开发的自定义协议软件，无需对自定义协议软件进行二次修改开发，可以根据需求开发新的专用协议处理过滤功能 ▲支持 MAC 强制访问控制通道，针对被访问端文件进行类别和级别标记； 支持 TCP 配置通道，目标地址可以填写具体的域名(提供界面截图加盖原厂公章)
可靠性要求	多机热备	可实现多台设备互相冗余的应用模式 双机热备场景下，支持主机向备机单次同步或自动同步配置
	网口冗余	使一端机多网口冗余，可实现链路备份冗余的工作模式，支持 lacp、负

		载均衡、主备模式；
	负载均衡	以浮动 IP 的形式对外提供服务；结合轮询、比重、流量比、服务类别等算法，保证业务实时的连续性。
审计要求	SNMP 支持	支持 SNMP 协议，可与标准网管平台无缝兼容，能够针对读团体字、系统位置、系统联系人等参数进行自定义；
	SYSLOG 支持	支持 SYSLOG 协议，可与标准日志服务器平台无缝兼容，可实时发送网闸运行状态
其他要求	管理配置功能	管理端采用 B/S 结构； 管理端：用于通道建立、策略制定、日志查询、分析、导出等； 安全终端管理：可通过串口终端管理方式对网闸进行维护； 为保证网闸安全性，管理网口和通讯网口隔离，仅允许通过内端机管理口对网闸进行配置管理或审计日志，禁止使用其他接口对网闸进行配置管理。 管理口拥有独立路由，可避免和通讯网口发生路由冲突或干扰
	▲产品资质要求	具有国家保密局涉密信息系统产品检测证书 具有保密局出具的科技成果鉴定证书
★配置要求	接口要求	内网≥8 个 10/100/1000M RJ45 接口（含一个管理口），≥1 个串口，≥2 个 USB 口； 外网≥8 个 10/100/1000M RJ45 接口（含一个 HA 口），≥1 个串口，≥2 个 USB 口。
	性能指标	网络吞吐量≥900Mbps； 系统整体时延：<1Ms； 并发连接数≥48000。

2.2.4 外联单位边界安全防护设备

技术指标	技术要求
产品规格	▲所投产品必须为下一代防火墙，非 UTM 或其他产品，产品采用 X86 多核及自主知识产权的多核并行安全操作系统构成；（提供信息安全产品自主原创证明加盖原厂公章）
	★1U 标准机架设备，必须配备千兆电口≥6 个。防火墙网络吞吐量≥5Gbps，应用层吞吐量≥2.6Gbps，并发连接≥150 万；
网络接入	支持路由、交换、虚拟线、LISTENING、混合工作模式；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持链路聚合，可根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口

	轮询等条件提供不少于 10 种链路负载算法；
	支持 DNS DOCTORING 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS DOCTORING，实现内网资源服务器的负载均衡；
安全控制	支持一体化安全策略配置，通过一条策略实现五元组、源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、WAF、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置，简化用户管理；
	▲提供策略命中、冗余、冲突、包含检查及策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；（提供截图证明加盖原厂公章）
	内置 P2P 应用、加密应用、数据库应用、工控物联网协议等应用特征库；
	内置文件过滤引擎，支持 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、OFFICE 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	内置内容过滤功能，可对 FTP 上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤；
	支持将五元组、源 MAC、地址范围、应用、用户等加入静态黑名单，可与 URL 过滤、病毒过滤、防代理功能进行联动实现动态黑名单封锁，支持静态和动态黑名单命中统计和监控；
	内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测；
	支持连接控制和监控，可对源/目的地理对象、应用制定连接限制策略，可展示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
安全防护	入侵防御：内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持 WEB 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击；
	支持扩展独立的 WAF 防护模块，WAF 防护特征总数在 1000 条以上，支持针对地址、应用设置 WAF 白名单，支持攻击规则搜索以及自定义；

	支持行为分析，及时发现异常行为并告警，同时能够与 APT 进行联动，实现协同防御；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；
	支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；支持 UDP 关联认证，对源地址进行合法性认证；
	支持 DNS FLOOD 防护，能对 DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒、DNS 格式等攻击提供 DNS REPLY 源认证、源限速、目的限速、域名限速等综合防护手段；
	▲支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP REQUEST FLOOD、NTP REPLY FLOOD 攻击防护；（提供截图证明加盖原厂公章）
	支持扩展 SSL VPN 功能，满足远程用户安全接入内网，支持 WINDOWS、ANDROID、IOS 等远程客户端接入；
系统管理	支持多个配置文件并存，配置文件备份能力不少于 4 个；配置文件支持选择部分配置和全部配置导入导出；
	支持主、备双系统以及多个系统版本文件并存，系统版本数量不少于 5 个；
数据中心	支持独立审计策略，可对 URL 地址、网页标题、网页内容、邮件行为、邮件内容、FTP 上传/下载行为及文件内容进行审计；
	提供完善的审计数据查询功能，可对用户访问网站、邮件收发、论坛微博、FTP、TELNET 等上网行为以及用户上网流量时长等内容进行查询；
	支持日志本地存储，可对不同类型日志设置存储空间，支持日志外发至多个服务器，可设置日志传输协议、时间类型、日志语言、是否合并及加密传输等参数；
显示监控	支持系统温度、CPU 温度、CPU 利用率、内存利用率、电源故障等告警，支持 CPU 利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪；
	支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；
质保	提供三年原厂质保，三年入侵防御升级、防病毒升级；

2.2.5 互联网边界安全防护设备

技术指标	技术要求
产品规格	所投产品必须为下一代防火墙，非 UTM 或其他产品，产品采用 X86 多核及自主知识产权的多核并行安全操作系统构成；
	★2U 标准机架设备，必须配备≥6 电口 2 光口，1 个扩展插槽，冗余电源。防火墙网络吞吐量≥8Gbps，并发连接≥200 万。
网络接入	支持路由、交换、虚拟线、LISTENING、混合工作模式；
	支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
	支持链路聚合，可根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 10 种链路负载算法；
	支持 DNS DOCTORING 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS DOCTORING，实现内网资源服务器的负载均衡；
安全控制	支持一体化安全策略配置，通过一条策略实现五元组、源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、WAF、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置，简化用户管理；
	提供策略命中、冗余、冲突、包含检查及策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；
	内置 P2P 应用、加密应用、数据库应用、工控物联网协议等应用特征库；
	内置文件过滤引擎，支持 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、OFFICE 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤；
	内置内容过滤功能，可对 FTP 上传文件、下载文件、删除文件、重命名文件、

	创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤；
	支持将五元组、源 MAC、地址范围、应用、用户等加入静态黑名单，可与 URL 过滤、病毒过滤、防代理功能进行联动实现动态黑名单封锁，支持静态和动态黑名单命中统计和监控；
	内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测；
	支持连接控制和监控，可对源/目的地理对象、应用制定连接限制策略，可展示被拦截的 IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；
安全防护	入侵防御：内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持 WEB 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击；
	支持扩展独立的 WAF 防护模块，WAF 防护特征总数在 1000 条以上，支持针对地址、应用设置 WAF 白名单，支持攻击规则搜索以及自定义；
	支持行为分析，及时发现异常行为并告警，同时能够与 APT 进行联动，实现协同防御；
	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等协议进行 DDOS 防护；
	支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；支持 UDP 关联认证，对源地址进行合法性认证；
	支持 DNS FLOOD 防护，能对 DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒、DNS 格式等攻击提供 DNS REPLY 源认证、源限速、目的限速、域名限速等综合防护手段；
	支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP REQUEST FLOOD、NTP REPLY FLOOD 攻击防护；
	▲防病毒：内置病毒检测引擎，支持 HTTP/SMTP/POP3/FTP/IM 等协议的病毒防御。内置至少 2 种专业反病毒厂商或研究机构的病毒特征库，符合等级保护相关标准对网关防病毒特征库和主机防病毒特征库异构的要求。（提供至少 2 家知名、专业防病毒厂商或研究机构的合作文件复印件，并加盖原厂公

	章）。
安全接入	标配 IPSEC VPN 功能，支持 AES、DES、3DES、MD5、SHA-1 等 VPN 加密、认证算法，支持对隧道内网络流量进行监控展示；
	支持扩展 SSL VPN 功能，满足远程用户安全接入内网，支持 WINDOWS、ANDROID、IOS 等远程客户端接入；
系统管理	支持多个配置文件并存，配置文件备份能力不少于 4 个；配置文件支持选择部分配置和全部配置导入导出；
	支持主、备双系统以及多个系统版本文件并存，系统版本数量不少于 5 个；
数据中心	支持独立审计策略，可对 URL 地址、网页标题、网页内容、邮件行为、邮件内容、FTP 上传/下载行为及文件内容进行审计；
	提供完善的审计数据查询功能，可对用户访问网站、邮件收发、论坛微博、FTP、TELNET 等上网行为以及用户上网流量时长等内容进行查询；
	支持日志本地存储，可对不同类型日志设置存储空间，支持日志外发至多个服务器，可设置日志传输协议、时间类型、日志语言、是否合并及加密传输等参数；
显示监控	支持系统温度、CPU 温度、CPU 利用率、内存利用率、电源故障等告警，支持 CPU 利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪；
	支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；
质保	提供三年原厂质保，三年入侵防御升级、防病毒升级；

2.2.6 远程安全访问控制设备

技术指标	技术要求
★产品规格	1U 设备，≥4 个千兆电口,整机吞吐≥600M 并发连接≥50 万 IPSEC 吞吐≥60M SSL 吞吐≥120M ，含 100 个 SSL VPN 的客户端许可。
用户管理	支持基于用户、用户组、用户角色进行授权，实现用户可访问资源、可信接入和客户端杀

	毒策略；	
	▲支持口令认证、证书认证、短信认证、硬件特征码绑定、人脸识别、图形码认证方式；（提供截图证明加盖原厂公章）	
虚拟专网	SSLVPN	支持 AES、DES、3DES、RC4、MD5、SHA1、RSA 等多种算法； 支持国家商密专用的 SM2、SM3、SM4 算法；
		支持会话功能，能够实时监控在线用户的登录时间、登录 IP、在线时间、访问流量，登录设备等多种信息；
	IPSecVPN	支持 DES、3DES、AES、MD5、SHA1、DH GROUP1/2/5、RSA 1024/2048 等加密算法； 支持高效数据流压缩算法；
		支持虚拟路由、隧道转发； 支持多机多隧道的负载均衡和备份；
		支持 DDNS 动态域名注册； 支持使用域名进行隧道定义及协商； 支持远程用户通过 L2TP 接入；
安全策略	支持基于源/目的 IP 地址、MAC 地址、端口和协议、时间、用户、角色的访问控制； 支持动态端口协议：SIP、FTP、RTSP、SQL*NET、MMS、RPC、TFTP、PPTP；	
	支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换；	
网络管理	支持 IPv6 协议数据报通信； 支持 DHCPv6；	
系统管理	▲支持“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类；（提供截图证明并加盖原厂公章）；	
	支持基于 IP 探测的链路备份功能； 支持服务器的负载均衡；	
	支持 SNMP 的 v1 、v2 、v2c 、v3 版本； 支持 SNMP MIB 扩展； 与当前通用的网络管理平台兼容，如 HP Openview 等；	

2.2.7 运维审计与风险控制设备

技术指标	技术要求
硬件要求	★标准 2U 硬件，网口≥1000M 电口*6 个,光口≥4*GE（不含硬件 BYPASS 模块),（含 2 个千兆 SFP 多模光模块)；双硬盘≥2T*2，RAID 1,硬盘可替换为 4T（两块硬盘同时替换)；1*RJ45 串口，1+1 热插拔冗余电源电源。
	★授权资产≥400 个，并发字符连接≥400 个，并发图形连接≥100 个。三年维保，永久使用。
用户管理要求	支持标准化对接 CAS、JWT 单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。
	支持采用国密加密算法进行核心敏感数据加密存储。
设备管理要求	IE/Chrom 代填应用发布：HTTP/HTTPS 协议的 web 设备，且可以直接代填账号和密码。
	支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。
数据库管理	▲标准支持 SQL Server、MySql、oracle、DB2、PostgreSQL、人大金仓（KingBaseES)、达梦（DM）数据库的协议运维代理，可实现自动登录，自动登录可直接调用本地 windows 系统的数据库客户端工具（包括 ssms、sqlwb、MySQLworkbench、mysqlcli、DbVisualizer、plsql、sqlplus、toad、db2cmd、QuestCentral、pgAdmin3、psql、ksql、Isql、DIsql、DMmanger 等)，无需应用发布前置机（需提供相关截图证明加盖原厂公章)。
	支持在 Mac 操作系统下调用 navicat 工具运维 mysql、oracle 等数据库资产。
	▲支持同时对数据库会话记录图形审计及命令提取（需提供相关截图证明加盖原厂公章)。
	支持对数据库运维会话的上行和下行命令进行审计。
自动改密要求	支持对数据库及 Web 应用的自动改密功能。
运维方式要求	▲支持 Windows/Mac 操作系统下 C/S 架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。(需提供相关截图证明加盖原厂公章)。
	运维客户端自带运维工具，可不依赖 xshell/Securecrt/mstsc 等工具进行运维操作
	客户端还至少需支持资产分组、资产连通性检测，批量运维、资产运维审批、命令审批、二次运维审批等能力。其中资产分组操作支持个性化设置，即每个运维人员可单独设置分组，相互之间独立。
	▲H5 运维方式：支持 ssh、telnet、rlogin、rdp、vnc 协议的 H5 运维，无需本地运维客户端工具（需提供相关截图证明加盖原厂公章)。
审计日志要求	支持审计主流数据库（如 DB2、oracle、mysql、sql server、PG、人大金仓、达梦）运维中的 SQL 语句，可进行关键信息定位查询，并可过滤数据库客户端自动发起的语句，方便查询真实人为的数据库操作。
应用发布要求	应用发布服务器支持集群模式 。
系统管理要求	支持 NAS 存储。
部署架构要求	支持内置 VPN 模块，无需与其他 VPN 设备联动，实现运维入口安全接入。
	支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步。

2.2.8 数据库审计与风险控制设备

技术指标	技术要求
★硬件要求	标准 2U， CPU≥4 核，内存容量≥8GB*2,）硬盘容量≥2TB*2（Raid 1），硬盘接口为企业级 SATA；电口≥1000M *6，光口≥1000M *4；双电源，2 个空余拓展板卡位。
	网络吞吐量≥2000Mbps，双向审计最大数据库流量≥200Mbps，峰值事务处理能力 TPS≥20000 条/秒，日志数量存储≥20 亿条，数据库实例授权许可数量≥12，硬件可扩容。
★部署方式	旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计。
协议支持	支持 Oracle、PostgreSQL、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ 等主流数据库的审计； 支持 GuassDB、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、K-DB 等国产数据库的审计； 支持 MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、ArangoDB、Neo4j、OrientDB 等非关系型数据库的审计； 支持主流业务协议 HTTP、HTTPS、Telnet、FTP 的审计； 可以通过导入证书的方式实现 MySQL 5.7 及以上版本采用了加密协议通讯的审计
审计功能	支持数据库操作表、视图、索引、存储过程等各种对象的所有 SQL 操作审计； 审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集； 支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容，支持通过返回行数控制返回结果集大小； 支持超长 SQL 语句（最长 4M）审计。
智能发现	支持自动发现流量中的数据库信息，简化配置。
安全审计	支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义；
	▲产品具有内置规则，规则类型有 sql 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警；（提供产品功能截图，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告证明加盖原厂公章）；
	内置安全特征库不少于 900 条，如 SQL 注入、缓冲区溢出等；
审计查询	支持基于数据库访问日期、时间、源/目的 IP、来源、数据库名、数据库表名、字段值、数据库登录账号、SQL 关键词、数据库返回码、SQL 响应时间、数据库操作类型、影响行数等条件的审计查询； 支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单
统计报表	系统内置多种报表模板库，报表不少于 20 种； 报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告； 支持基于表维度的报表分析； 支持 HTML、PDF、PNG、Word 等格式的报表导出。
模型分析	▲可依据客户端工具名、数据库账号、客户端 IP、操作系统用户名、客户端主机名、数据库名/SID、操作类型、服务端 IP 等配置行为模型，并可查看相应告警日志（提供相关截图证明加盖原厂公章）。

数据管理	支持根据在线数据最小保留天数和在线数据的磁盘空间占比自动清理早期数据。
Agent 管理	支持在审计管理端批量安装、卸载、重新安装审计代理； 支持在审计管理端启动、停止、挂起 Agent； Agent 支持设置 CPU 亲和性、最大资源使用率限制（CPU、内存）； ▲可监控 Agent 的转发速率，以及 Agent 所在数据库服务器的 CPU、内存利用率，并可设置 CPU、内存利用率的上线阈值，超阈值时 Agent 将自动停止转发数据（需提供功能截图，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告加盖原厂公章）； Agent 支持按照客户端工具、数据库账号过滤审计日志； Agent 支持在 RDP 或 SSH 登录数据库服务器运维时，审计原始登录人员的 IP 地址。
三层关联	▲可提供客户端访问 Web 服务器的 URL 和应用服务器访问数据库的 SQL 语句关联功能（需提供功能截图，并提供国家权威检测机构（公安部或国家保密科技测评中心）检测报告加盖原厂公章）。
易用性	支持对 SQL 语句进行业务化翻译。
租户化管理	支持租户化管理，针对租户的账户只授权租户可查看租户内的数据库产生的审计日志、告警信息。

2.2.9 日志审计分析设备

★硬件规格	标准 2U 硬件，1 个 console 口 网口类别：6 个千兆工作管理口(1 管理口+1HA 口+4 审计口) 硬盘≥2T*1，内存≥8G；双电源，日志处理能力 4000EPS（峰值：5000EPS） 单个磁盘可扩展至 4T(仅有 1 个盘位)，网口可扩展至 10 个（4 电、4 光） 内存最大可扩展至 16GB，资产授权数量：80（资产授权数量最大可扩展至 120 个，按资产授权数量报价收费）
用户管理	用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户；
资产管理	注册用户资产时，提供自动发现识别能力； 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。
部署方式	支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据； 支持集中式管理和升级模式； 支持分级管理模式。
日志收集	支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP、kafka 等协议方式进行日志收集,支持阿里云 SLS 日志的采集； 可通过接收协议限制日志接收速率，包括 Http 接收、syslog 接收、SNMPtrap 接收、TCP 接收、WMI 接收、aliyun 接收。 ▲支持对 Agent 进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。（需提供相关截图证明加盖原厂公章）
日志分析	可以基于日志等级进行过滤； 支持对收集到的重复日志进行自动聚合归并，减少日志量；

	▲内置 5000+解析规则，支持对收集的 5000+设备类型日志进行解析（标准化、归一化），解析规则库多达 200+，解析规则可以根据客户要求定制扩展（需提供相关截图证明加盖原厂公章）； ▲支持美观易用的思维导图模式的解析规则界面自定义（需提供相关截图证明加盖原厂公章）； 支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次 支持基于跨设备的多事件关联分析； ▲内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为 6 大类 50+子类的安全分析场景（需提供相关截图证明加盖原厂公章）； 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。
日志转发	▲syslog 转发：支持将收集到的日志进行加密(国密算法 SM4)、签名(国密算法 SM3)转发传输，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；（需提供相关截图证明加盖原厂公章） 支持大数据安全域同步、APT 沙箱报告转发等大数据联调功能； kafka 转发：支持将收集到的日志进行加密(国密算法 SM4)、签名(国密算法 SM3)转发传输；Kafka 收发支持 SSL 加密； 日志支持文本方式输出给第三方平台，进行数据共享；
日志备份	可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比等策略； 支持日志本地备份及恢复； 支持日志备份自动传送到远程服务器，支持 FTP、SAMBA、NFS 和 FILE，4 种方式的远程服务器，从远程仓库恢复数据；
日志查询	支持 B/S 模式管理，支持 SSL 加密模式访问； 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； 支持用任意关键字对所有事件进行高性能全文检索； 支持可指定多个查询条件进行组合查询； 支持将查询的条件存储为查询模版，方便再次使用；
脆弱性管理	支持从 IBM Rational AppScan 导入资产弱点漏洞信息； 支持从 NetSparker Web 应用扫描器导入网站弱点漏洞信息； 支持从 Nessus 网络扫描器导入网络弱点漏洞信息； 支持从 OpenVAS 扫描器导入弱点漏洞信息； 内置 73000+条 CVE 漏洞数据知识库； 内置数十项符合 OWASP 的 Web 漏洞数据知识库。
地理安全系统	内置 GeoSec 地理安全子系统，内置世界以及中国安全 GIS 地图； 支持用地理地图展示来源和目的威胁的趋势； 支持在地理地图上标注威胁事件的发生分布。
告警功能	可预设置安全告警策略，超过阀值将产生告警； 可以通过邮件、短信和屏幕显示进行告警； 自动防止在短时间内大量发送报警信息(告警抑制)； 具备报警合并和在一个时间段内抑制报警次数的能力。 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警； 资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定

	的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警； 远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警。
综合查询及报表管理	内置合规性报表 1000+种，SOX、ISO27001、WEB 安全等解决方案包； 内置完善的等级保护合规报表； 内置综合性自动化审计报告； 支持用户自定义报表，自定义的报表支持多个统计维度的数据集合； 支持报表导出为 PDF 和 Word 格式文件。

2.2.10 Web 应用安全防护设备

技术指标		技术要求
★硬件规格要求		产品必须为标准机架式 WAF 硬件设备而非软件 WAF。产品必须为专业性 WEB 应用防火墙设备，具备专业性 WEB 应用防火墙资质，而非 NGAF、NGFW、UTM 设备及资质
网络接口		标配≥2*GE 电管理口，标配≥4*GE 电业务口（含 2 组硬件 Bypass），≥4*GE 光业务口
电源		单电源
防护网站数量		不限
设备性能		网络吞吐量（Mbps）≥2Gbps HTTP 应用层吞吐≥1Gbps HTTP 并发连接数≥5 万 HTTP 最大新建连接数≥5000
基本功能	部署模式	支持透明串接、反向代理、旁路镜像等多种部署模式部署，支持链路聚合
	高可用	支持集群模式、主-主模式、主备模式、硬件 BYPASS、软件 BYPASS
	保护对象	支持多条链路数据的防护，防护网段数量不限
		支持 ipv4/ipv6 双协议栈
		可通过设置数据缓存、页面压缩进行 web 加速
		可以设置后端 TCP 连接模式，可根据业务特点设置长连接和短连接，并且可以通过设置连接复用，减轻后端服务器压力。
	Web 服务自发现	▲支持自动发现网络环境中存在的 Web 站点业务系统，记录服务器的 IP、Port、域名等信息。（提供功能截图加盖原厂公章）。
	HTTPS 防护	支持 HTTPS 协议的选择可以选择 SSL/TLS 协议版本，可选 SSLv3、TLS1.0、TLS1.1、TLS1.2
		▲支持HTTPS站点SSL算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果。（提供功能截图加盖原厂公章）。
		支持透明串接和旁路反向代理下的 HTTPS 业务的安全防护
		支持源地址识别，部署在 SSL 网关后面，能够解析到真实的访问者 IP，并能对真实的 IP 进行防护和阻断

		支持证书批量管理，并且支持证书有效性检测
		在单个服务器通过相同的 IP 地址为多个 HTTPS 域名提供服务时，WAF 可以通过启用 SNI，准确确定域名与证书的对应关系。
	攻击检测	支持对跨站脚本(XSS)和注入式攻击（包括 SQL 注入、命令注入 、代码注入、文件注入、LDAP 注入、SSI 注入等）的检测防护
		支持对 HTTP 请求关键字段进行合规性的检测（包括 Host 字段、User-Agent、Content-type 字段等）。
		支持防护 Java 反序列化及基于 Java 的通用攻击
		支持 XML 防护，XML 攻击行为包括 XML Ddos
		支持对 HTTP 头部各字段内容长度进行限制并可以自定义调整限制大小，包括参数名长度、参数值长度、HTTP 请求头部长度、URI 长度、cookie 长度、User-Agent 长度、Content-type 长度、Host 长度等。
		支持识别 HTTP 报文常见的编码和编码攻击：URL 解码、Base64 解码、HTML 解码、16 进制转换、JSON 解析、XML 解析、PHP 反序列解析、UTF-7 解码等
	HTTP 协议规范性检查	检查 HTTP 报文合法性
		检查 HTTP 报头是否有缺失或为空
		检查允许提交的 HTTP 方法
		检查请求报文是否畸形
		通过检查上传和下载的文件类型，防止下载敏感文件和上传 webshell 文件
		检查 HTTP 报头长度，防止缓冲区攻击
	Webshell 检测（语义分析）	内置 Webshell 检测规则，可以对上传的文件内容进行检查，防止恶意 Webshell 文件上传，对已经上传的 webshell 发起请求的行为进行拦截阻断
	敏感信息泄露检测	▲内置身份证、银行卡、手机号、社保号等个人敏感信息数据，对服务器返回的敏感个人信息数据通过星号进行隐藏，并支持用户自定义敏感词。（提供功能截图加盖原厂公章）。
		能够检测防止服务器导致的信息泄露行为，包括：目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等信息泄露行为。
		支持禁止防敏感词发布，防止提交政治敏感、违反法规相关的言论信息，保障网站的内容健康呈现
		支持服务器信息隐藏，可配置删除服务器响应头信息
	爬虫、扫描器等自动化工具的安全检测	▲内置安全规则可有效识别 Acunetix、nessus 、WebScan、Webdump 等扫描器的扫描行为。（提供功能截图加盖原厂公章）。
		内置安全规则可有效识别 baidu、google、yahoo 等常见网络爬虫的访问行为
	第三方组件漏洞防护	支持防护 WEB 容器漏洞，防止 Nginx、IIS、Tomcat 等 WEB 服务器漏洞
		支持防护 Kuwebs、phpcms、TRS WCM、JBR-CMS、DeDeCMS 内容管理系统等开源 CMS 漏洞
		支持防护 WEB 服务器插件漏洞，防止 Apache Struts2 漏洞

	盗链攻击检测	支持多种盗链识别算法能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问。
	Cookie 安全	支持 Cookie 自学习，支持 Cookie 防篡改、防劫持
	自定义规则	支持对 HTTP 请求中 URI、HOST、参数、参数名、请求头、Cookie、版本号、方法和请求体及 HTTP 响应的响应体等条件进行自定义正则，支持多种组合条件，并且对于编写的正则表达式需要支持在 WAF 的管理界面上在线验证合规性。
	基于时间的访问控制	可基于时间设置对客户端 IP 放行、阻断或检测
	支持第三方扫描工具结果导入	虚拟补丁，支持 Appscan 扫描结果导入
	防护动作	支持阻断、重定向、智能加黑名单、丢弃、告警、仅检测等动作。不同的防护规则，可以选择不同的防护动作及返回码，也可针对不同规则设置专属 URL 白名单。
高可靠性	链路聚合	支持链路聚合，提升网络带宽、增加容错性和链路负载均衡
	VLAN 子接口	支持 VLAN 子接口，业务口可承载多个 VLAN 通道
	HA	支持集群模式、主-主模式、主备模式
	运行模式	透明代理部署下，可支持对全局设置物理直通、网桥直通、纯代理、正常防护模式，也可针对单个保护站点设置不同的运行模式。反向代理部署下，可支持对全局设置纯代理或正常防护模式，也可针对单个设置不同的运行模式。
高级功能	智能语义分析	内置对 SQL 注入、XSS 攻击检测的语义分析规则。
	机器学习	1、具有机器学习安全引擎，可以对用户 web 业务系统建立安全的访问模型 ，学习的内容包括 URL 地址、URL 请求参数等信息 2、▲支持设定学习的周期，域名信息，可信任的客户端 IP，不可信的客户端 IP 以及不学习的 URI 信息。（提供功能截图加盖原厂公章）。
	智能攻击者锁定	支持智能识别攻击者，对网站连接发起攻击的 IP 地址进行自动锁定禁止访问被攻击的网站，可配置攻击者锁定时间，可配置将攻击者直接加入网络黑名单。
	安全审计	能详细记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，cookie 等所有的请求头内容。
		能详细记录服务器响应头信息，服务器响应内容

2.2.11 防病毒系统

2.2.11.1 虚拟化防病毒系统

技术指标	技术要求

★授权配置		配置 1 个控制中心，配置 10 颗 CPU 防病毒功能，提供三年升级服务；
部署与实现	一体化控制中心	1.虚拟化安全产品自带高性能数据库，无需外置数据库即可实现日志存储和分析关联； 2.虚拟化安全产品自带升级、查询、代理功能，无需额外部署升级服务器、代理服务器等节点； 3.产品提供已加固的安全操作系统作为集中控制系统的运行环境，支持集中控制系统打包在安全操作系统中以实现简易交付；
	▲部署模式	同时支持无代理部署和轻代理部署两种部署方式，实现 VMware vSphere、Citrix XenServer、华为 FusionSphere、华为 FusionSphere(KVM)等混合统一管理。(提供界面截图加盖原厂公章)；
	多租户支持	1.支持直接使用虚拟化平台租户账号登录/管理安全配置； 2.支持不同租户日志、管理、策略相互隔离；
	高可用	统一管理控制应支持高可靠机制，保障控制节点无单点故障 ；
兼容与支持	▲虚拟化平台支持	应支持 VMware 、Ctrix、Huawei 、H3C、中兴、浪潮、青云等国内外主流虚拟化厂商平台，提供兼容性认证材料或产品界面截图证明加盖原厂公章；
	操作系统支持	1. 应至少支持 Windows 7/8/10 等云桌面常见操作系统类型，Windows Server2003/2008/2012/2016 等虚拟化环境常见基于 Windows NT 的服务器操作系统； 2. 应支持 SuSE、Red Hat、Ubuntu、Debian、CentOS、Asianux、NeoKylinLinux 等虚拟化环境常见基于 Linux 内核的操作系统；
虚拟化杀毒	杀毒防护方式	支持快速扫描、全盘扫描；支持个性化扫描，能够基于不同路径、不同文件类型、时间等进行自定义病毒扫描查杀；支持实时防护。
	自主信任	应支持对病毒文件进行手动恢复操作、对目录、文件、扩展名进行白名单操作，以提升查杀效率和降低误杀率；
	黑白名单	支持除文件、文件夹例外，还支持单独的病毒黑白名单的管理运维；
	病毒回溯	支持对已识别病毒文件的名称、路径、类型等进行记录溯源 ；
	查杀调度	能感知物理机的任务状态，智能调度任务执行，防止引发启动、查杀风暴；
	缓存机制	1.支持对虚拟机相同文件不会重复检测； 2.支持对虚拟机文件进行增量检测扫描，只检测扫描有修改的文件；
	分析呈现	支持基于虚拟主机维度、恶意文件类型维度进行多种分析呈现展示；
	白名单预置	产品应支持预置基于文件指纹的白名单功能，提高病毒检测和查杀的效率；
	病毒库更新	支持手动升级病毒库，页面展示病毒库的更新时间及升级结果。
系统加固	应用程序控制	1.支持对应用程序进行监控、阻止动作； 2.支持对应用程序名称、应用程序路径设置例外； 3.支持对 windows 和 linux 系统应用程序设置进行统一设置。
防火墙		1.支持对出入虚拟机/终端流量的访问控制； 2.支持通过源目的 IP、源目的端口、协议、方向进行控制； 3.支持批量进行防火墙规则的删除和复制；
分析呈现	态势感知	支持数据中心威胁态势感知，大屏动态展示安全运维状况，结合地理位置信息全面呈现威胁攻击详情；

	流量统计	▲支持按总流量、恶意软件、新建连接对流量进行统计和展示，提供截图证明加盖原厂公章；
		支持按主机池、分组、虚拟机/终端、网络协议、网络协议组、国家/地区、城市等维度对流量进行统计和展示；
	日志分析	支持按照不同分组、虚拟机/终端、网络协议、网络协议组、国家/地区、城市，分不同威胁类别以柱状图、折线图（曲线图）、饼图、原始日志等形式进行展示。
	报表	1.支持手动或者定时定期生成报表； 2.可指定任意虚拟机/终端、主机池进行报表生成； 3.可自定义安全日志报表呈现形式，比如：数量排名、图形展示、安全日志类型等。
其它特性	Syslog 支持	产品应支持 Syslog，支持将安全日志发送到第三方服务器上。
	NTP 支持	产品应支持自定设定 NTP 和手动设定时间 。
	多账号管理	产品应支持多账号，不同账号设定不同功能使用和访问权限 。
	监控与告警	1. 支持实时显示告警数量，可支持手动解除告警； 2. 支持不少于 12 种异常监控与告警规则。
	产品个性化	产品支持自定义 Logo、产品名称等定制。
	IPv6 的支持	控制台支持对 IPV6 可配置，可通过 IPV6 网络访问，兼容 IPv6 的网络场景。

2.2.11.2 终端杀毒系统

技术指标	技术要求
★授权配置	配置 1 个控制中心，配置 300 个终端防病毒功能，提供三年升级服务；
控制中心安装环境要求	操作系统支持 Windows Server 2008 R2/2012/2012 R2/2016 的 64 位版本（简体中文版）； 支持 CentOS 7、Redhat 7 等 Linux 系统（要求 Docker 版本务必大于 1.8.2）；
操作系统支持	中标麒麟/银河麒麟/普华/深度/红旗等操作系统。
系统管理	控制中心：采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、统一管控、统一终端准入合规、终端软件管理、硬件资产管理以及各种报表和查询等功能；
	支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告；
	支持控制中心防暴力破解，采用手机 APP 动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证，要求令牌 APP 自主研发；
资产管理	支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件
	资产自助登记：新增资产登记类别、设置字段是否必填、设置字段是否显示、设置终端输入类型、可设置设备类型、设备用途、使用人、电话、邮箱等信息要求终端登记
	支持正版软件的正版序列号的读取功能，确保软件正版化。
防病毒	支持病毒木马威胁的快速扫描、全盘扫描、强力扫描、文件专杀、隔离区恢复、系统修复、插件管理

防感染模式	扫描到感染型病毒时，自动进入防感染模式，重新开始全盘扫描并阻止恶意样本反复感染文件
黑白名单例外	▲支持手工导入 MD5+SHA1 的黑白名单方式，支持 txt 批量导入方式；（提供产品界面截图，并加盖原厂公章）
	支持下发忽略白名单的病毒扫描；
	支持对 windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理；
▲产品资质	产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》内网主机监测（基本级）资质证书；（提供产品资质证书） 产品具备软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书；（提供产品资质证书）

2.2.12 IT 统一运维管理系统

技术指标	技术要求
基础要求	运维监控系统支持管理机房服务器、网络设备、数据库、存储等设备。通过数据采集服务对机房的设备硬件性能、网络状况和系统进行资源监测管理、网络设备管理、统一监控展示、告警管理、健康报告，实现可视化运维监控、预警监控、安全管控、实时监控、实时反馈、以及各种方式告警呈现并生成定制的运维监控报表，保证各业务生产平台持续稳定运行；同时帮助机房维护人员脱离繁杂的信息化建设细节，通过对信息资源的统一监控，提高系统利用率，降低运维成本。
总体要求	1、为保证平台的稳定性和安全性，要求必须采用 Linux 操作系统。 同时为保证用户对本软件的知识产权及相关产品版权，要求提供软件运行所需数据库及数据库授权。
	2、要求平台为终身授权，开放系统功能模块供用户使用，需要支持管理网络设备、服务器、数据库、存储、标准应用。同时，在免费售后服务期限内，免费提供产品售后及升级服务。
	3、要求平台为基于内网的企业级运维监控产品，平台以业务系统监控为主线，实现集业务、软件（包含数据库、中间件、虚拟化软件）、网络、设备、Web 应用的多维度立体化统一运维监控及数据分析。支持微信、钉钉、邮箱等进行报警的接收和查询。同时支持以邮件、短信、页面、声音的多种报警方式。
	4、要求平台支持业务视图、管理视图和我的视图的多视图管理。业务视图包括业务状态；管理视图包括用户权限管理、关联接口管理；我的视图包括：我所负责管理的系统运行状态监控以及我所管理的业务所对应的报警，对于我所管理的服务器的 CPU、内存指标项要求在一个图表里同时展示对比图。 要求平台提供大屏展示的自定义拖拉式控件编辑、自定义大屏数据展示功能。
	5、要求平台实现 3D 可视化设计功能，并能进行立体图形展示。展示时要与相应的服务器、数据库等信息相结合，提供在 3D 拓扑图上进行报警定位。
	6、要求平台支持单机部署、或分布式部署，以实现监控负载均衡。要求平台支持安全网闸隔离状态下多个网络的相关业务、软件、网络、设备的统一监控、统一报警。
	7、要求平台具备用户权限管理功能，支持超级管理员用户、guest 用户，以及自定义的普通用户，每个用户具备分权限管理的功能。
	8、要求平台提供在一个界面内对被监控清单设备的报警、提醒、正常的直观展示；要

	求平台提供业务拓扑图以展示业务系统与所关联的服务器/数据库/中间件/指定端口/服务/程序/Web Service 等资源的对应关系；要求平台提供对业务系统所关联服务器的性能、系统、网口、配置、日志的报警展示。
资源监测管理	9、资源监测管理：系统集网络安全设备、应用服务和基础支撑系统等监测管理于一体，支持 SNMP 、IPMI、CLI 、JMX 等远程监控手段和 Agent 代理监测， 各类标准应用协议仿真，提供对整个业务网络的 7*24 不间断监控。
	10、服务器系统管理：系统能够管理和监测 Windows、Linux 、IBM AIX、、SUN Solaris 、等不同操作系统的服务器或集群的运行状态和性能数据，包括服务器的基本信息、CPU 负载、内存利用率、应用进程、文件系统、磁盘空间和吞吐、事件与错误日志等信息的分析与监视。帮助用户及早发现服务器系统的性能瓶颈与故障隐患。
	11、数据库管理：根据预定义的监测项目对 Oracle、SQL Server、MySQL 等多种数据库，按照属性相关性分为数据库工作状态、数据库表空间的利用情况、数据文件和数据设备的读写命中率、数据碎片的情况、数据库的进程状态、数据库内存利用状态等属性监测组，分组监测数据库系统的性能、事务、连接等性能数据。
	12、中间件管理：产品支持对 WebLogic 、MQSeries、Tomcat、等各类不同中间件，提供包括配置信息、连接池、线程队列、负载监测、通道情况监测等多类监测组，分析与监测中间件的各项运行状态参数。
	13、基础运行环境管理：对于 IT 环境系统，系统支持各种智能设备的快速监测，同时通过 SNMP、数据库接口等其他接口方式可以实现客户化的扩展监控。
网络设备管理	14、系统具备拥有灵活、高效的网络采集引擎，能通过对象识别、采集并发及针对的厂商扩展脚本，可准确、 可靠的提供网络设备交互服务。系统支持网络探测和信息采集，对发现的网元对象能自动识别、分析、保存，形成统一的网管资源库。
统一监控展示	15、通过统一监控展现功能，能够将不同类型的设备、系统、应用等资源的监控平台进行集成，避免使用多个系统进行监控管理。通过综合的展现平台来同时展示各种监控视图，以便于运维人员在一套系统上统揽全局。
告警管理	16、多样化即时消息通讯接入：支持微信、钉钉、邮件的接入，提供便捷扩展接口以支持特定的医疗信息化内部即时通讯平台。
	17、权限管理：平台已授权人员，通过平台注册、审核后，进行对应权限组的告警消息收发、订阅、查询。
	18、分组管理：支持把不同种类（错误、告警、提醒等）的消息推送给指定的人员。支持按照告警信息级别，推送给有对应级别权限的人，进行处理。
	19、过滤功能：支持用户自定义不同级别的告警信息关键字。对于这些级别之外的消息进行过滤，不会推送消息给运维人员，过滤掉无用的信息。
	20、定时检测：可自定义设置检测时间，设置检测的频率，检测出现的各类错误、告警、提醒等消息。
	21、邮件预警：支持系统的人员管理、分组管理、模板管理、消息管理、汇总统计图表等。支持管理员自行调整系统监控分组管理，哪些用户可以接收何种级别的告警信息。
	22、消息组管理：支持包含：服务器、数据库、存储、备份等不同消息组；支持人员管理：管理消息组里面的人员，以及对应的数据组权限；支持消息模板：数据组所使用的消息模板管理。
	23、消息推送：提供消息推送服务，包含消息通道的管理，消息接收对象的管理、消息发送策略的配置等。
	24、健康报告下载：系统具备报表下载功能，能够为用户提供告警、状态、时间、资源

	多个角度的统计和分析报表，以 Excle 报表形式展现分析统计结果。
★兼容性	运维监控软件须具有很强的应用兼容性，须与整个 IT 全业务系统对接进行全业务流程运维监控。因此，在搭建和监控过程中不得与用户现有其它业务系统冲突（提供承诺函加盖投标人公章）。
★授权要求	本次配置≥200 台被监控节点监控授权，最大支持扩容至≥1000 个节点。（提供承诺函加盖投标人公章）。 同时，在免费售后服务期限内，免费提供产品售后及升级服务。
★服务	提供三年原厂技术支持服务。

2.2.13 网络安全运维服务

（1） 安全整改服务：配合医院和等保测评机构对医院现有信息化环境进行有效整改；

（2） 值守服务：提供重大节日，省市级攻防演练期间工程师值守服务；

（3） 漏扫服务：根据采购人要求，按需提供人工漏扫服务，提供漏扫报告；

（4） 培训服务：根据采购人需求，提供专业安全服务人员为用户提供安全培训，帮助提高用户单位相关人员的安全意识和相关安全技能，减小因人员造成的安全风险。

2.2.14 系统集成及运维服务要求

2.2.13.1 巡检服务主要要求

✧ 通过定期的、计划性的预防性维护，将设备问题消灭在萌芽状态，确保采购方业务系统能正常稳定的运行。

✧ 每月巡检一次，在每月初的第一周对所有维保设备予以全面检测，确认设备运行状态，检查系统错误记录，排除潜在隐患。

✧ 通过定期的、计划性的预防性维护，将设备问题消灭在萌芽状态，确保甲方业务系

2.2.13.2 运维服务主要要求

✧ 建立本项目运维服务体系，制定运维服务流程和运维服务方案。

✧ 建立主动式服务流程、响应式服务流程、故障处理流程、备品备件管理

流程、服务改进流程等。

✧ ★本项目要求投标人提供“7×24 小时”服务。提供全年每周 7 天、每天 24 小时的全天候服务和每天 24 小时热线电话服务，节假日照常工作。

✧ 如果发生硬件系统停机故障，应在 60 分钟内全面恢复。

2.2.13.3 服务团队主要要求

本项目中标商应针对本项目专门成立项目组，配置高级项目经理一人，项目组成员不少于 8 人。

由于本次项目涉及到数据容灾建设和信息安全建设，同时要对医院现有的信息化架构进行改造，因此要求项目组成员应具备数据容灾、虚拟化、网络、网络安全、数据库、存储设备相关认证资质的工程师，投标文件中提供相关技术证书扫描件并加盖投标人公章。

特情驻场服务：供应商应根据用户要求，对重要时间节点（如系统升级、应用上线、年底结转等）提供必要的短期驻场服务，提供 7*24 小时技术支持服务，费用包含在投标总报价中。要求投标人派驻提供特情驻场服务的工程师具备相应的技术资质认证证书，投标文件中提供相关技术证书扫描件并加盖投标人公章。

★投标人需对本条做出书面承诺：中标后，采购人将对中标人提供的上述证书证明材料逐一进行复核；中标人提供的项目组成员必须为本单位人员，并不得随意更换项目组成员，在进场实施之前中标人必须向采购人提供为项目组成员缴纳社保的证明材料（进场实施时间点之前最近三个月社保），如发现中标人安排的项目组成员相关证书和社保材料与投标文件中承诺不一致的，或相关材料存在虚假行为的，采购人要求中标人在规定时间内更换项目实施团队组成人员，直至满足招投标参数为止（如招标文件与投标文件不一致的以有利于采购人要求的为准）；由此带来的后果包括并不限于暂不签订合同、可能对中标人产生的信誉以及对医院运营影响产生的相关费用索赔由中标人全权负责。

2.2.13.4 服务档案主要要求

✧ 对服务范围内的所有系统和设备，应建立相应的系统维护档案，并根据每次故障维修报告和预防性维护报告建立技术档案，记录每次故障响应服务和预防性维护的详细信息。

✧ 投标人须为本项目建立专门的系统维护档案，服务提供方工程师第一次到现场巡检时，要做出保修设备的详细配置清单、所使用的操作系统、版本号、系统的使用情况及系统的配置参数。

✧ 每次巡检为每台保修设备填写巡检表，记录设备的运行情况，以及出现过的问题和解决的办法，设备的配置变动情况。对每次故障处理时，填写设备服务记录表，记录故障的现象，处理的过程，换设备的情况，并记录更换设备的原型号和现型号。巡检后提交巡检报告和巡检表，故障处理后提交设备服务记录表，双方签字。

2.2.13.5 培训要求

投标方应提供不少于以下培训内容：

（1） 不少于 3 人×3 天的数据容灾技术培训；

（2） 不少于 3 人×3 天的虚拟化平台容灾培训；

（3） 不少于 3 人 x3 天的容灾恢复演练培训；

（4） 不少于 3 人×3 天的网络安全培训。

投标方须在响应文件中提出全面、详细的培训课程以及时间表，具体执行时间在合同签定后由采购方指定，培训所发生的所有费用，包括培训费、报名费、材料费、场地费、住宿费、交通费、考试费、证书费、认证费等全部由投标人承担。

本表是对第五章“政府采购合同格式”的补充和修改。如果两者之间有抵触，以本专用条款表为准。

条款号	内容
6	履约保证金：本项目不收取履约保证金。
7	★免费质保期：3 年。免费质保期间，中标人免费包维修、保养、安检、调换等；对于采购方人为原因造成的故障，中标人只收取维保成本费用。所有软件终身免费升级。
8	★1. 交货期：设备交货期 30 工作日，设备安装调试工期 15 工作日。 2. 交货方式：现场验收。 3. 交货地点：采购人指定。

9.1	★付款方式：合同签订后支付合同金额 30%的预付款，到货后支付合同金额 40%的到货款，货物安装调试验收合格移交后 5 个工作日内，支付合同金额 30%的验收款。支付验收款之前乙方向甲方开具全额正规发票，甲方对满足合同约定支付条件的项目 30 日内将资金支付到约定的供应商账户（以双方共同签字的合同、到货验收单、项目验收文件等材料日期计算）.付款前需提供完税发票，采购人收到发票后 30 日内将资金支付至中标供应商账户（以发票开具日期计算）。
10.3	项目验收：项目完成全部建设内容，提交全部有关技术文件、资料等文档，中标供应商须书面提出申请，经采购人同意并组织专家进行最终验收。如验收不能通过，中标供应商应在验收规定的期限内对存在问题进行整改， 直至系统合格，方能通过验收。
13	违约责任： 具体违约条款及其它未尽事宜，将在双方签订合同时议定。

第五部分　合同

赣 榆 区 政 府 采 购

合同

合同编号：

采购人：

中标人：

以下为中标后签订本项目合同的通用条款，中标供应商不得提出实质性的修改，关于专用条款将由采购人与中标供应商结合本项目具体情况协商后签订。

赣榆区政府采购合同

甲方：【采购单位】
乙方：（卖方）_____
备案方：赣榆区公共资源交易中心

甲、乙双方根据　　年　　月　日【标段名称】项目（标段编号：【标段编号】）的采购结果，签订本合同。

一、货物内容
1.1 货物名称：
1.2 型号规格：
1.3 技术参数：
1.4 数量（单位）：
二、合同金额
2.1 本合同金额为（大写）：_____元（¥_____）人民币。
（详见投标报价表）
三、技术资料
3.1 乙方应按招标文件规定的时间向甲方提供使用货物的有关技术资料。
3.2 没有甲方事先电子同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。
四、知识产权
4.1 乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的专利权、商标权或著作权。
五、无产权瑕疵条款
5.1 乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。如乙方所交货物有产权瑕疵的，视为乙方违约，按照本合同第 13 条第 3 款的约定处理。但在已经全部支付完合同款后才发现有产权瑕疵的，除了支付违约金，乙方还应负担由此而产生的一切损失。
七、质保期
7.1 质保期　　年（自交货验收合格之日起计）。　　。
八、交货期、交货方式及交货地点
8.1 交货期：　　。
8.2 交货方式：　　。
8.3 交货地点：　　。
九、合同款支付
9.1 付款方式：合同签订后支付合同金额 30%的预付款，到货后支付合同金额 40%的到货款，货物安装调试验收合格移交后 5 个工作日内，支付合同金额 30%的验收款。支付验收款之前乙方向甲方开具全额正规发票，甲方对满足合同约定支付条件的项目 30 日内将资金支付到约定的供应商账户（以双方共同签字的

合同、到货验收单、项目验收文件等材料日期计算)。付款前需提供完税发票，采购人收到发票后 30 日内将资金支付至中标供应商账户（以发票开具日期计算)。

9.2 当采购数量与实际使用数量不一致时，乙方根据实际使用量提供产品和服务，合同的最终结算金额按实际使用量乘以中标单价进行计算。

十、质量保证及售后服务

10.1 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

10.2 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

（1）更换：由乙方承担所发生的全部费用。

（2）贬值处理：由甲乙双方合议定价。

（3）退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、合同款利息及银行手续费等)。

10.3 测试要求：乙方安装后现场测试，提供测试报告，甲方验收签字确认。

十一、调试和验收

11.1 甲方对乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准进行现场初步验收，外观、说明书符合招标文件技术要求的，给予签收，初步验收不合格的不予签收并可立即要求退换。货到后，甲方需在五个工作日内验收。在采购人将所有的货物按招标文件要求和国家标准或行业标准进行检测验收后，发现有其他非故意的损坏或质量问题的，由中标供应商立即予以更换，不得拒绝和延误。

11.2 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

11.3 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收。

11.4 验收时乙方必须在现场，验收完毕后作出验收结果报告；安装调试费用由中标供应商负责。

11.5 对技术复杂的项目，甲方可组织有关部门和专家进行验收，并出具验收报告，相关费用由甲乙双方协商解决。

十二、货物包装、发运及运输

12.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

12.2 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

12.3 乙方在货物发运手续办理完毕后 24 小时内或货到甲方 48 小时前通知甲方，以准备接货。

12.4 货物在交付甲方前发生的风险均由乙方负责。

12.5 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方货物已送达。

十三、违约责任

13.1 甲方无正当理由拒收货物的，甲方向乙方偿付拒收合同款总值的百分之五违约金。

13.2 甲方无故逾期验收和办理合同款支付手续的，甲方应按逾期付款总额每日千分之五向乙方支付违约金。

13.3 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之五向甲方支付违约金，由甲方从待付合同款中扣除。逾期超过约定日期 10 个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值 5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

13.4 乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

十四、不可抗力事件处理

14.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

14.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

14.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十五、争议解决

15.1 双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，按下列第（1）种方式解决：

（1）向仲裁委员会申请仲裁。

（2）向合同签订地法院起诉，合同签订地在此约定为赣榆区。

十六、合同生效及其它

16.1 合同经双方法定代表人或授权委托代理人签字并加盖单位公章后生效。

16.2 下述合同附件为本合同不可分割的部分并与本合同具有同等效力：

（1）供货清单和分项价格表

（2）技术规格

（3）乙方报价函的内容及其澄清内容

（4）其他与本合同相关的资料

（5）本合同适用的特殊条款

16.3 本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

16.4 本合同正本一式四份，具有同等法律效力，甲乙双方、备案方各执一份，采购人报一份至政府采购监督管理部门。

甲方：	乙方：
地址：	地址：
法定代表人：	法定代表人：
委托代理人：	委托代理人：
电话：	电话：
传真：	传真：

签订日期：　　年　月　日

第六部分　投标文件格式

赣榆区政府采购

投标文件

标段名称：

标段编号：

投标人名称：

投标人地址：

法定代表人：

委托代理人：（委托代理时填写）

日　　期：

格式 1、响应函

响 应 函

致：连云港市赣榆区中医院根据贵方赣榆区中医院信息安全建设项目标段（标段编号：320721-J-GYJZ2023G020-1）采购文件，正式授权下述签字人全权代表参加贵方组织的采购活动，按照采购文件要求提交响应文件。

据此函，签字人兹宣布同意如下：

1.按采购文件项目需求提交响应报价，报价、服务期等详见开标一览表。

2.我方同意在本标段采购文件中规定的响应文件递交截止之日起 60 天内遵守本响应文件中的承诺且在此期限期满之前均具有约束力。

3.我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商应当具备的条件：

(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)参加此项采购活动前三年内，在经营活动中没有重大违法记录。

4.我方根据采购文件的规定，承担完成合同的责任和义务。

5.我方已详细审核采购文件，我方知道必须放弃提出含糊不清或误解问题的权利。

6.如果在响应文件有效期内撤回或者有其他违约行为，我方的保证金可被贵方全部或部分没收。

7.同意应贵方要求提供与本次采购活动有关的任何数据或资料。

8.我方完全理解，最低报价不是中标（成交）的唯一条件。

9.若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

10.我方将严格遵守《中华人民共和国政府采购法》第七十七条规定，供应商有下列情形

之一的，处以采购金额5‰以上10‰以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

(1)提供虚假材料谋取中标、成交的；

(2)采取不正当手段诋毁、排挤其他供应商的；

(3)与采购人、其他供应商或者采购代理机构恶意串通的；

(4)向采购人、采购代理机构行贿或者提供其他不正当利益的；

(5)在招标采购过程中与采购人进行协商谈判的；

(6)拒绝有关部门监督检查或提供虚假情况的。

法定代表人或其委托代理人签字（或盖章）：

供应商公章：

日期：

注：未按照本响应函的格式要求填写的，将造成非实质响应，从而导致该供应商响应无效。

格式 2、开标一览表

开标一览表

标段编号：320721-J-GYJZ2023G020-1

标段名称：赣榆区中医院信息安全建设项目

标题	内容
投标报价	
服务期限	

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式3、具备履行合同所必需的设备和专业技术能力的声明及证明材料

具备履行合同所必需的设备和专业技术能力的声明

（供应商名称）郑重声明：我单位具备履行本项采购合同所必需的设备和专业技术能力，为履行本项采购合同我单位具备如下主要设备和主要专业技术能力：

主要设备有：。

主要专业技术能力有：。

注：须附证明材料。

声明人（盖章）：

日期：年月日

格式 4、参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明

声　明

我公司郑重声明：参加本次政府采购活动前 3 年内，我公司在经营活动中没有因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式 5、法定代表人授权委托书

法定代表人授权委托书

【采购单位】：

本授权书声明：注册于（委托单位全称）的法定代表人代表本公司授权（姓名和职务）为本公司合法代理人，就贵方组织的有关【标段名称】项目（标段编号：【标段编号】）的招标采购及合同签订、执行、完成，以本单位名义处理一切与之有关的事务。

本授权书于年月日签字（或盖章）生效，特此声明。

委托单位（盖章）：　　法定代表人（签字或盖章）：

签发日期：年月日

附法定代表人与委托代理人身份证明正反面电子件。

说明：

1．委托书内容填写应当明确、文字工整清楚，涂改无效。

2．委托书不得转借、转让、买卖。

3．委托代理人根据授权范围，以委托单位的名义签订合同，并将此委托书提交给采购单位作为合同附件。

格式 6、商务条款偏离表

商务条款偏离表

请逐条对应采购文件“项目需求”等内容要求的商务条件，填写该表。

项号	采购文件的商务条款	投标文件的商务条款	偏离说明

注：“偏离说明”填写“正偏离”“负偏离”或“无偏离”。

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式 7、售后服务承诺书

售后服务承诺书

（供应商按“项目需求”等内容要求自行填写，格式自定）

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式 8、财务状况报告及税收、社会保障资金缴纳情况承诺函

财务状况报告及税收、社会保障资金缴纳情况承诺函

致：*【采购单位】*

我方*供应商名称* 参加*【标段名称】*（项目编号：*【标段编号】*）采购，根据《关于简化政府采购供应商资格审查有关事项的通知》（连财购〔2023〕4 号），我方承诺具备《中华人民共和国政府采购法》第二十二条第（二）、第（四）项，《中华人民共和国政府采购法实施条例》第十七条第（二）项规定条件的，具体包括：

（1）具有良好的商业信誉和健全的财务会计制度（财务状况报告）；

（2）有依法缴纳税收和社会保障资金的良好记录。

我方对上述承诺的真实性负责，如有虚假，将依法承担提供虚假材料谋取中标、成交责任，同时同意有关主管部门将相关失信信息记入公共信用信息系统并在相关政府门户网站公开。

特此承诺

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式 9、技术规格偏离表

技术规格偏离表

请按所响应产品的实际技术参数，逐条对应采购文件“项目需求”中要求的技术规范填写该表，该表不能作为所响应产品的技术文件，供应商应在响应文件中单独提供技术文件。

项号	采购文件需求			响应产品规格及技术参数				偏离说明
	货物名称	数量	技术参数要求	货物名称	数量	品牌、厂家、型号规格	技术参数	

注：“偏离说明”填写“正偏离”“负偏离”或“无偏离”。

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式 10、项目需求响应

项目需求响应

（供应商按“项目需求”等内容要求自行填写，格式自定）

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式 11、其他材料

其它材料

（投标人对招标文件响应有必要提供的材料或评标办法中要求提供的材料）

投标人（盖章）：

法定代表人或委托代理人（签字或盖章）：

日期：　　年　　月　　日

格式 12、中小企业声明函

中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司参加（单位名称）的（项目名称）采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业的具体情况如下：

1. （货物名称），属于（采购文件中明确的所属行业）行业；制造商为（企业名称），从业人员人，营业收入为万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

2. （货物名称），属于（采购文件中明确的所属行业）行业；制造商为（企业名称），从业人员人，营业收入为万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：　　年　　月　　日

填报说明：

1、从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2、请供应商如实填写，所填内容将作为评审的依据。其内容填写须与报价明细表一致，如填写不完整或不一致，将不享受扶持政策。

3、中标供应商的《中小企业声明函》随中标结果公开。

格式 13、残疾人福利性企业声明函

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国中医院关于促进残疾人就业政府采购政策的通知》(财库〔2017〕141 号)的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物，或者提供其他残疾人福利性单位制造的货物(不包括使用非残疾人福利性单位注册商标的货物)。相关企业的具体情况如下：

1. （货物名称），制造商为（企业名称），属于残疾人福利性单位；
2. （货物名称），制造商为（企业名称），属于残疾人福利性单位；

……

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称(盖章)：

日期：　　年　　月　　日

填报说明：

1、请供应商如实填写，所填内容将作为评审的依据。其内容填写须与报价明细表一致，如填写不完整或不一致，将不享受扶持政策。

2、中标供应商的《残疾人福利性单位声明函》随中标结果公开。