

兰溪市中医院数据中心系统项目

公开招标文件

项目名称：兰溪市中医院数据中心系统项目

项目编号：**jhjp-lxszyy20230310012**

采购单位：兰溪市中医院(盖章)

采购代理机构：金华景鹏工程咨询有限公司(盖章)

2023 年 03 月

目录

第一章公开招标公告	1
第二章前附表	8
第三章招标需求	13
第四章投标供应商须知	56
第五章开标和评标须知	66
第六章评标细则	75
第七章合同	80
第八章投标文件格式	85



第一章公开招标公告

项目概况

兰溪市中医院数据中心系统项目的潜在投标供应商应在浙江政府采购网（<http://zfcg.czt.zj.gov.cn/>）或政府采购云平台（<https://www.zcygov.cn/>）或政府采购云平台电子投标客户端获取（下载）招标文件，并于 2023 年 04 月 11 日 10:00（北京时间）前递交（上传）投标文件。

一、项目基本情况

项目编号：jhjp-lxszyy20230310012

项目名称：兰溪市中医院数据中心系统项目

采购方式：公开招标

预算金额（元）：12800000

最高限价（元）：12700000

采购需求：

标项序号	标项名称	数量	单位	最高限价（元）	简要规格描述	备注
1	兰溪市中医院数据中心系统项目	项	1	12700000	详见《招标需求》	

合同履行期限：详见招标文件

本项目（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》第二十二条规定和浙财采监【2013】24号《关于规范政府采购供应商资格设定及资格审查的通知》第六条规定，且未被“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、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

2. 落实政策：

（1）落实政府采购政策需满足的资格要求：

☒ 专门面向中小企业：

☐ 货物全部由符合政策要求的中小企业制造，提供中小企业声明函；

☐ 货物全部由符合政策要求的小微企业制造，提供中小企业声明函；



- ☐工程全部由符合政策要求的中小企业承接，提供中小企业声明函；
- ☐工程全部由符合政策要求的小微企业承接，提供中小企业声明函；
- ☒服务全部由符合政策要求的中小企业承接，提供中小企业声明函；
- ☐服务全部由符合政策要求的小微企业承接，提供中小企业声明函；

(2) 采购项目需要落实的政府采购政策：执行节约能源、保护环境相关的节能产品政府强制采购和优先采购政策，执行环境标志产品政府优先采购政策；执行扶持不发达地区和少数民族地区、促进中小企业发展、支持监狱企业发展、促进残疾人就业、支持中小企业信用融资等政府采购政策。

3.本项目的特定资格要求：无。

三、获取招标文件

时间：公告发布之日至投标截止时间前；每天上午 00:00 至 12:00，下午 12:00 至 23:59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

地点（网址）：浙江政府采购网（<http://zfcg.czt.zj.gov.cn/>）或政府采购云平台（<https://www.zcygov.cn/>）或政府采购云平台电子投标客户端；

方式：请登录浙江政府采购网（<http://zfcg.czt.zj.gov.cn/>）或政府采购云平台（<https://www.zcygov.cn/>）或政府采购云平台电子投标客户端进入搜索相应项目获取（下载）招标文件，并致电 0579-81293312 进行确认。（获取招标文件时需提供以下资料）

- (1) 政府采购报名表（格式见公告附件）；
- (2) 经有关部门年检通过且在有效期内的《营业执照副本》或《事业单位法人证》复印件；
- (3) 授权委托书（法定代表人报名需要提供法定代表人身份证明书）、法定代表人身份证复印件、受委托人身份证复印件；

(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；

以上资料均应复印件加盖企业公章扫描上传政府采购云平台系统或发送至 1687413311@qq.com 邮箱，纸质报名资料邮寄至金华景鹏工程咨询有限公司存档备用。

售价（元）：免费（不提供纸质版招标文件）。

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2023 年 04 月 11 日 10: 00（北京时间）



投标地点（网址）：政府采购云平台（<https://www.zcygov.cn/>）在线投标

开标时间：2023 年 04 月 11 日 10: 00

开标地点（网址）：兰溪市振兴路 500 号企业服务中心 A 座 11 楼开标室

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. 供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起 7 个工作日内，对采购文件需求的以书面形式向采购人一次性提出质疑，对其他内容的以书面形式向采购人和采购代理机构一次性提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

2. 《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》（浙财采监〔2022〕3 号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监〔2021〕22 号）、浙江省财政厅关于进一步加大政府采购支持中小企业力度助力扎实稳住经济的通知》（浙财采监〔2022〕8 号）已分别于 2022 年 1 月 29 日和 2022 年 2 月 1 日和 2022 年 7 月 1 日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

根据《浙江省财政厅关于进一步加大政府采购支持中小企业力度助力扎实稳住经济的通知》（浙财采监〔2022〕8 号）简化对政府采购供应商资格条件的形式审查，供应商书面承诺符合参与政府采购活动资格条件的，不需要再提供财务状况报告、依法缴纳税收和社会保障资金记录、无重大违法记录等证明材料。

3. 根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监〔2021〕22 号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表；鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政务服务网-政府采购投诉处理-在线办理。

4. 其他事项：（1）潜在供应商可在浙江政府采购网（<https://zfcg.czt.zj.gov.cn/>）进行免费注册，具体详见网站供应商注册要求，中标供应商应在合同签订前完成注册并



成为正式注册供应商。否则将无法完成合同签订与付款程序。

(2) 本次招标采取资格后审。

(3) 本招标公告中附件的招标文件仅供阅览使用,潜在供应商应当按照本招标公告规定方式获取招标文件,未按照规定方式获取的招标文件的,对招标文件提起质疑投诉不予受理。

(4) 已成功报名的投标供应商如若不参加本项目的投标,应至少提前 1 个工作日(投标截止时间往前推)以书面的形式(格式可参见附件 a)告知我公司,书面文件扫描件发至我公司邮箱(1687413311@qq.com)。

(5) 为确保招投标活动的公开、公平、公正,切实维护各方合法权益,凡在招标投标、开标评标过程中,受到敲诈、勒索或发现围标串标、虚假投标、恶意竞标等涉黑涉恶线索者,请及时保留相关证据并向有关部门举报。

(6) 企业信用融资:省财政厅、浙江银监局、省金融办制定了《浙江省政府采购支持中小企业信用融资试点办法》浙财采监[2012]13 号),所称的政府采购信用融资,是指银行业金融机构(以下简称银行)以政府采购诚信考核和信用审查为基础,凭借政府采购合同,按优于一般中小企业的贷款利率直接向申请贷款的投标人发放贷款的一种融资方式。投标人可登录浙江政府采购网(<https://zfcg.czt.zj.gov.cn/>)的中小企业信用融资栏目了解相关信息。供应商可以通过浙江政府采购网(<https://zfcg.czt.zj.gov.cn/>)首页的“浙江政采贷”模块进入申请,还可以通过政府采购云平台(<https://www.zcygov.cn/>)首页的“金融服务”模块进入申请。

政府采购金融服务提示:

为扩大政府采购金融服务面,除政采云网上金融服务合作银行外,兰溪市范围增加线下合作银行二家,具体信息如下:

杭州银行金华兰溪支行:

联系人:江昌奇

联系电话:15558679555



邮政储蓄银行兰溪市支行：

联系人：掌丽

联系电话：18357991025（0579-88824616）

七、电子投标事项特别说明

1.本项目实行电子投标，投标供应商应按照本项目招标文件和政府采购云平台的要求编制、加密并递交投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政府采购云平台技术支持热线咨询，联系方式：400-881-7190。

2.投标供应商应在开标前完成 CA 数字证书办理。（办理流程详见政府采购云平台 <https://www.zcygov.cn/>）。完成 CA 数字证书办理预计一周左右，建议各投标供应商抓紧时间办理。

3.投标供应商通过政府采购云平台“电子交易客户端”制作投标文件，电子投标工具请供应商自行前往浙江政府采购网下载并安装。

4.投标供应商将加密的电子版投标文件于投标截止时间前上传到政府采购云平台系统中。

5.具体的投标文件加密上传等操作详见政府采购云平台平台操作指南。

注：建议使用谷歌浏览器，使用其他浏览器可能发生无法解密等未知情况。

6.投标供应商应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标截止时间后送达的投标文件，将被政府采购云平台拒收。

7.本项目允许投标供应商在响应文件提交截止时间前将备份电子投标文件（后缀名为.bfbs，此备份文件为生成电子加密标书时自动生成的文件）密封后，邮寄到金华景鹏工程咨询有限公司，或于投标截止前送到开标地点，逾期送达或未密封将被拒收。



备份文件不强制要求提交，未提供造成项目开评标活动无法进行下去的，投标无效，相关风险由投标供应商自行承担。

8.已成功报名的投标供应商请及时添加工作人员钉钉号(钉钉号: jhjp001),开标现场将在钉钉群进行全程直播。

八、对本次招标提出询问、质疑、投诉，请按以下方式联系

1.采购人信息

名称：兰溪市中医院

地址：兰溪市兰荫北路 108 号

项目联系人（询问）：吴先生

项目联系方式（询问）：15868408976

质疑联系人：陈先生

质疑联系方式：0579-88901033

2.采购代理机构信息

名称：金华景鹏工程咨询有限公司

地址：金华市婺城区九峰街 139 号 4 幢 603 室

项目联系人（询问）：黄浩轩

项目联系方式（询问）：0579-81293312

质疑联系人：陈女士

质疑联系方式：0579-82275376

3.同级政府采购监督管理部门

名称：兰溪市政府采购管理办公室

地址：兰溪市丹溪大道 28 号

联系人：楼影

监督投诉电话：0579-88903775



附件 a:

弃标函

致：金华景鹏工程咨询有限公司

本单位（单位名称）在认真研读兰溪市中医院数据中心系统项目招标文件后，决定放弃本项目投标，不便之处，敬请谅解！

投标供应商名称（公章）：

法定代表人或授权委托人（签字）：

日期：年月日

注：已成功报名的投标供应商如若不参加本项目的投标，应至少提前 1 个工作日（投标截止时间往前推）以书面的形式（格式参见此附件）告知我公司，书面文件扫描件发至我公司邮箱（1687413311@qq.com）。



第二章前附表

序号	名称	内容
1	项目名称	<u>兰溪市中医院数据中心系统项目</u>
2	采购数量及单位	详见第三章招标需求
3	投标报价及费用	1、本项目投标应以人民币报价；2、 <u>代理费参照发改办价格[2003]857号取费标准 45%计取，由中标（成交）供应商支付，由中标供应商支付，结果公告发布后 5 个工作日内支付</u> ；3、不论投标结果如何，投标供应商均应自行承担所有与投标有关的全部费用。
4	现场踏勘	☐ 组织 ☒ 不组织
5	样品	☐ 提供 ☒ 不提供
6	演示	☐ 要求 ☒ 不要求
7	答疑与澄清	投标供应商如认为招标文件表述不清晰、存在歧视性或者其它违法内容的，应当按照采购公告要求以书面形式要求采购人和采购代理机构作出书面解释、澄清。
8	电子投标文件组成	1、资格证明文件；2、技术商务文件；3、价格文件。
9	电子投标文件密封要求	1、投标供应商线上制作投标文件并采用CA数字证书进行电子签章及加密。 2、投标供应商邮寄或现场递交的备份电子投标文件应密封封装，注明投标供应商名称、项目名称、项目编号等，并封口处加盖公章。
10	电子投标文件的递交	1、在开标截止时间前须在政府采购云平台系统里上传加密的电子版投标文件。 2、备份电子投标文件递交的方式为：邮寄或送达。 3、备份电子投标文件，介质可以是U盘或DVD光盘，只允许存储一个文件。 4、当发生加密文件解密异常时，采购代理机构将启用已提交的备份电子投标文件。 5、以下情形视为未提交有效投标文件： （1）仅提交备份电子投标文件的； （2）加密文件解密异常，且提交备份电子投标文件无效的； （3）加密文件解密异常，且提交的备份电子投标文件不明确，存在一个或一个以上备选（替代）备份电子投标文件。



		6、投标供应商递交备份电子投标文件时，如出现下列情况之一的，将被拒收： （1）未按规定密封或标记的投标文件； （2）由于包装不妥，在送交途中严重损坏的； （3）超过规定时间送达的。
11	投标截止时间	2023 年 04 月 11 日 10: 00
12	开标时间及地点	2023 年 04 月 11 日 10: 00 在兰溪市振兴路 500 号企业服务中心 A 座 11 楼开标室。
13	评标办法及评分标准	综合评分法
14	评标结果公示	评标结束后2个工作日内，评标结果公示于浙江政府采购网 (https://zfcg.czt.zj.gov.cn/)；兰溪市公共资源交易专栏 (http://www.lanxi.gov.cn/col/col11229196152/index.html) 等网站
15	中标公告及中标通知书	采购人确定中标供应商之日起2个工作日内，在上述媒体发布中标公告，中标公告期限为1个工作日，在公告中标结果的同时向中标供应商发出中标通知书。
16	政策落实	1、扶持中小企业（监狱企业、残疾人福利性单位）： 根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号），本单位在政府采购活动中应当通过加强采购需求管理，落实预留采购份额，价格评审优惠、优先采购等措施，提高中小企业在政府采购中的份额，支持中小企业发展。项目相关情况如下： （1）项目预算：<u>1280 万元</u>，最高限价 <u>1270 万元</u> （2）项目属性：<u>①货物类</u>（①货物类/②服务类/③工程类） （3）项目对应的中小企业划分标准所属行业：<u>信息传输业</u>（具体根据《中小企业划型标准规定》执行） （备注：现行中小企业划分标准行业包括农、林、牧、渔业，工业，建筑业，批发业，零售业，交通运输业，仓储业，邮政业，住宿业，餐饮业，信息传输业，软件和信息技术服务业，房地产开发经营，物业管理，租赁和商业服务业和其<u>是</u>（是/否）属于预留份额专门面向中小企业采购的项目。 （5）上述第 4 项中确定为“是”的采购项目，预留份额通过（①）措施进行：



	①将采购项目整体或者设置采购包专门面向中小企业采购； ②要求供应商以联合体形式参加采购活动，且联合体中中小企业承担的部分达到___/___(比例)； ③要求获得采购合同的供应商将采购项目中的___(比例)分包给一家或者多家中小企业。 (6)对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对小微企业报价给予___10%___的扣除，用扣除后的价格参加评审。 对于接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的，对联合体或者大中型企业的报价给予___4%___的扣除，用扣除后的价格参加评审。 注：货物和服务项目中未预留份额专门面向中小企业采购的，以及预留份额项目中的非预留部分采购包，采购单位、采购代理机构应结合项目实际，对符合规定的小微企业报价原则上按最高优惠幅度 20%给予扣除，用扣除后的价格参加评审；对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的，采购单位、采购代理机构应结合项目实际，对联合体或者大中型企业的报价原则上按最高优惠幅度 6%给予扣除，用扣除后的价格参加评审。按财库〔2022〕19 号文件规定执行。 专门面向中小企业采购的项目或者标项，不再执行价格评审优惠的扶持政策。 2、节能产品、环境标志产品的强制采购政策 根据财政部、国家发展和改革委员会、生态环境部等部门公布的政府采购节能产品、环境标志产品品目清单的规定，依据品目清单和认证证书实施政府优先采购和强制采购。采购人拟采购的产品属于品目清单范围内的强制采购品目的，投标人提供的产品应具有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，并在响应文件中提供该产品节能产品、环境标志产品认证证书，否则无效。（注：本项目执行最新政府采购节能产品、环境标志产品品目清单。） 3、节能产品、环境标志产品的优先采购政策 根据财政部、国家发展和改革委员会、生态环境部等部门公布的政府采购节能产品、环境标志产品品目清单的规定、依据品目清单和认证证书实施
--	---



		政府优先采购和强制采购。采购人拟采购的产品属于品目清单范围内的优先采购品目的，投标人提供的产品应具有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，并在响应文件中提供该产品节能产品、环境标志产品认证证书，（注：本项目执行最新政府采购节能产品、环境标志产品品目清单。）
17	信用查询	根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》财库[2016]125号的规定： （1）采购人或采购代理机构将对本项目供应商的信用记录进行查询。查询渠道为信用中国网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）； （2）截止时点：提交投标文件（响应文件）截止时间前3年内； （3）查询记录和证据的留存：信用信息查询记录和证据以网页截图等方式留存。 （4）使用规则：被列入失信被执行人、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及其它不符合《中华人民共和国政府采购法》第二十二条规定条件的，其投标将被拒绝。 （5）联合体成员任意一方存在不良信用记录的，视同联合体存在不良信用记录。
18	签订合同	中标通知书发出后20天内。
19	履约保证金	按合同总金额的1%计收，履约保证金以银行转账或银行、保险公司出具的保函等非现金方式提交，履约保证金以银行转账方式提交的在履约完成后无息退还；履约保证金以履约保函方式提交，在履约完成后自动失效。
20	预算总价	人民币1280万元，最高限价1270万元，支付方式：采购人自行支付。
21	付款方式	1、合同生效以及具备实施条件后7个工作日内支付合同金额的40%，余款在项目验收合格后支付。 2. 中标供应商在结算合同价款时需提供正式发票。
22	投标文件有效期	90天。
23	节能产品	☐ 强制采购节能产品 ☒ 优先采购节能产品 ☐ 不适用
24	环境标志产品	☒ 优先采购环境标志产品 ☐ 不适用



25	企业信用融资	浙江省财政厅、浙江银监局、浙江省金融办制定了《浙江省政府采购支持中小企业信用融资试点办法》浙财采监[2012]13号), 所称的政府采购信用融资, 是指银行业金融机构(以下简称银行)以政府采购诚信考核和信用审查为基础, 凭借政府采购合同, 按优于一般中小企业的贷款利率直接向申请贷款的投标人发放贷款的一种融资方式。投标人可登录浙江政府采购网(https://zfcg.czt.zj.gov.cn/)的中小企业信用融资栏目了解相关信息。供应商可以通过浙江政府采购网(https://zfcg.czt.zj.gov.cn/)首页的“浙江政采贷”模块进入申请, 还可以通过政府采购云平台(https://www.zcygov.cn/)首页的“金融服务”模块进入申请。 为扩大政府采购金融服务面, 除政采云网上金融服务合作银行外, 兰溪市范围增加线下合作银行二家, 具体信息如下: 杭州银行金华兰溪支行: 联系人: 江昌奇 联系电话: 15558679555 邮政储蓄银行兰溪市支行: 联系人: 掌丽 联系电话: 18357991025 (0579-88824616)
26	所属行业	本项目所属行业为<u>信息传输业</u>, 根据《中小企业划型标准规定》(工信部联企业[2011]300号)。



第三章招标需求

一、项目编号：jhjp-lxszyy20230310012

二、采购单位名称：兰溪市中医院

三、项目需求及技术要求：

1. 项目采购清单

1、计算单元部分建设需求			
序号	设备名称	数量	单位
1	数据库服务器（HIS）（核心产品）	3	台
2	超融合系统（核心产品）	1	套
3	超融合交换机	4	台
4	光纤交换机	4	台
5	数据库存储（HIS）（核心产品）	2	台
6	pacs 影像存储	1	套
7	Pacs 存储存储网交换机	2	台
8	Pacs 存储业务网交换机	2	台
9	备份存储	1	套
10	容灾平台	1	套
11	容灾互联交换机	1	台
12	虚拟化软件	1	套
2、网络单元部分建设需求			
1	数据中心交换机	2	台
2	外联交换机	2	台
3	带外管理交换机	1	台
4	安全运维区汇聚及管理网核心交换机	4	台
5	智慧医院 SDN 控制平台	1	套
3、统一运维			
序号	设备名称	数量	单位
1	算法平台	1	套
2	统一运维平台	1	套
4、网络安全单元部分建设需求			
序号	设备名称	数量	单位
1	内网防火墙	2	台
2	外网防火墙	2	台
3	漏洞扫描及风险监测	1	台



4	SSL VPN	1	台
5	上网行为管理	2	台
6	日志审计	1	台
7	运维审计	1	台
8	数据库审计	1	台
9	Web 应用防火墙	1	台
10	安全管理中心	1	套
11	流量探针	1	套
12	终端杀毒	1	套
13	数据库安全防护	1	台
5、云桌面			
序号	设备名称	数量	单位
1	终端 1	250	台
2	终端 2	100	台
3	云桌面软件	1	套
4	服务器	6	台
5	显示器	350	个
6	鼠标和键盘	350	套
7	万兆交换机	2	台
8	接入交换机	9	台
6、机房搬迁及售后服务			
1	老院区机房软硬件搬迁	1	批
2	老院区与新院区机房链路	1	条/年
3	中标单位提供 5 年售后服务（首年要求专人驻点服务）	1	项

技术参数要求

一、计算单元部分建设需求

1、数据库服务器（HIS）

指标项	技术要求
服务器外型	2U 机架式，标配原厂导轨
CPU 型号	≥2.9GHz/16 核心/24MB/185W
CPU 实配数量	≥2 颗
内存功能	Advanced ECC、内存在线热备，具备内存主动式检测，用户可验证内存是否经过厂商认证
内存规格	≥512GB DDR4-2933 内存，最大支持 24 根 DDR4 内存，最大容量 3.0TB



硬盘规格	≥2 个 240GB SATA SSD 硬盘, 配置≥8 个 2.5 寸热插拔硬盘槽位, 可扩展至≥30 个 2.5 寸热插拔硬盘槽位。
Raid 卡	≥1 个 SAS Raid 阵列卡, 支持 Raid0/1/10/5/6, 支持 RAID 1 ADM/RAID10 ADM;
	≥2GB 缓存, 支持缓存数据保护, 且后备保护时间不受限制;
PCI I/O 插槽	最多提供≥8 个标准 PCIE3.0 插槽可用, 同时提供阵列卡和网卡扩展
网卡	配置≥2 张双端口 16Gb FC HBA 卡
	配置≥2 张双端口万兆网卡含 4 个光模块
GPU	支持 3 个双宽 GPU
接口	≥5 个 USB3.0 接口, 最高可扩展至 7 个 USB 接口;
冗余电源	2 个≥800w 铂金版热插拔冗余电源, 支持 96%能效比的钛金版电源选件
冗余风扇	热插拔冗余风扇
工作温度	符合 ASHARE A4 标准, 5-45° C 标准工作温度
嵌入式管理	配置≥1Gb 独立的远程管理控制端口, 可选配置前面板独立的 USB 管理端口。
	提供基于嵌入式管理的硬件性能调优功能, 内置 BIOS, 虚拟化最大性能、低延时、关键业务(RAS 特性)、OLTP 等十种以上场景模板。提供原厂技术说明文件
	配置虚拟 KVM 功能, 可实现与操作系统无关的远程对服务器的完全控制, 包括远程的开机、关机、重启、更新 Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作, 提供服务器健康日记、服务器控制台录屏/回放功能, 能够提供电源监控, 支持 3D 图形化的机箱内部温度拓扑图显示, 可支持动态功率封顶。
	支持联合管理功能, 无需软件即可实现多台服务器统一管理功能, 如监控硬件健康状况, 固件升级等。
	提供升级工具, 无需安装代理即可可统一升级同一网络中服务器的固件及驱动程序。
其它安全选项	提供 UEFI 安全启动;
	可配置机箱入侵侦测, 在外部打开机箱时提供报警功能。

2、超融合系统

指标项	技术要求
-----	------



★资源配置	计算资源：
	1、CPU：≥2 颗 Intel（2.1GHz/24 核）CPU
	2、内存：DDR4 RDIMM，单节点≥512 GB，不低于 2933 MHz
	3、硬盘：按容量配置。
	4、4x1Gb，2 块 2x10Gb SFP+网卡（含 SFP+光模块），2*16Gb FC（含光模块）
	5、集群节点数不少于 10 节点，合计可提供不少于 300 个虚拟机，单虚拟机约 6C，16GB 资源。
	存储资源：
	1、全闪盘单节点配置 1.92T SSD≥4 块 2、数据盘配置用 10K SAS 盘，本次数据容量要求做完下述“超融合数据保护”后集群最终存储可用数据容量≥120TB
★部署方式	本次采用双机房双活模式部署，一个机房整体出现故障时，可以由另一个机房的设备提供虚机进行恢复。
▲超融合数据保护	超融合软件采用对存储进行数据保护，要求实配同一集群内任意坏两块数据盘数据不丢失。
超融合管理	要求超融合管理在医院能够统一管理，包括计算、存储资源，不接受界面跳转的方式独立管理
数据本地化	为确保最短 IO 路径和读写延迟并减少网络流量，分布式存储应支持优先将数据写在本地 SSD 磁盘上，并且当虚拟机迁移到任意节点，其数据也迁移到虚拟机所在物理节点
高可用性	支持 HA 功能，当一台物理机发生故障时，相关的虚拟机可以实现在集群之内的其它物理机上重新启动，或者当某些应用发生僵死之时，可以迅速重启服务，保障业务连续性
虚拟机在线迁移	支持在线的虚拟机迁移功能，可以实现虚拟机在集群之内的不同物理节点之间在线迁移，保障业务连续性
数据压缩	提供在线重复数据删除和实时数据压缩功能；
快照和克隆	提供以虚拟机为中心的快照和克隆，具备自动快照管理功能，支持将快照保存在本地或远端；可定制时间间隔自动拍摄快照，最短快照时间间隔不高于 15 分钟



虚拟机隔离性	虚拟机之间可以做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障系统平台的安全性
▲数据容灾保护	本次超融合平台需支持容灾备份功能，当本数据中心机房出现灾难，业务可以在其余数据中心机房上快速拉起。要求实配 100 个虚拟机个数的授权；
横向扩展	通过简单操作自动将新节点加入现有存储集群，实现集群无缝扩展，不中断业务正常运行
远程数据复制	异步数据复制支持时间策略配置站点间流量限制，避免影响系统生产性能
性能数据采集分析	提供整个集群的性能数据，便于进行性能问题诊断和报表
在线升级	在不需关闭业务系统和主机节点的情况下，可以实现在线的软件升级
自动故障切换	提供故障切换能力，当组件自身故障或者需要进行补丁更新时，不影响整个集群正常运行，保证业务连续性
运维易用性	提供集群健康监控、故障分析；提供一键式升级，包括超融合软件、提供在同一界面升级 Hypervisor，在不需关闭业务系统的情况下，可以实现平台软件的在线升级
跨地域的集中式管理	可在同一界面中对分布在不同数据中心或物理位置的多个集群进行统一管理，需同时通过一个界面统一管理计算、存储、虚拟化等资源
智能化运维	管理内容必须包括：支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开关机、重启、更新 Firmware，虚拟 KVM，虚拟软驱，虚拟光驱等操作；可监控、报告及控制处理器、内存及系统级的能耗，允许通过一体化管理控制台实现基于策略的功耗封顶
	通过统一管理软件进行日常维护管理，能看到所有虚拟机磁盘文件 IO 性能和整个集群中 CPU、内存使用情况；可以通过标准 SNMP 接口实现和现有监控系统的整合



3、超融合交换机

指标项	技术要求
▲兼容性	为适配智慧医院网络智简管理要求，要求设备支持本项目 SDN 相关特性，并被控制器统一纳管使用；
性能要求	交换容量 $\geq 4.5\text{Tbps}$ ，包转发率 $\geq 1900\text{Mpps}$ ；以官网所列最低参数为准；
端口要求	实配万兆光口 ≥ 24 ，QSFP+ ≥ 2 ；
扩展要求	支持 ≥ 2 个扩展插槽，可扩展 40G，万兆插卡及安全插卡。提供官网链接及截图证明；
成熟度	为确保用户安全可靠的组网，要求所选产品入网年度 ≥ 3 年，提供工信部入网证明；

4、光纤交换机

指标项	技术要求
系统架构	机架式安装，无拥塞架构设计，所有 FC 端口全线速
端口数量	最大可扩展端口 ≥ 24
端口速率	同时支持 FC 16Gb/s，8Gb/s 和 4Gb/s 速率
互联扩展	可支持多台交换机级联和 Fabric 扩展
实际配置	配置 24 个 FC 端口，满配 16Gb 光模块和光纤线

5、数据库存储

指标项	技术要求
产品要求	投标产品必须为成熟产品，需提供官方 100%系统可用性证明，需提供相关证明材料。
体系结构	多控制器架构，多个控制器之间采用 PCI-E 或 Infiniband 总线点对点全网状直接互联。需提供厂商官网或官网彩页截图证明。配置 2 个存储控制器，双控制器高速缓存$\geq 256\text{GB}$（缓存不包含 SSD 磁盘、PCI-E SSD、闪存、压缩或重删缓存和 NAS 控制器缓存）每个控制器配置 2 颗处理器，单颗 Intel 存储处理器核数≥ 10核，单颗 CPU 频率$\geq 2.2\text{GHz}$。 支持控制器在线升级，可在不更换控制器机框及不搬移硬盘的情况下将控制器升级至同系列存储任意其他控制器型号，实现容量和性能的在线升级，而无需数据迁移。需提供厂商官网或官网彩页截图证明
主机接口	配置 16Gbps FC 主机端口 ≥ 8 个，支持 16Gbps/32Gbps FC，10GbE/25GbE 接口等，最大支持 16 个主机端口。



磁盘配置	★配置企业级 SSD 存储资源冗余后可用容量≥20T
内置智能优化	存储具备收集精确且细粒度的状态数据并将其存储在节点上的数据库中，通过人工智能/机器学习模型可以使用这些信息来计算当前性能压力和预测性能趋势，并参照自身资源使用情况来优化所有进程和任务的优先级，以便在不影响任何现有应用程序和工作负载的情况下让各种任务和程序使用相应级别的资源，从而优化应用的性能。智能优化场景至少包括硬盘重建、硬盘扩容及在线数据迁移三种场景
智能管理运维平台	针对核心数据库及业务的存储，本次需配置业务负载 I/O 检测功能，实现应用负载 I/O 数据块结构检测，清晰展示不同数据块的存储数量，并依据应用负载 I/O 数据块的规律呈现曲线图，I/O 数据块粒度支持 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, 可直观展示应用负载 I/O 的特点、规律及压力，从而为每一个应用业务分配合理的资源。需提供产品管理软件的应用负载 I/O 截图及曲线图截图证明
	配置智能管理运维平台，提供基于机器学习及大数据分析的智能管理运维技术，实时进行容量分析、性能趋势分析和健康状况检查等，并提供可用性预测、自动预警、健康预警和自动生成建议报告；实现端到端的应用分析，精准定位主机及虚拟机到存储之间的瓶颈所在，准确发现故障源并给出处理及修复建议，此功能无容量限制。
自动精简	配置全容量许可精简功能，实现存储空间超分配，精简回收颗粒度≤128KB，后续扩容无需额外购买许可
LUN 数量	存储提供双控 LUN 数量≥65536
数据重构	每 TB 数据重构时间小于 20 分钟，需提供厂商官网或官网彩页截图证明，数据重构时间（需提供第三方权威机构出具的检测报告复印件）
克隆	配置全容量许可的克隆功能，后续扩容无需额外购买许可。
快照	配置全容量许可快照功能，有效预防各种软故障的发生，快照无需预留空间，后续扩容无需额外购买许可
存储双活	支持存储双活功能，在不加额外网关的情况下可以实现和同厂商中端和高端型号存储组成双活阵列，在一台阵列故障以及 RAID 失效等情况下，依然可以实现双活切换而不会中断业务，且双活切换时间不大于 10 秒
VMware VM 性能拓扑功能	配置 VMware VM 性能拓扑功能，可以在存储管理界面下展示基于 VM 的性能拓扑图，在一定时间周期内监控每一个 VM 的 I/O 经过的节点和性能状态，包括存储系统、存储 LUN、主机服务器、DataStore、VMDK 及 VM 等



	环节，当发现性能异常时可快速定位性能问题所在（提供第三方权威机构出具的检测报告复印件）。
操作系统	Windows、Linux、VMware、UNIX（HP-UX、AIX、Solaris 等）

6、Pacs 影像存储

指标项	技术要求
产品组成	提供软硬件一体机产品不接受纯软件+第三方服务器；
▲节点数量	本次配置≥3 个节点，支持节点在线平滑扩展，系统能够自动识别所加入的节点；
CPU	每节点配置≥2 个 10 核 Intel 处理器，主频≥2.1GHz；
内存	每节点配置≥192GB 内存；
★硬盘	每节点配置≥2 块 480GB 企业级 SSD 系统盘，每节点配置≥4 块 1.92TB 企业级 NVMe SSD 硬盘，配置数据盘可用容量≥150T；
接口	单节点配置≥4 个 10GE 以太网接口和≥1 个管理网口，前端业务网络与管理网络物理隔离；
▲数据保护	要求本次采用不低于（4+2）：1 纠删码的可靠性冗余机制进行部署
兼容性	通过 VMware 兼容性认证，提供 VMware 的链接以及官网截图
NAS 协议	兼容 POSIX 标准接口，支持 NFS、CIFS、FTP 共享；
跨协议访问	兼容 SMB2.0、SMB2.1、SMB3.0、NFS3.0、NFS4.0、NFS4.1、NFS4.2 协议，支持 CIFS/NFS 跨协议访问；
鉴权认证	提供鉴权认证功能，包括用户鉴权、匿名鉴权、AD 鉴权、LDAP 认证、CHAP 鉴权；
回收站	支持文件回收站功能，支持文件删除后自动保存一段时间，可以从回收站恢复文件，支持文件过期后自动删除，（需提供第三方权威机构出具的检测报告复印件）；
文件拷贝	支持同一个文件被不同用户通过不同路径访问，通过链接指针瞬间拷贝文件
WORM 技术	配置 WORM 技术，一次写入后禁止删除，有效保障数据安全性，支持手动或自动提交文件为保护状态
负载均衡	将存储服务分担给多台集群内节点，从而提高了业务处理能力，保证了业务的高可靠性
闪存加速	配置 SSD 读写缓存功能，通过 SSD 盘存放热点数据来提升读性能，支持



	日志写加速;
智能负载均衡	支持节点间智能负载均衡功能, 支持轮询方式, 支持按照 CPU 使用率、剩余内存容量、客户端连接数、网络吞吐量、综合负载等多种方式, 实时选择最优的节点用于业务分担;
性能 Qos	支持按照业务设置性能上限, 包括 IOPS/带宽等
多副本	支持多副本保护, 支持 2 到 6 个副本
数据副本数可在线调整	支持存储池的数据副本数可在线配置, 可以更改集群已创建存储池的副本数量
数据重构	支持数据重构 Qos, 可设置不同档位的重构速率, 调整故障重构的优先级;
快照保护	支持快照数据保护, 支持创建只读快照、可写快照、定时快照、一致性组快照;
	支持手动或自动创建快照, 支持快照过期后自动删除, 单个卷最大支持 ≥ 2048 个快照, 支持快照回滚恢复, 支持快照映射到业务主机进行读写;
节点扩展	单一系统支持 ≥ 4096 个节点的横向扩展
管理界面	提供功能全面的中文图形化管理软件, 支持 Web 或其它图形化方式进行远程管理;
管理 HA	支持管理节点 HA 高可用, 管理平台部署于主备两个节点, 主节点故障时, 自动完成主备切换;
系统监测	提供对存储系统各个参数的实时监测, 管理界面内可查看各个存储池的信息, 包括冗余策略、所属硬盘池、数据健康度和状态等, 支持对硬盘容量、硬盘负载、内存占用、CPU 占用的监控;
性能监控	支持存储卷性能监控, 包括 IOPS、带宽、时延、平均 I/O 大小等, 管理界面可查看每个集群、存储池的 IOPS/带宽, 支持保存 ≥ 7 天的性能监控数据;

7、Pacs 存储网交换机

指标项	技术要求
性能要求	交换容量 $\geq 2.49\text{Tbps}$, 包转发率 $\geq 1000\text{Mpps}$;
端口要求	万兆光口 ≥ 46 , QSFP+ ≥ 2 ; 实配 1 根 5 米 50G 堆叠线缆
▲接口扩展	扩展插槽 ≥ 2 , 提供产品图片及官网证明材料。



安全扩展	支持安全 ALL IN ONE 插卡，支持防病毒、LB、IPS 等安全功能，提供官网链接及截图证明。
应急接管	考虑网管故障的应急接管需求，产品选择时倾向选型免费内置应急接管智能网管，一键启动的交换机。可配合接入交换机设备实现整网拓扑可视，实现在网络设备上对整网交换机的统一管理，无需再额外配置网管平台。若无此特性，则本项负偏离。提供官网链接及截图证明；
成熟度	为确保用户安全可靠的组网，要求所选产品入网年度 ≥ 3 年，提供工信部入网证明。

8、Pacs 业务网交换机

指标项	技术要求
▲兼容性	为适配智慧医院网络智简管理要求，要求设备支持本项目 SDN 相关特性，并被控制器统一纳管使用；
性能要求	交换容量 $\geq 4.5\text{Tbps}$ ，包转发率 $\geq 1900\text{Mpps}$ ；以官网所列最低参数为准；
端口要求	实配万兆光口 ≥ 24 ，QSFP+ ≥ 2 ；
扩展要求	支持 ≥ 2 个扩展插槽，可扩展 40G，万兆插卡及安全插卡。提供官网链接及截图证明；
成熟度	为确保用户安全可靠的组网，要求所选产品入网年度 ≥ 3 年，提供工信部入网证明；

9、备份存储扩容

指标项	技术要求
原有存储扩容	适配原有备份一体机增加虚拟机备份模块，虚拟化备份管理软件，提供虚拟化平台的虚拟机备份、恢复，以及虚拟化平台之间的虚机迁移和复制，备份过程中不影响生产系统的正常运行。（包含 100 个虚拟机备份授权）
	备份一体机硬件扩容，包含 5 块 8TB 大容量硬盘，4 根 32GB 内存
	备份一体机硬件及软件维保 5 年技术支持信息共享，在线 FAQ 网站 7*24 可达，针对普适性疑问和故障可以通过查询解决；在服务有效期内，提供 5*8 小时免费热线电话支持（英方公司工作日：9：00-17:30），响应时间：15 分钟内响应；在服务有效期内，提供软件的维护版本（补丁和小版本升级）；维保期内提供 1 年 1 次巡检服务，对备份任务及备份规则进行查验是否正常运行。



10、容灾平台

指标项	技术要求
部署方式	采用无中心服务器部署，支持节点设备热插拔，全 Scale-out 架构，无缝横向扩展，可依据性能与容量的需求按需配置、无缝动态节点扩展，满足业务发展弹性需求。
基本要求	提供全业务环境容灾功能，包括操作系统状态、应用程序和数据的一体化容灾保护，不接受分别对操作系统、应用、数据进行容灾备份方式。
裸机恢复	1. 支持整机一体化快速恢复，无需对恢复对象预安装操作系统、应用配置等，即可实现对系统、数据与应用的一体化整机快速恢复；
	2. 支持磁盘级恢复模式，即按需恢复所需磁盘；
	3. 支持源机恢复；
	4. 支持异机恢复，且对不同品牌不同型号服务器进行恢复时可自动更新驱动；
	5. 提供恢复历史列表，包括但不限于：恢复客户端名称、恢复客户端 IP、源客户端、源客户端 IP、恢复时间点等；
	6. 提供 Linux PE 引导盘和 Windows PE 引导盘，每款 PE 均可支持 Linux 和 Windows 系统恢复；
保护功能	支持统一 Web 界面同时管理多个容灾节点，保护时可将设备分配到其它容灾节点进行保护，接管时可将故障系统接管到其它容灾接管。
容灾能力	主动容灾平台需支持同时保护物理服务器业务、虚拟化平台业务、云平台业务的能力；无需预先安装操作系统和应用软件。当被保护的多个生产系统故障时，主动容灾平台需支持 3-5 分钟快速故障系统的接管；针对生产系统的逻辑故障，支持同时接管到任意时间点的生产系统状态
应急接管	1) 当客户端系统发生故障，服务端（DR0 Server）可在分钟级提供应急接管；
	接管系统和原系统的配置及数据须完全一致，具体包括：系统环境及配置（IP/账户/口令等），程序软件，分区属性，加密环境等；
	同一客户端可生成多个接管系统（无数量限制），每个接管系统均为独立系统，可用于应急保障、测试验证、恢复演练等场景，对接管系统的数据更改并不影响客户端；
	支持接管模式及演练模式。演练模式不联通外部网络，仅供验证数据一



	致性与可用性，以确保数据保护有效性；
	支持多台客户端的同时应急接管；
	支持应急接管时自动识别系统盘
	2)通过产品 WEB 界面，提供应急接管操作，包括但不限于：
	支持按需选择要应急接管的磁盘；
	支持拖动式应急接管时点选择；
	支持 CPU、内存调整；
	支持 IP 替换，无需应急接管后进去操作系统配置；
	支持虚拟网卡增加；
	支持应急接管虚拟机的启动、停止和删除；
	提供远程管理 Console 界面；
	支持应急接管后虚拟机配置修改；
★实配	实配本次项目所需所有授权和相关可用容量不少于 20TB。

11、容灾互联交换机

指标项	技术要求
▲兼容性	为适配智慧医院网络智简管理要求，要求设备支持本项目 SDN 控制器统一纳管使用；
性能要求	交换容量 $\geq 4.5\text{Tbps}$ ，包转发率 $\geq 1900\text{Mpps}$ ；以官网所列最低参数为准；
端口要求	实配万兆光口 ≥ 24 ，QSFP+ ≥ 2 ；（配置 4 个万兆单模模块）
扩展要求	支持 ≥ 2 个扩展插槽，可扩展 40G，万兆插卡及安全插卡。提供官网链接及截图证明；
成熟度	为确保用户安全可靠的组网，要求所选产品入网年度 ≥ 3 年，提供工信部入网证明；
▲分布式网关	为了确保容灾时，生产端和容灾端网关互通，要求采用 SDN 分布式网关部署，确保容灾端和主医院数据中心端网关同步。需提供相关证明材料佐证并加盖原厂公章。

12、虚拟化软件

指标项	技术要求
虚拟化平台	Vmware vSphere7 或以上、含 vCenter 实配 2 个 CPU 的 Vmmware 授权和一个 vCenter 授权



二、网络单元部分建设需求

1、 数据中心交换机

指标项	技术要求
★兼容性	为适配智慧医院网络智简管理要求，要求设备支持本项目 SDN 相关特性，并被控制器统一纳管使用；
性能要求	交换容量 $\geq 4.5\text{Tbps}$ ，转发性能 $\geq 1990\text{Mpps}$ ，以官网所列最低参数为准
冗余性	实配双电源，五风扇框；
▲规格	整机最大路由地址表 $\geq 320\text{K}$ ，整机最大 ARP 地址表 $\geq 270\text{K}$ ，整机最大 MAC 地址表 $\geq 280\text{K}$ ；（需提供第三方权威机构出具的检测报告复印件）
▲接口要求	实配万兆光口 ≥ 24 ，40GE 光接口 ≥ 2 个，100 GE 光接口 ≥ 2 个，实配 5 米堆叠线缆 1 根；满配万兆多模光模块

2、外联交换机

指标项	技术要求
性能要求	交换容量 $\geq 330\text{ Gbps}$ ，包转发率 $\geq 50\text{ Mpps}$ ；以官网所列最低参数为准
▲应急接管	考虑网管故障的应急纳管需求，产品选择时倾向选型免费内置应急接管智能网管，一键启动的交换机。可配合接入交换机设备实现整网拓扑可视，实现在网络设备上对整网交换机的统一管理，无需再额外配置网管平台。若无此特性，则本项负偏离。提供官网链接及截图证明；
接口要求	≥ 24 个 10/100/1000Base-T 自适应以太网端口， ≥ 4 个千兆 SFP 口。

3、带外管理交换机

指标项	技术要求
性能要求	交换容量 $\geq 420\text{ Gbps}$ ，包转发率 $\geq 135\text{ Mpps}$ ；以官网所列最低参数为准
▲应急接管	考虑网管故障的应急纳管需求，产品选择时倾向选型免费内置应急接管智能网管，一键启动的交换机。可配合接入交换机设备实现整网拓扑可视，实现在网络设备上对整网交换机的统一管理，无需再额外配置网管平台。若无此特性，则本项负偏离。提供官网链接及截图证明；
接口要求	≥ 48 个 10/100/1000Base-T 自适应以太网端口， ≥ 4 个万兆 SFP+口。满配万兆多模光模块

4、安全运维区汇聚及管理网核心交换机

指标项	技术要求
性能要求	交换容量 $\geq 750\text{Tbps}$ ，包转发率 $\geq 218\text{Mpps}$ ；以官网所列最低参数为准
接口要求	≥ 24 个 10/100/1000Base-T 自适应以太网端口（其中不少于 5 个 combo



	口), 10 个万兆 SFP+口; 满配万兆多模光模块。
▲应急接管	考虑网管故障的应急纳管需求, 产品选择时倾向选型免费内置应急接管智能网管, 一键启动的交换机。可配合接入交换机设备实现整网拓扑可视, 实现在网络设备上对整网交换机的统一管理, 无需再额外配置网管平台。若无此特性, 则本项负偏离。提供官网链接及截图证明;
NTP 同步	支持 NTP 协议, 可作为数据中心 NTP 时钟同步节点, 满足数据中心内时钟同步需求
成熟度	为确保用户安全可靠的组网, 要求所选产品入网年度 ≥ 3 年, 提供工信部入网证明。

5、智慧医院 SDN 控制平台

指标项	技术要求
部署	支持容器化部署, 支持数据中心、园区等控制器产品部署在同一平台, 节约资源需求。为保证控制器的稳定性和成熟性, 提供软件著作权等权威材料进行证明。
融合架构	保证整个网络运行的统一、连续和完整性, 所有控制系统提供整体安装部署的能力, 对用户需呈现统一的配置入口、监控入口和运营入口, 避免各个功能独立作为软件平台单独部署、维护及对接带来不稳定性;
安全对接	可通过标准云插件方式实现对跨品牌安全设备的纳管, 实现配置自动下发和设备统一管理, 可以和 F5 等主流负载均衡设备对接, 实现对 F5 的负载均衡业务及路由业务的发放。可以和山石、迪普、深信服等主流安全设备对接; 要求提供权威的证明材料。
组网架构	Fabric 支持 Spine-Leaf 的组网架构, 可以灵活适配从 1GE、10GE、25GE、40GE、100GE、400GE 的全系列网络产品;
大二层特性	每张 Fabric 网络存在多个独立的互联边界设备, 通过三段式 VXLAN 方案由控制器自动化下发配置, 组成跨数据中心大二层网络。提供产品功能截图佐证。
服务链	支持构建安全资源池, 定义 SFC 服务链, 进行业务防护的按需防护, 可以有效满足东西向、南北向的防护需求; 安全资源池可以按需由硬件、或者 NFV 形态安全产品组成, 包括 LB、FW;
▲融合角色	因本项目采用服务器交换机与安全交换机融合的模式, 因此需支持 service leaf 和 server leaf 合一, 实施落地时安全资源池与服务器共享



	接入 leaf。（需提供第三方权威机构出具的检测报告复印件）
▲兼容性	数据中心利旧现网核心交换机 2 台，要求 SDN 控制平台可对现网核心交换机 S10508-V 纳管，提供可纳管说明。
▲服务范围	本项目实配虚拟服务节点 2 个,可提供服务链安全服务。实配 SDN 特性交换机授权不少于 8 个，网络设备管理授权不少于 16 个。
平台	资源：CPU≥48 核，主频≥2.1GHz，内存≥512GB，硬盘≥1100GB SSD，2 端口万兆网卡≥2，千兆电口≥4

三、统一运维

1、 算法平台

指标项	技术要求
算法要求	包含子算法：混合行为分析、人员行为分析、明厨亮灶、水利、消防安全、安全出行、城市管理、智慧交通算法包
	通用算法:徘徊检测、剧烈运动（打架斗殴）、人员倒地、攀高检测、区域入侵（时段）、区域入侵（时刻）、人群聚集（医闹）、快速移动（奔跑）、区域离开等
	特殊算法：进出人数统计、火焰识别、区域内人数统计、睡岗检测、玩手机、吸烟、离岗检测、未统一着装、违停检测、物品遗留、物品拿取、未戴口罩、未戴厨师帽、未穿厨师服、老鼠、煤气罐、光膀子、船只、漂浮物、电瓶车入电梯、路面消防通道堵塞、楼内消防通道堵塞、非机动车违停、渣土车识别、骑非机动车未戴头盔、非机动车违规雨棚、非机动车载人、沿街晾晒、垃圾箱满溢、违规撑伞、暴露垃圾、出店经营、井盖异常、横幅识别、违规广告、裸土未覆盖、犬类识别、空调外机低挂、交通拥堵、普通违法停车、占用公交车道、机动车占用非机动车道、实线变道、压实线、货车占道、逆行、倒车、垂钓、浒苔、烟雾、撒小卡片、积水、占道经营、流动摊贩、交通事故检测、非机动车闯红灯。
算力要求	GPU：实配 CP14*2, T4*2
应用能力	可支持视频监控、门禁、报警、电子地图、访客、考勤、巡更、车辆超速违停检测、人车智能检索、系统运维、视频图像质量诊断等应用子系统
纳管能力	支持 IPC 、卡口、NVR、编码器、解码器、网络键盘、报警主机、门禁主机、访客机等设备的接入、管理、配置和查询



管理能力	提供平台组织管理、角色管理、用户管理、权限分配
接入要求	支持 GB/T28181、ONVIF、GA1400 等标准协议的设备接入
接入能力	单设备支持 128 路实时视频流分析，或 512 路图片流分析
结构化	支持多类算法识别分析，支持人员、车辆结构化分析，
扩展能力	支持 3 台或者 3 台以上设备组成云，以集群的方式运行，集群增加服务器，整体接入性能、流媒体转发性能、智能分析性能均有提升
码流接入	支持最大接入码流为 1024Mbps, 最大转发码流为 1024Mbps, 最大回放码流为 1024Mbps
算法仓	支持算法仓功能，支持多种主流厂家算法配置（需提供第三方权威机构出具的检测报告复印件）。
▲能力要求	实配硬盘≥8T，实配通用算法≥80 路，特殊算法 40 路，及配套硬件资源。

2、统一运维平台

指标项	技术要求
基础功能	支持服务器、虚拟机、存储、中间件、操作系统的统一纳管； 平台需具备全面性，必须支持通过 IPMI、SNMP 和 RESTful 协议带外方式对主流厂商服务器进行硬件层面的精细化管理，包括服务器序列号、硬件型号、产品 ID、风扇状态/风速、温度、电源功率/状态/模式、处理器状态/缓存/速度、内存大小/状态/频率、网卡状态相关信息的监控。同时支持服务器硬件系统事件的采集，包括硬件错误事件，并支持将服务器系统事件转换为运维平台的告警信息，必须提供产品功能截图；
虚拟化监控	提供对虚拟化的全面监控，包括 CAS、Hyper-V、VMware、FusionCompute。 对 ESX，Hyper-V 服务器以及其上运行的 VM 的相关性能指标项进行数据采集并监控；
自定义	对同类型监控对象支持按需自定义监控模板，包括采集哪些指标、采集间隔、阈值、告警级别、触发次数，实现灵活高效的个性化监控需求。
地址扫描	支持地址扫描，提供子网中 IP 地址的可用性状态，可以定期对 IP 地址的在线状态进行检查，避免地址冲突。IP 地址分配情况自动统计，必须提供产品功能截图；
▲IP 地址回收	提供 IP 地址回收功能，对于检测到的长期不使用的 IP 地址，系统可以自动或者手动回收。必须提供产品功能截图；
部署方式	本次项目所提供软件平台需满足统一容器底座，支持融合部署，可实现统一界面呈现；



远程运维	含远程运维组件，可通过组件设备实现远程运维方式，即插即用，实现云端专家在现场支持的类似效果。
实际配置	实配 150 个监控授权，必须包含服务器、应用、虚拟机等设备的监控管理；200 个 IP 地址可视化管理授权；

四、网络安全单元部分建设需求

1、内网防火墙

指标项	技术要求
▲硬件要求	2U 机架式设备，至少配置 ≥ 16 个千兆电口， ≥ 5 个千兆光口， ≥ 4 个万兆光口，冗余电源；三层吞吐量 $\geq 20\text{Gbps}$ ；并发连接数 ≥ 500 万，每秒新建连接数（HTTP） ≥ 12 万；开启五年 IPS, AV 特征库升级服务，15 个 SLL VPN 用户授权。
部署模式	产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式；
网络协议	所投产品必须支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能；（提供截图证明）
共享上网检测	所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作（提供截图证明）
入侵防御	所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息；（提供截图证明）
SSL 解密	所投产品必须支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4 和 IPv6 地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计（提供截图证明）
蜜罐策略	所投产品必须支持 IPv4 和 IPv6 流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN 的引流策略，并支持强制引流，能够通过设置服务器和端口进行引流（提供截图证明）
云端协同	所投产品必须支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能（提供截图证明）
产品联动	所投产品必须支持与态势感知系统联动，上报网络活动产生的数据至态势感知系



	统；并支持接收来自态势感知系统推送的处置策略，及时拦截绕过防护措施产生的高级威胁。（提供截图证明）
	所投产品必须支持与终端及服务器杀毒软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。（提供截图证明）

2、 外网防火墙

指标项	技术要求
▲硬件要求	1U 机箱，网络处理能力 $\geq 8\text{Gbps}$ ，并发连接 ≥ 180 万，每秒新建连接 10 万/秒，冗余电源，配置 ≥ 8 个 10/100/1000M 自适应电、2 个 SFP 光接口和 2 个 SFP+光接口, 1 个 Console 口；默认含 25 个 IPsecVPN 并发隧道数（最大 3000）和 25 个 SSLVPN 并发用户数（最大 500）， ≥ 2 个扩展插槽，一块 128G 硬盘；开启五年 IPS, AV 特征库升级服务
部署模式	产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式；
网络协议	所投产品必须支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能；（提供截图证明）
共享上网检测	所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作（提供截图证明）
入侵防御	所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息；（提供截图证明）
SSL 解密	所投产品必须支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4 和 IPv6 地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计（提供截图证明）
蜜罐策略	所投产品必须支持 IPv4 和 IPv6 流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN 的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流（提供截图证明）
云端协同	所投产品必须支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、



	云沙箱、威胁情报云检测等功能（提供截图证明）
产品联动	所投产品必须支持与态势感知系统联动，上报网络活动产生的数据至态势感知系统；并支持接收来自态势感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁。（提供截图证明）
	所投产品必须支持与终端及服务器杀毒软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。（提供截图证明）

3、 漏洞扫描及风险监测

指标项	技术要求
性能要求	任务并发数 ≥ 10 ，单任务并发 IP 数 ≥ 90 ，权可扫描总数量不多于 384 个无限制范围 IP 地址。
硬件要求	▲软硬一体化 1U 标准机架式设备，硬盘容量 2TB*1，内存 16GB，支持 1 个扩展插槽，2*USB 口，单电源，网络接口：管理口 ≥ 1 个*RJ45 串口、千兆电口 ≥ 6 个，USB 口 ≥ 2 个。
总体要求	支持用户自定义系统名称、版权信息和系统的 Logo 信息，而无需进行定制化。（提供截图证明）
	漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容。（提供截图证明）
系统漏扫功能要求	▲厂商漏洞特征库大于 200000 条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与 CVE、CNNVD、Bugtraq、CNCVE、CNVD 等国际、国内漏洞库标准兼容。（提供截图证明）
	提供采用 SMB、SSH、Telnet、RDP、SNMP 等协议对 Windows、Linux 系统进行登录授权扫描。
	具备弱口令扫描功能，支持弱口令扫描协议数量 ≥ 22 种，包括 FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP 等协议进行弱口令扫描，允许用户自定义用户、密码字典。（提供截图证明）
网站漏扫功能要求	产品提供 Web 应用漏洞扫描功能，支持对 Discuz、大汉 CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2 等国内外常见第三方组件进行扫描。
	漏洞特征库大于 8500 条，漏洞评分支持 CVSS3.0 标准。
	支持将漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级。（提供截图证明）



	支持自定义 User-Agent、自定义请求头，自定义 Cookies 或录制获取、自定义 LocalStorage、SessionStorage 对 Web 应用进行扫描。
	支持获取整个网站目录结构，并能导出所爬行到的 URL。
	存在误报漏洞可通过产品在扫描结果处支持以即时通讯的方式第一时间反馈给厂商协助修改。（提供截图证明）
	支持对 Struts2 远程命令执行漏洞进行命令执行和文件上传的渗透测试验证操作。（提供截图证明）
策略管理	支持自定义扫描策略模板，可以将自定义策略模板导出备份，也可以导入备份的策略模板，能够对策略模板进行编辑、另存为新的模板。
用户管理	提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。
	▲支持对用户有效期进行详细设置，可以设置不限制，也可以设置每天的哪个时段、每周的周几至周几、每月几号至几号才能正常使用。（提供截图证明）

4、 SSL VPN

指标项	技术参数
▲硬件规格	VPN 专用硬件平台，1U 机箱，单电源，≥6*10/100/1000 电口，最大支持 300 用户，含 300 个 SSL 授权。
IPv6 支持	双机能够在 IPv6 环境下进行 HA 组网工作，浮动 IP 地址支持 IPv6。（要求提供截图）
基本功能	支持预防' syn flood' 攻击，忽略 icmp 回显请求（不能被 ping）。（要求提供配置截图）
	支持虚拟门户功能，能够按照不同的用户组来定义不同的虚拟门户，不同的虚拟门户登录界面、访问地址均可以不同。用户通过不同 URL 登入会获取不同的登入界面，并且每个登入界面可定制。（要求提供配置截图）
	支持基于用户、用户组分配虚拟 IP，并且支持虚拟 IP 绑定功能。（要求提供配置截图）
	支持对基于 TCP、UDP、ICMP 的所有 B/S、C/S 应用系统的支持，例如视频、oa 系统、Transroute 等。
	支持自动跳转功能，用户登录后自动弹出默认的应用界面。可自定义应用图标，可自行设置智能终端应用图标、PC 端应用图标（提供配置截图）
	支持智能终端访问的业务和 PC 端访问的业务分离，可自主设置具体应用仅允许 PC 访问或者仅允许智能终端访问。（提供配置界面截图）



	支持流量控制功能，可以对组设置流量控制策略，策略中包括：组、服务信息，可以选择多个组，多个服务，流量大小，周期类型包含：天，周，月。 (要求提供配置截图)
管理员功能	管理员可分为状态管理员，系统配置管理员，VPN 管理员，应用安全管理员，防火墙管理员，日志管理员，系统维护管理员，创建管理员可以为其分配相应的管理员权限。(要求提供配置截图)
	支持组管理员，组管理员由系统管理员设定。组管理员可以进到配置端查看组信息，可以基于此组建立第二级的子组，可选择用户，选择主机绑定策略；设置终端安全策略；设置隧道控制策略；设置访问控制策略。(要求提供配置截图)
认证功能	支持网关能够支持证书透传功能，即将证书直接传递给业务系统，可以根据证书中的 O、OU、CN 作为访问控制项，提供用户对某个业务系统的访问控制权限。(要求提供配置截图)
	支持自带 CA 认证中心，可签发证书，注销证书，支持本地证书批量转换成证书用户，实现用户名密码+证书双因子认证，这样以方便签发证书；支持与第三方 CA 中心结合认证，能支持第三方 CA 的证书格式：der、base64 编码的 crt、cer、p7b、p12、pfx 方式，支持第三方的 CRL。(要求提供配置截图)
日志及监控	能显示在线用户列表，并能把在线用户以列表形式导出，可以导出为 txt、HTML 文件。(要求提供配置截图)
	支持显示各模块日志信息，可以用柱型图比较系统日志等级的数量，可以查看用户登录日志和资源访问日志，用户日志可以按照年、月、日、类型查询。 (要求提供配置截图)
	支持 CPU 告警、支持内存告警、支持用户授权数告警、支持管理员账号登陆锁定告警、支持用户账号登陆锁定告警，告警方式为邮件、短信、邮件和短信。 (要求提供配置截图)
	支持虚拟服务用户在线人数显示，支持虚拟服务连接数在线统计；可以记录虚拟服务的访问日志，接口配置虚拟服务地址池满足业务负载均衡要求。(要求提供配置截图)
移动安全	设备可支持远程应用发布功能，发布 C/S 应用客户端界面而非整个桌面进行发布：只传输鼠标、键盘操作和显示数据，无需安装客户端即可支持 C/S 模式软件系统的远程使用；SSL VPN 不限制远程应用发布的服务器并发 (要求



	提供配置截图)
	IOS、android 客户端登陆必须支持用户名+密码+动态口令、用户名+密码+数据库认证、用户名+密码+短信认证等双因子认证方式(要求提供配置截图)
	支持移动应用封装功能, 客户上传移动应用 APP 进行封装、加固(要求提供截图)
	支持移动 app 工作区数据擦除以及设备整体数据擦除, 防止智能终端丢失后造成数据泄密(要求提供截图)
	对接入的智能终端可手动设置其状态“禁止”或启动(要求提供截图)

5、 上网行为管理

指标项	技术参数
★设备规格	新建连接数为 ≥ 15000 个/秒; 1 U 硬件, 标配 6 个千兆电接口(其中含 1 个管理接口和 1 个 HA 接口), 1TB 硬盘
多核处理	采用国际先进的多核处理器硬件架构及多核并行处理系统(提供多核并行处理办法相关的专利证明)
管理口	设备必须具备独立的(具备标识的)网络管理接口。所有接业务接口均被用满后, 仍然可以存在独立的管理口可以访问设备
硬件 Bypass 按钮	设备必须提供物理硬件 bypass 按钮, 便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。(提供设备照片)
界面 Bypass	支持远程登录在界面实现 Bypass, 并可进行切换。(提供截图证明)
网桥模式	设备可直路串联在一条或多条原有网络线路上, 进行行为分析、审计和控制。不改变网络拓扑, 路由表项。
Portal 模式	支持设备模式选择, 可以设置为 Portal 模式实现 Portal 服务器功能;(必须提供配置界面截图)
高可用性	支持多台设备主主模式部署(提供截图证明)
IPv6 支持	能够支持 IPv6 环境下的网址访问审计、生成分析报表等功能; 能够在 IPv6 环境下, 正确审计显示用户的 IPv6 地址
支持对恶意 URL 的云查杀	支持基于云端大数据安全平台, 对恶意 URL 访问进行封堵和记录日志。 支持恶意 URL 访问日志查询, 日志应包含时间/用户/终端类型/内外网 IP 地址和端口号/MAC/网址/网站类型/访问控制类型。(提供上述功能截图证明)



支持失陷主机检测	支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志。（提供功能截图证明）
	支持通过恶意软件特征检测方式识别失陷主机并记录日志（提供功能截图证明）
SOC 联动	支持接收来自 SOC 运营管理平台的指令（（提供功能截图证明））
应用审计及控制	应用协议库包含的应用数量不低于 6000 种，应用规则总数不低于 10000 种（提供网管链接）
URL 分类反馈	当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈；（必须提供配置界面截图）
阻塞提示	不同网页被阻塞后会跳转不同的阻塞页面，支持用户完全自定义；（提供功能截图）
网盘 PC 客户端文件审计	支持对 Windows 百度网盘客户端的文件标题和内容审计（（提供功能截图证明））
外发关键字过滤	支持对 QQ、微信和百度网盘的 PC 客户端外发文件进行关键字过滤和封堵（（提供功能截图证明））
软件联动	支持在安装终端管理软件时，不再需要安装客户端即可审计 IM 聊天内容
数据库审计控制	可审计、控制 Oracle, MySql, SqlServer, PostgreSQL 等数据库的访问与操作，包括添加、删除、修改、查询等。（（提供上述功能截图证明））
DNS 审计	通过 DNS 审计策略对 DNS 通信内容进行审计和控制（（提供功能截图证明））
多级虚拟通道	支持多级虚拟通道，可以将物理带宽分成至少 7 级虚拟通道，合理分配物理带宽资源
流控策略	支持基于用户、时间、应用、源 IP、目的 IP 和服务创建流量控制策略
终端管理软件联动	能够与终端管理软件联动，设备检测到未安装终端管理软件的 PC，可将其 Web 访问自动重定向到特定页面并提示下载；（提供上述功能截图证明）
用户识别	支持对 802.1X、华为 controller、Kerberos、AD、POP3、Radius、数据库识别、PPPOE、华三 iMC、城市热点、深澜计费等系统的单点登录。（提供上述功能截图证明）
日志 FTP 导出	支持通过 FTP 和 SFTP 方式将日志导出到指定服务器，日志支持 SSL 加密和 ZIP 压缩，支持自定义导出数据的时间段和数据定时上传的频率。支持定义导出日志数据的范围、用户、位置和工具。
支持三权制	支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免



衡管理机制	超级管理员权限过大的弊端。系统管理员和审计员的账号创建，权限变更需要审核员审批才能生效。管理员和审计员的操作会形成日志受审核员监督。（提供审核员审批操作截图）
-------	---

6、 日志审计

指标项	技术参数
性能要求	▲支持≥240 个日志源；日志处理能力 EPS：≥9000/秒（峰值：≥12000/秒）
硬件要求	▲标准 2U 硬件，网口：≥10 个工作管理口（1 管理口+1HA 口+8 个千兆电口，8 个千兆光口（配 2 个多模 SFP 光纤模块）），1 个 console 口 内存：≥32GB；磁盘：≥2T*2 raid1（支持 raid1：只能是偶数、raid5：大于等于 3 块盘）；双电源；
功能扩展	采用解决方案包上传对产品进行功能扩展，无需代码开发。提供截图证明 支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器。
日志收集	支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP 协议日志收集；支持阿里云 SLS 日志的采集。 支持使用代理（Agent）方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。 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。提供截图证明 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等。 支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等。
日志分析	可以基于日志等级进行过滤 可以通过自定义配置过滤掉用户不关心的日志 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），解析维度多达 200+，解析规则可以根据客户要求定制扩展，提供截图证明 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（提供截图证明） 进行关联分析的规则可定制 支持关联规则性能以界面列表形式显示，可了解触发次数、最近一周监控状态等信息（提供截图证明）；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（ 需提供第三方权威机构出具的检测报告复印件 ）。
应用性能 监控	支持监控设备自身 CPU、内存、磁盘等工作运行状况
	通过在目标主机上安装 Agent 程序，支持监测目标主机的 CPU 利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息（ 需提供第三方权威机构出具的检测报告复印件 ）；
报表管理	内置合规性报表 1000+种，内置 SOX、ISO27001、WEB 安全等解决方案包，内置完善的等级保护合规报表
用户管理	根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理
	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（提供截图证明）；
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（提供截图证明）；

7、 运维审计

指标项	技术参数
性能要求	▲授权资产：≥500 个；硬件性能：并发字符连接≥500 个，并发图形连接≥100 个
硬件要求	▲机箱高度：2U；标配网口：≥2 千兆电口管理口，千兆业务电口≥4，千兆业务光口≥4（含 2 个千兆 SFP 多模光模块）；硬盘容量：≥2T*2，RAID 1 内存：≥8G；USB 口：USB2.0 口*2；串口：RJ45 口*1；电源：1+1 热插拔冗余电源
单点登录认证	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。（需提供相关截图证明）
短信口令认证对接	支持与 Get、Post、Soap 发送方式的 HTTP 短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud 联动。（需提供相关截图证明）
双因子认证	堡垒机须内嵌动态令牌和 USBkey 认证引擎，可使用动态令牌或 USBkey 进行双因子认证。（需提供相关授权和资质复印件）
密码存储	支持采用国密加密算法进行核心敏感数据加密存储，且支持使用软件/硬件方式加密；（需提供相关截图证明）
兼容客户端类型	单点登录支持调用多种本地客户端工具：字符：xshell、secureCRT、putty，图形：mstsc、realvnc，文件传输：secureEX、flashFXP、filezilla、winscp，数据库：ssms、sqlwb、mysqlworkbench、mysql、dbvisualizer、plsql、sqlplus、toad、db2cmd、quest central、navicat，无需应用发布服务器（需提供相关截图证明）



URL 访问管控	支持对 HTTP/HTTPS 类资产进行 URL 黑白名单限制，禁止在未授权情况下，通过手动输入 URL 跳转至其它 web 网站。
数据库兼容性	标准支持 DB2、oracle、mysql、sqlserver、PG、人大金仓、达梦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、workbench、mysql、DbVisualizer、plsql、sqlplus、toad、dbcmd、Quest Central、pgadmin3、psql、ksql、Isql、Disql、DMmanger、navicat 等），无需应用发布前置机（需提供相关截图证明）
MAC 兼容性	支持在 Mac 操作系统下调用 navicat 工具运维 mysql、oracle 等数据库资产（需提供相关截图证明）
数据库命令管控	数据库支持命令阻断功能，精确到数据库，表、字段级别（需提供相关截图证明）
数据库双重审计	支持同时对数据库会话记录图形审计及命令提取；支持对数据库运维会话的上行和下行命令进行审计。（需提供相关截图证明）
专用客户端运维	支持 Windows/macOS 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）
SSH 网关代理直连	支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备。（需提供相关截图证明）
SSH-agent-forwarding	可以使用 SSH-agent-forwarding 登录到 SSH 服务器，用于登录堡垒机和登录 SSH 主机使用相同私钥的场景。
禁审功能	支持提供禁止审计功能，可对部分设定策略的会话不审计录像，防止机密信息二次泄漏。（需提供相关截图证明）
命令审批	支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令（ 需提供第三方权威机构出具的检测报告复印件 ）。
国密 TLS 单向通信	支持国密 TLS 单向认证通信，使用国密算法保证 HTTPS 协议层面的数据机密性和完整性；开启后需使用支持国密算法的浏览器才能访问堡垒机（需提供相关截图证明）
配置备份	系统配置文件支持自动备份到 FTP/SFTP 服务器上，支持配置备份周期。
存储管理	支持 NAS/CIFS 存储（需提供相关截图证明）
API 接口	▲需提供用户、资产、授权的增删改查等 API 接口，允许第三方平台调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量。（需提供相关截图证明）



跨地域部署	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。
身份鉴别	支持使用基于国密算法的动态令牌、国密 USBkey 对堡垒机的登录实行双因素认证。以满足对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性。针对国密动态令牌、国密 USBkey 提供国家密码局颁发《商用密码产品认证证书》



8、数据库审计

指标项	技术参数
性能指标	▲支持的数据库实例个数：6；审计性能：峰值 SQL 处理能力≥ 10000 条/秒；硬件最大吞吐量 1000Mbps；双向审计数据库流量 100Mbps；标配日志存储数 10 亿条；审计日志检索能力≥ 1500 万条/秒。2U 机架式；内置交流双电源；产品采用专用工控机硬件架构，非普通 PC 服务器，MTBF(平均故障间隔时间)≥ 65000 小时；处理器采用 Intel 高性能 CPU，内存$\geq 2*8GB$，硬盘$\geq 2TB(2T*1)$；网络端口：配备至少 2 个千兆电口管理口（admin 口 1 个、HA 口 1 个）；支持千兆网络环境下的监听能力；标配至少 4 个千兆电口。
部署方式	▲支持分布式部署，管理中心可实现统一配置、一键批量升级所有节点、统一报表生成、统一查询；（需提供功能截图）
协议支持	支持 Oracle（包括 21C 及其他版本）、MySQL、SQL Server、Sybase ASE、DB2、Informix、Cache、PostgreSQL（14 及其他版本）、Teradata、MariaDB、Hana、LibrA、Sybase IQ、TiDB、Vertica、PolarDB、PolarDB-X 等主流数据库的审计；
	支持达梦（DM8 及其他版本）、南大通用（GBase）、高斯（GaussDB）、人大金仓（KingbaseV8、V7 及其他版本）、K-DB、神舟通用（Oscar）、OceanBase 等国产数据库的审计；（需提供功能截图）
	支持 MongoDB、HBase、Hive、Redis、Elasticsearch、Cassandra、HDFS、Impala、Graphbase、Greenplum、Spark SQL、SSDB、ArangoDB、Neo4j、OrientDB 等数据库的审计；（需提供功能截图）
	支持主流业务协议 HTTP、Telnet、FTP 的审计；
	可以通过导入证书的方式实现 SQL Server 2005 及其他版本采用了加密协议通讯的审计；（需提供功能截图）
	可以通过导入证书的方式实现 MySQL 5.7 及其他版本采用了加密协议通讯的审计；（需提供功能截图）
	支持对各种协议自动识别编码及在 web 界面手工配置特定编码如 GB13000、UTF-8、UTF-16 等；（需提供功能截图）
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；（需提供功能截图）
	审计信息能够记录执行时长、影响行数、执行结果描述、返回结果集，提供功能截图，提供功能截图（需提供第三方权威机构出具的检测报告复印件）；



	支持跨语句、跨多包的绑定变量名及绑定变量值审计；
	支持本地直连数据库场景下的审计，通过本地 Agent 捕获本地数据库客户端程序中实际响应的 SQL 指令，实现对本地运维人员的数据库操作行为的审计，支持主流数据库如 Oracle、PostgreSQL、MySQL、SQL Server 等；（需提供功能截图）
安全审计	支持审计记录中敏感数据的脱敏处理，内置常见敏感数据脱敏规则，并支持脱敏规则自定义；
	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，要求提供产品功能截图（ 提供第三方权威机构出具的检测报告复印件 ）；
	内置安全规则不少于 900 条，如 SQL 注入、缓冲区溢出等；
	可自定义审计规则，审计规则至少支持 18 个条件；（需提供功能截图）
	规则各条件之间支持与或非逻辑关系；（需提供功能截图）
	支持安全规则优先级设置，在匹配规则时支持按照优先级顺序进行匹配并返回唯一匹配结果；
	支持内置安全规则通过规则包进行单独升级，需提供产品功能截图（ 需提供第三方权威机构出具的检测报告复印件 ）；
查询分析	为保障高效的查询性能，要求产品后台采用全文检索引擎检索，具体体现为：可通过检索报文进行审计记录的查询；
	历史会话中的审计记录支持直接导出，支持通过“查询分析”按钮跳转至审计日志页面进行进一步的分析筛选；（需提供功能截图）
Agent 管理	支持在页面批量安装、配置、删除、挂起、唤醒、启动、停止、升级、回退所有的 Agent；
	支持在审计页面直接升级或回退已安装在数据库服务器上的 Agent，显示相应的升级/回退进度和结果，且升级或回退不需要输入数据库服务器的账号、密码；（需提供功能截图）
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，需提供功能截图并盖原厂公章，（ 提供第三方权威机构出具的检测报告复印件 ）；
易用性	支持对 SQL 语句进行业务化翻译，为用户提供 SQL 语句概述，便于用户理解；
	支持在日志页面一键取证；（需提供功能截图）
可维护性	内置一键检测功能，可检测设备状态，包括流量、服务状态、设备状态、配



	置、许可和日志等；
	内置运维终端，可实现日志查看与下载、监控日志、设备状态检测、查看系统资源使用、查看共享内存使用、查看 Kapa 消费情况、执行 SQL 语句、执行常用命令、特权运维等；（需提供功能截图）
防统方相关功能项	▲产品需要有医疗防统方专版，且支持与通用版本的切换；内置的 HIS 系统厂商信息包括方正国际、天津天健、东联、联众、创业、军卫、联想、金仕达卫宁、东软、东华等；支持通过 IP 地址关联人员的工号、姓名、手机、科室、房间、主机名、Mac 地址等信息；首页支持通过曲线图方式直观展示每小时统方告警数量，支持首页显示统方告警名称的 TOP5 和 BOTTOM5；（需提供功能截图）

9、Web 应用防火墙

指标项	技术要求
▲ 硬件规格	网络吞吐量≥1Gbps，应用层处理能力≥500Mbps，网络并发连接数≥65 万，HTTP 并发≥24 万，HTTP 新建连接数≥5000/s。标准 1U 机箱，1TB 硬盘，冗余电源，标准配置千兆 6 个 10/100/1000M 自适应电口，1 个 Console 口。提供五年 WAF 软件特征库服务。
部署模式	产品具备串联和旁路部署方式，串联部署方式支持透明在线部署，不改变网络或网站配置，无需配置 IP 地址，实现即插即用 产品具备旁路部署对镜像流量分析的同时实现阻断功能，产品具备专门的阻断接口设置和对端 MAC 地址设置功能（提供相应截图证明）
网络自适应	产品具备支持 IPv4 和 IPv6 双协议栈流量过滤 产品具备对 HTTP、HTTPS 协议的代理网关功能，支持透明代理、反向代理、负载均衡等模式 产品具备代理模式对 HTTP、HTTPS 协议的单个连接允许请求数、长连接有效时间、最大空闲连接数和上传文件最大值等数据进行自定义配置
Web 安全	产品具备协议合规检测，可根据实际网络状况自定义协议参数合规标准，过滤非法数据 产品具备 SQL 注入、XSS 跨站攻击防御策略，支持特征检测与语义算法检测 产品具备识别和阻断注入攻击，包括命令注入攻击，XPath 注入防护，XML 注入防护，SSI 注入防护，JSON 注入防护，LDAP 注入防护 产品具备 Web 业务控制防御功能，提供针对爬虫、黑链、内网代理以及盗链的防护功能（提供相应截图证明）



	产品具备防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值与动态令牌组合的三种方式实现暴力破解防护
	产品具备 Web 业务加固防御功能，提供人机识别、弱密码检测、会话安全、CGI 安全、跨站请求伪造以及业务流程控制的防御功能
威胁情报中心	产品具备支持威胁情报中心联动功能，基于 FTP 或 FTPS 协议登录云端获取数据来源
	产品具备对威胁情报中心提供的相关数据运用到产品防御策略中，提供基于僵尸网络、恶意 IP、扫描探测、Webshell、代理 IP、漏洞利用、暴力破解、恶意代码以及木马蠕虫等情报类型（提供相应截图证明）
蜜罐防御	产品具备轻量级蜜罐防御功能，提供伪造的后台管理系统页面防御功能（提供相应截图证明）
虚拟补丁	产品具备虚拟补丁功能，支持导入 Appscan 和 SecVSS scan 扫描器的扫描结果生成 WAF 的规则，对此类网站漏洞直接防护
智能封禁	产品具备智能封禁功能，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间
外联检测	产品具备非法 URL 外联检测功能，针对特定外联 URL 进行监控或阻断，并且支持自定义 URL 地址
机器学习	产品具备机器学习引擎，针对业务建模，可通过学习 URL、host 等信息展示网站结构树形图，并支持对 URL 的访问量和响应健康度进行图形化统计
	产品具备设定最少学习样本数，学习时间段等信息，当样本数大于设定的阈值数，可直接进入防护状态
DDoS	产品具备智能分析 DDOS 防护，内置五个防护等级，并可自定义防护等级
	产品具备检测并抵御 IP，TCP，UDP，ICMP，DNS，HTTP 协议的 20 多种 DDoS 攻击类型
入侵防御	产品具备入侵防御功能，并提供入侵防御特征库，特征库需要提供 22 种类型并提供至少 13000 条入侵特征库
	产品具备检测恶意活动，包括恶意 SSL 证书、钓鱼攻击、非法获取权限，重定向攻击，拒绝服务等
	产品具备检测漏洞后门类攻击，包括漏洞利用、后门攻击、文件包含、缓冲溢出、目录遍历，shellcode 等
	产品具备检测僵木蠕类攻击，包括木马、蠕虫病毒、僵尸网络等（提供相应截图证明）
网页防篡改	产品具备支持 windows、linux 的 32 位与 64 位操作系统的网页防篡改功能，并提供相应的客户端下载功能（提供相应截图证明）



实时态势展示	产品具备安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP 并发请求及实时事件统计（提供相应截图证明）
统一管理	产品具备通过集中管理平台进行状态集中监控、配置集中管理、日志集中分析功能
移动端管控	产品具备移动终端管理功能，不需要安装 APP 和第三方插件，通过手机浏览器即可管理设备，并可查看设备 CPU、内存使用情况（提供相应截图证明） 产品具备移动终端对设备的一键管控功能，提供网站一键下线的终端应急措施（提供相应截图证明）
运维工具	产品具备界面诊断工具功能，支持在线抓包、ping、traceroute 等运维工具

指标项	技术要求
▲硬件规格	服务器配置要求：2 颗 12 核 CPU 主频 2.20GHz 以上，内存≥256GB，硬盘 1：2 块 960G SSD 固态硬盘组成 Raid 1 硬盘 2：12*4TB 企业级 SATA 3.5 寸硬盘，总容量 48T；
数据采集与存储	1、支持接入并管理日志采集器、流量采集器，可支持第三方采集器接入（提供相关功能的界面截图）； 2、支持对网络设备、安全设备、服务器、应用等日志进行解析、范式化、预处理； 3、支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、agent 等采集方式； 4、支持文件导入的方式导入日志数据，支持的文件类型至少包含 csv、.log、txt； 5、日志接入支持界面交互式配置，通过图形化界面配置日志解析条件，利用正则表达式、分隔符、Key-Value、JSON 等方法定义解析规则，系统自动生成解析规则，无需通过代码编写解析规则（提供相关功能的界面截图）； 6、▲支持自定义日志类型功能，支持对日志类型名称、存储方式、存储时间、分区方式、重要度等基础属性信息进行配置，达到分类存储日志的目的；（提供相关功能的界面截图）
资产管理	1、支持主机资产和网站资产管理功能，并分别提供不同管理模块，支持主机资产和网站资产的关联管理。主机资产的类型包括但不限于 IOT 设备、服务器、工作主机、网络设备、安全设备、终端安全管理、数据库服务器、中间件服务器、存储设备、应用服务器、安全域、虚拟化设备；支持对主机资产的服务信息进行管理，服务信息应包括：IP 地址、端口、协议、服务名、服务版本和 Banner；支持对 IPV6 资产的管理，支持对资产分类、资产属性进行自定义扩展。（提供相关功能的界面截图）； 2、▲支持和同品牌的资产探查设备、服务器管理系统、网络流量探针、终端管理系统、网站监测系统、云安全管理平台进行协同对接，同步资产信息，支持对发现资产的方式



	的优先级、资产更新策略进行配置。（提供相关功能的界面截图）
威胁预警	1、支持对重大网络安全事件（如永恒之蓝）进行威胁预警，通过厂商对重大网络安全事件的追踪生成预警包，通过预警包导入完成网络安全事件的影响面评估，并持续的跟进事态的发展，快速完成重大网络安全事件的预警及处置； 2、针对此类风险支持统计潜在风险资产数、受攻击资产数、失陷资产数以及资产的日同比及周同比对比。支持影响面趋势视图统计分析。支持基于网段潜在风险资产数、受攻击资产数、失陷资产数责任人等影响面分布。 3、▲支持根据风险资产数量统计自定义关键点节点条件，比如大面积爆发、有效控制、威胁缓解等。支持事态扩散过程发展趋势图的展示及详细告警列表及告警信息展示。（提供相关功能的界面截图）
脆弱性管理	1、系统至少支持绿盟、启明、网神、天融信、Tenable 五款漏扫报告的解析识别和导入管理，支持人工漏洞报告导入，使用模板进行漏洞信息的导入； 2、支持对绿盟、启明、网神、Tenable 中至少两款主流扫描设备进行漏洞扫描任务调度和弱口令扫描任务调度，支持对绿盟、启明、网神、盛华安至少三款第三方配置核查扫描报告及人工配置核查报告的解析识别和导入管理； 3、支持通过网络流量同步漏洞、弱口令信息；支持和同品牌的服务器管理系统、终端管理系统、云安全管理平台协同对接，同步漏洞信息；支持直接同步绿盟漏扫设备的漏扫任务及扫描结果；支持直接同步盛华安配置核查系统的配置核查扫描任务和扫描结果。 4、漏洞信息、弱口令、配置核查可直接调用工单系统，漏洞信息可直接添加到调查任务，支持添加到已有任务或创建新的调查任务；（提供相关功能的界面截图）；
告警分析	支持从告警名称、攻击者、失陷情报、挖矿木马、勒索软件的 5 个维度快速筛选告警并归并，支持按照 5 个维度分别提供单独的可视化数据展示模块，包括展示攻击/告警分布趋势、处置建议、归并告警列表等信息，保证展示内容的实用性从而提高分析处置效率。（提供相关功能的界面截图）
场景分析	账号安全分析场景应包含异地账号登陆、暴力破解、弱口令检测、明文密码泄露、VPN 账号登录行为统计场景；邮件安全分析场景包含邮件威胁分析、敏感关键词邮件列表、敏感后缀邮件列表；（提供相关功能的界面截图）
事件调查	支持通过创建事件调查任务对威胁事件和可疑事件进行调查分析，调查任务中可添加的证据数据包括：日志、告警、漏洞、弱口令、配置核查、文本；支持对以攻击者和受害者情况视角对调查任务中的数据做统计分析；支持调查结果的图形化展示；（提供相关功能的界面截图）



实体分析	支持以 IP 地址、域名作为实体的快速分析能力。 对于外部 IP 分析，支持集中展示该 IP 相关的威胁趋势、攻击阶段、威胁分类、威胁关联情况等数据以及该 IP 对资产的登录分析等。（提供相关功能的界面截图） 对于内部 IP 分析，支持集中展示该 IP 相关的威胁信息、脆弱性信息、暴露面、登录分析、外连分析数据等。（提供相关功能的界面截图） 对于域名分析，支持集中展示该域名相关的鉴定结果、威胁情报信息、访问源统计、解析结果、首次出现时间、访问趋势等。（提供相关功能的界面截图）
工单响应	▲支持通过工单形式通知告警、漏洞、弱口令及配置核查，通知方式包括邮件、短信、企业微信、钉钉、蓝信；工单包含待下发、待处置、处置中、已处置、已完成、已撤销状态吗，支持对工单状态的跟踪；支持对工单 SLA 要求进行设置，SLA 超期支持通知提醒；支持多人协同的工单跟踪处理方式；工单流转中支持添加附件。提供相关功能的界面截图）
联动处置	支持与第三方防火墙联动，通过 SSH 命令方式封装各种处置策略并下发； 支持与同品牌防火墙、上网行为管理、终端安全管理、终端安全准入、WAF、服务器安全管理进行联动处置，可直接在本平台下发处置策略，支持对处置策略配置生效时长，支持对同一处置策略批量下发给多台联动设备，支持撤销联动处置命令。（提供相关功能的界面截图）
态势大屏展示	资产态势支持统计展示全网资产分布情况，并且支持按照资产分组展示对应的资产数量、风险值和风险等级的明细列表；支持统计资产总数，以及统计资产注册状态占比情况；支持统计资产上开放的端口情况、服务情况、协议情况；支持统计资产发现来源（资产探查、数据同步、脆弱性发现、流量解析、人工方式）的分布情况；支持按照资产发现来源（资产探查、数据同步、脆弱性发现、流量解析、人工方式）统计最近 30 天资产发现的趋势。
系统管理	1、支持通过企业微信、钉钉、蓝信方式向个人或群发送系统消息通知（提供相关功能的界面截图） 2、支持对接威胁情报平台，实现对可疑 IP、域名、URL 的情报鉴定。（提供相关功能的界面截图） 3、可对平台日志采集发送速率、平台数据处理速率、ES 入库速率、HIVE 入库速率、流量采集器发送速率、平台接收速率等维度进行最近 5 分钟、最近 24 小时、最近 7 天维度的监控；（提供相关功能的界面截图）



10、安全管理中心

11、流量探针

指标项	技术要求
▲硬件规格	2U，内存≥16G，存储 CF 卡 4G，1T 企业级硬盘，流量吞吐≥600Mbps，并发连接数≥200 万，新建连接数≥8 万/秒，≥6 个千兆电口。
旁路部署	支持通过流量镜像的方式旁路部署在虚拟化网络中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断 TCP 威胁会话连接，支持通过流量被动识别资产。
流量采集	采集过滤条件支持但不限于源地址、目的地址、服务、流量采样比、时间等； 需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置；（提供功能截图） 支持离线采集，可通过手动 PCAP 导入或 FTP 等协议批量上传导入等方式对离线流量进行采集
流量识别与解析	支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库 3000+。 支持 LDAP、Kerberos、Radius 等认证解析； ▲具有自定义解析流量能力，支持基于正则表达式、TLV 格式、固定长度等提取模式对应用流量解析；（提供功能截图）
威胁检测	系统具备全面的间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等 系统具备全面的漏洞检测能力，可检测常见的溢出攻击、跨站脚本、SQL 注入、拒绝服务、跨站请求伪造、目录遍历、websHELL 上传等 系统需具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报；（提供功能截图） 系统本地需具备攻击告警的过滤能力，能够针对 IP 地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析；（提供功能截图）
数据外发	通信模式支持但不限于 KA**A、ZMQ、SYSLOG 等协议，需支持多路外发，并支持外发多地址的负载均衡处理；（提供功能截图） 支持灵活配置外发策略，日志类别可配置 传输模式支持加密、压缩、以及认证，认证包括但不限于 kerberos 认证、LDAP 认证。（提供功能截图）



旁路阻断	支持旁路 IPv4 和 IPv6 的 IP 阻断、URL 重定向、DNS 重定向。
二次开发接口	系统提供二次开发接口，接口形式为 Restful API，提供功能配置、统计等接口；

12、终端及服务器杀毒

指标项	技术要求
▲ 控制中心要求	控制中心支持级联方式和单一部署两种方式，控制中心根据客户端点数的增加支持横向扩展，操作系统支持 Windows Server 2008 R2/2012/2012 R2/2016 的 64 位版本（简体中文版）；
	配置 500 个 Linux/Windows 终端 5 年升级授权点授权。
	控制中心支持安装在虚拟机上；
语言要求	产品全功能支持简体中文/繁体中体/英语自由切换。提供功能截图
控制中心管理	管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性。提供功能截图
	客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察。
	支持在线更新病毒库、补丁库、威胁情报等数据，并且支持“按月、按周、按天、按小时”灵活设置更新时间。支持隔离网环境更新数据。
病毒防护概况	病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本
病毒查杀日志	病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。
病毒扫描	支持信任区设置，病毒扫描或实时防护时不扫描目录或文件。
	病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。
	支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约 10 层模式下的扫描。提供功能截图
主动防御	支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。
网络防护	支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。



	支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。提供功能截图
	支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。提供功能截图
终端病毒处理弹窗	客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理。
杀毒引擎	支持不少于三个杀毒引擎混合使用，提高病毒检出率。提供功能截图
漏洞修复设置	支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。
	支持影响到编辑 Office 文档时提醒，可取消此次修复任务。
	允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。
外设管理	支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMCIA）设置使用权限，并支持生效时间设置。
	支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID 和设备来源。
	支持对支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。提供功能截图
进程管理	支持对单点维护功能，可远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、签名、产品名称、公司名称等，支持远程结束进程。
	支持远程查看计算机各个网卡配置信息。
	支持终端进程红名单、黑名单、白名单功能。可设置核心进程必须运行，也可保护核心进程不被结束，违规并告警。
违规外联	支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。支持例外白名单添加。
能耗管理	支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。提供功能截图



13、数据库安全防护

指标项	技术要求
性能规格	▲2U, ≥16 个数据库, 网口类别: ≥1 管理口+≥1HA 口+≥4 电口≥4 光口, 网口类型: 1000M 电口*6 1000M 光口*4 2 组电口 bypass 无光口 bypass, 网络扩展: 最大可再扩展 3 模块, 硬盘: ≥2T*2 (支持 RAID1), CPU: Intel 4 核 CPU, 内存: ≥16G, 电源: 双电源
部署模式	为适应各种复杂的部署环境, 产品部署模式上应满足以下的要求: 1、支持透明串联部署, 支持硬件 bypass 2、支持反向代理方式部署, 反向代理部署支持 IPV6, 支持 HA, HA 模式下支持策略实时或定期同步 3、策略路由引流部署 4、支持软件化部署, 支持入侵检测和入侵防御两种防护模式, 入侵检测模式对业务是完全零影响 5、支持旁路部署 6、支持集群部署
支持数据库	▲支持 Oracle、MySQL、Mariadb、PostgreSQL、DB2、MSSqlserver、hive、hbase、kingbase、gbase8a、sybase、informix、MongoDB、达梦 (DM)、人大金仓 (KingBase)、ODPS、vertica、Guassdb 100/200、GreenPlum、spark 等数据库支持 (需提供产品截图)
访问控制	支持多种数据来源筛选管控, 包括 IP、客户端主机名、操作系统用户名、客户端工具名、数据库账号 (需提供产品截图)
	支持与数据分级分类系统结合, 实现基于身份认证和数据分级分类细粒度访问控制
	对于越权的动作可以选择: 阻断、脱敏、仅告警 (需提供产品截图)
	支持阻断未经授权的逻辑备份操作, 如 mysqldump、oracle exp、pg_dump 等
	支持分组管理进行分组合管控
	实现资产和访问控制、身份认证直接的对应
运维审批	支持申请运维任务通过邮件发送且通过邮件正文的链接审批 (需提供产品截图)
安全防护能力	内置的特征策略包含缓冲区溢出、SQL 注入、提权、数据库内核入侵探测等常见攻击特征, 内置多种数据库安全规则 (需提供产品截图)
	自定义规则支持根据账号、数据库名、客户端工具、操作系统用户名、客户端 IP、操作类型、SQL 关键字等制定防护策略 (需提供产品截图)
	自定义规则支持根据执行结果、影响行数、执行时长等设置防护策略
	自定义规则支持针对不同的数据库类型进行独立的策略动作设置
	支持基于返回行数的 sql 访问控制
	支持基于一定时间范围内基于同一会话、同一 ip、同一用户、同一工具等维度对数据库访问频次及返回行数的限制



	规则动作支持允许访问、命令阻断、会话阻断和动态脱敏
	支持数据库防护虚拟补丁技术，防护未升级数据库，并可以更新维护（需提供产品截图）
动态脱敏	自定义敏感数据规则，敏感信息发现结果的在线新增、修改和删除
	多种脱敏算法，如字符串取整、遮蔽等
	支持自定义策略脱敏，关键字、正则表达式、字符长度等。
	支持动态脱敏效果预览
	对于越权的数据访问进行动态脱敏，防止数据泄露
	支持复杂 SQL 脱敏，例如：字符串拼接、截取、正则表达式替换及截取、行列转换、分析函数等。
	对源数据库的操作影响在毫秒级以内
操作日志	支持多操作日志记录(例如：攻击日志、访问控制日志、脱敏日志、告警日志)、日志查询，可以对接日志审计平台。
	支持记录审计系统所有人员对设备的访问行为
	自审计日志包含时间、用户、来源 IP、操作名称、操作内容、操作结果等内容

五、云桌面

1、终端 1

指标项	技术要求
终端 1	不低于 ARM 4 核/2GB DDR3L/8GB Flash/6*USB/1000M/挂架云终端-Linux

2、终端 2

指标项	技术要求
终端 2	不低于 4 核 3.6GHz/4GB DDR4/256GB SSD/4*USB3.0/4*USB2.0/1*COM/1000M/底座云终端-国内版 需提供串口，接打印机使用 必须符合当前的 Win7 32 位操作系统使用需求，后续业务升级后需支持切换至 win10 64 位或麒麟或统信操作系统要求。

3、云桌面软件

指标项	技术要求
云桌面软件	▲1、云桌面管理软件 350 个 License，块存储 License-管理 12 个物理 CPU，实配 12 个物理 CPU 的分布式存储虚拟化授权，含规划部署服务；



	▲2、同一个管理平台下支持创建 VDI 和 VDI 不同类型桌面镜像文件，根据桌面镜像部署对应的虚拟机
	3、当主机、虚拟机、集群的 CPU 利用率、内存利用率、磁盘利用率或主机、虚拟机的磁盘吞吐量、网络吞吐量等达到预设值的阈值时，触发相应告警。将指定的告警信息以邮件方式发送给指定接收邮箱，或者以短信方式发送给指定短信接收电话。
	4、支持一键检测功能，帮助管理员快速了解整个平台的运行状态、性能以及可能存在的隐患。对于检测异常的指标项，系统会提供有效的改进建议，确保业务系统稳定可靠的运行。
	6、系统自带云盘服务，无需额外增加网盘服务器及软件或系统授权，即可实现用户数据在不同桌面或者 PC 电脑上数据漫游及共享，要求云盘具备不少于两种的访问方式
	7、为确保文件合规传输，系统支持针对普通文件或敏感文件开启多级审批机制，审批通过后，文件方可流转，并进行全流程跟踪记录。
	8、用户无需安装单独的客户端软件，通过浏览器即可登录并连接云桌面，方便快捷。且支持对 Web 客户端页面 logo、背景等信息进行定制
	▲3、终端 1 和终端 2 均必须符合当前的 Win7 32 位操作系统使用需求，后续业务升级后需支持切换至 win10 64 位或麒麟或统信操作系统要求。

4、 服务器

指标项	技术要求
服务器	1、2* CPU 模块 (2.9GHz/16 核/22MB/150W)，14*32GB 内存，6*8TB 7.2K 数据盘，2*600GB 系统盘，1.92 TB NVMe SSD 全闪盘, RAID 卡 (支持 8 个 SAS 口, 2G 缓存), 3*2 端口万兆光接口 (含光模块)，4 端口 1GE 电接口，2*电源模块
	2、配置≥1Gb 独立的远程管理控制端口；

5、 显示器

指标项	技术要求
显示器	采用屏幕尺寸须不小于 21.5 英寸，分辨率不小于 1920×1080@60Hz。
	宽高比使用 16:9 比例。

6、 鼠标和键盘

指标项	技术要求
-----	------



鼠标和键盘	标准有线鼠标和键盘
-------	-----------

7、 万兆交换机

指标项	技术要求
万兆交换机	交换容量 $\geq 2.56\text{Tbps}$ ，包转发率 $\geq 720\text{Mpps}$ ；
	万兆光口 ≥ 32 ，QSFP+ ≥ 2 ，满配万兆多模光模块。3 米 40G 堆叠线缆 1 根
	为确保用户安全可靠的组网，要求所选产品入网年度 ≥ 3 年，提供工信部入网证明。

8、 接入交换机

指标项	技术要求
接入交换机	交换容量 $\geq 430\text{Gbps}$ ，包转发率 $\geq 140\text{Mpps}$ ；若存在双指标，以低为准；
	千兆电口 ≥ 48 ，万兆光口 ≥ 4 ；
	为确保用户安全可靠的组网，要求所选产品入网年度 ≥ 3 年，提供工信部入网证明。



★四. 商务条款

包装及运输	1.产品包装应符合国家或专业（部）标准规定。货物的交付时，应附有产品合格证书（包括合格证、部件合格证、材料合格证等）、产品说明书、装箱单、易损件、备件及专用工具清单等，一套完整的技术文件资料。 2. 中标供应商应保证所供货物是全新的、未使用过的货物。中标供应商应保证其货物在正确安装、正常使用和保养条件下，在建筑物使用寿命内应确保正常使用。 3.中标供应商应负责设备的途中运输，对途中运输的安全负责。
合格标准	一次性验收。
质保期及售后服务	1.质保期5年（需提供5年原厂商的质保服务），质保期从安装调试完毕，最终验收合格之日开始计算。除非采购人另有要求，质保期内的服务均为免费上门服务。如遇软件产品升级、改版，应免费提供更新、升级服务。 2.在质保期内，需提供7x24x4技术支持服务，同时提供原厂首次硬件基本安装服务。采购人有故障申报，供货方须在半小时内电话响应并提供解决方案；若不能以电话方式解决故障，须在4小时内赶到现场24小时解决，或与采购人协商解决。 3、机房首年提供至少一名专业技术人员驻场维护服务，定期进行培训，培训人员具备单独运营维护能力。
项目投标报价要求	1. 投标报价包括产品购置费、软件开发费、平台对接费用、附件配件费、运输费、安装调试费、技术服务费、保修期内维护费、培训费、代理服务费和税金等，即投标报价为投标供应商所能承受整个项目的一次性最终、最低报价，如有漏项，视同已包含在其它项目中，合同总价和单价不做调整。 2. 按国家规定由中标供应商缴纳的各种税收已包含在投标总价内，由中标供应商向税务机关缴纳。
完成时间及地点	完成时间：合同签订45天内（具体以医院实际进度为准），完成安装、调试完成，且验收合格。 地点：由兰溪市中医院指定。
验收标准及要求	根据中华人民共和国现行技术标准，按招标文件以及有关技术评定标准等规范，由甲方统一组织验收。 1. 采购人组织对供应商履约的验收。验收方成员应当在验收书上签字，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用。 2. 采购人可以邀请参加本项目的其他供应商或者第三方机构参与验收。参与验收的供应商或者第三方机构的意见作为验收书的参考资料一并存档。 3. 严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技



	术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付挂钩。履约验收的各项资料应当存档备查。 4. 验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金。 验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。
付款方式	1、合同生效以及具备实施条件后 7 个工作日内支付合同金额的 40%，余款在项目验收合格后支付。 2、中标供应商在结算合同价款时需提供发票。



第四章投标供应商须知

一、说明

1.适用范围

1.1 本招标文件仅适用于本次招标采购所叙述的兰溪市中医院数据中心系统项目；

2.定义

2.1“采购代理机构”系指组织本次招标的**金华景鹏工程咨询有限公司**；

2.2“采购人”系指组织本次招标的兰溪市中医院；

2.3“投标供应商”系指向采购代理机构提交投标文件的投标供应商；

2.4“货物”系指投标供应商按招标文件规定须向采购人提供的一切设备、备品备件、工具、手册及其它有关工程、技术资料 and 文字材料；

2.5“服务”系指招标文件规定投标供应商须承担的运输、调试、技术支持、维修保养及其它类似的服务；

2.6“项目”系指投标供应商按招标文件规定向采购人提供的产品和服务。

2.7“★”标记且加黑的文字系指必须满足不能负偏离或必须应答的条款。

★3.合格的投标供应商

3.1 具有独立承担民事责任的能力；

3.2 具有良好的商业信誉和健全的财务会计制度；

3.3 具有履行合同所必需的设备和专业技术能力；

3.4 有依法缴纳税收和社会保障资金的良好记录；

3.5 参加本次政府采购活动前三年内，在经营活动中没有重大违法记录；

3.6 法律、行政法规规定的其它条件；

3.7 该行业国家规定必备的资质、资格；

3.8 本《招标文件》中所要求其他条件；

4.投标费用

4.1 不论投标结果如何，投标供应商应自行承担所有与投标有关的全部费用。采购代理机构在任何情况下均无义务和责任承担上述这些费用。

二、招标文件细则

5.招标文件的组成

5.1 招标文件除本《招标文件》内容外，采购代理机构在招标期间发出的质疑回答、补遗书和其他正式有效函件，均构成招标文件的组成部分。



5.2 投标供应商应认真对照阅读招标文件中所有的事项、格式、条款和技术规范等。投标供应商没有按照招标文件要求提交全部资料，或者投标供应商没有对招标文件在各方面都做出实质性响应是投标供应商的风险，并可能导致其投标被拒绝。

6. 质疑与投诉

6.1 质疑

6.1.1 根据《政府采购质疑和投诉办法》（财政部 94 号令）的规定，供应商认为采购文件、采购过程、中标或者成交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起 7 个工作日内，以书面形式向采购人、采购代理机构提出质疑。

采购文件要求供应商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。

6.1.2. 质疑应当以书面形式提出，格式见《政府采购质疑和投诉办法》（财政部令第 94 号）附件范本，下载网址：浙江政府采购网 (<https://zfcg.czt.zj.gov.cn/>)，位置：“首页-下载专区-质疑投诉模板”。供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

- 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。

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，或者其授权代表签字或者盖章，并加盖公章。质疑函应明确阐述招标过程或中标结果中使自己合法权益受到损害的实质性内容。

6.2 投诉

6.2.1 质疑供应商对采购人、采购代理机构的答复不满意，或者采购人、采购代理机构未在规定时间内作出答复的，可以在答复期满后 15 个工作日内向《政府采购质疑和投诉办法》第六条规定的财政部门提起投诉。

7. 招标文件的修改

7.1 在投标截止时间前，采购代理机构有权修改招标文件。采购代理机构可主动地或在解答投标供应商提出的澄清问题时对招标文件进行修改。



7.2 招标文件的修改将以书面形式通知所有购买招标文件的投标供应商，并对其具有约束力。投标供应商在收到上述通知后，应立即向采购代理机构回函确认。

7.3 为使投标供应商准备投标时有充分时间对招标文件的修改部分进行研究，采购代理机构可在投标截止前通知投标供应商，适当延长投标截止期。

7.4 招标文件的澄清、答疑、修改、补充文件是招标文件的组成部分，投标供应商须按照招标文件的澄清、答疑、修改、补充文件的要求参与投标，投标供应商没有做出实质性响应是投标供应商的风险，并可能导致其投标被拒绝。

三、投标文件

8.投标文件的语言、计量及货币

8.1 投标及投标供应商与采购有关的来往通知、函件和文件均应使用中文编写。

8.2 除在技术规格中另有规定外，计量单位应使用公制单位。

8.3 投标货币为人民币，单位为元。

9.对投标文件的要求

9.1 投标供应商应仔细阅读招标文件的所有内容，按招标文件的要求提供投标文件，并保证所提供的全部资料的真实性，以使其投标对招标文件做出实质性响应，否则，其投标可能被拒绝。

9.2 在招标文件对需求参数及服务要求中，投标供应商必须充分应答应满足采购人的强制性的需求，如“★”等，否则将导致废标。

9.3 投标供应商须对所参投服务的专利等知识产权负责，因知识产权问题引起的纠纷由投标供应商自行承担，采购方不承担因此产生的任何责任。

10.电子投标文件的组成

10.1 电子投标文件由资格证明文件、技术商务文件、价格文件三部份组成。**电子投标文件中均需采用 CA 签章。**投标供应商应根据“政府采购云平台供应商项目采购-电子交易操作指南”及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位。

10.2 递交的投标文件应分为资格证明文件、技术商务文件和价格文件，资格证明文件、技术商务文件为除报价及价格组成外的所有内容。资格证明文件、技术商务文件不得含报价，否则作废标处理。

10.3 资格证明文件的组成

10.3.1 经有关部门年检通过且在有效期内的《营业执照副本》或《事业单位法人证》复印件；



10.3.2 提符合参加政府采购活动应当具备的一般条件的承诺函；

10.3.3 小企业声明函（如有）（格式见附件）；

10.3.4 残疾人福利性单位声明函（如有）（格式见附件）；

10.3.5 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（如有）；

10.3.6 符合国家政策扶持不发达地区和少数民族地区的相关证明材料（如有）；

10.3.7 提供招标公告中符合投标供应商特定条件要求的有效资质证书复印件（如有）；

10.4 技术商务文件的组成

10.4.1 投标声明书(格式见附件)；

10.4.2 法定代表人身份证明书及身份证复印件(格式见附件)；

10.4.3 法定代表人授权委托书原件和委托代理人身份证复印件(格式见附件)（委托代理时需提供）；

10.4.4 提供有效的营业执照副本或事业单位法人证复印件并需加盖单位公章；

10.4.5 提供采购公告中符合投标供应商特定条件要求的有效其他资质复印件并加盖公司公章及需要说明的资料（如有）；

10.4.6 投标供应商同类项目实施情况一览表（格式见附件）（投标供应商同类项目实施情况一览表、合同复印件、用户验收报告、用户评价等）；

10.4.7 资信及商务响应表（格式见附件）；

10.4.8 投标供应商的信誉、荣誉证书；（如有）

10.4.9 投标供应商的基本情况（主要产品、技术力量、生产规模、经营业绩等）；

10.4.10 产品销售许可证；（如有）

10.4.11 安全生产许可证或者产品代理资格证明文件；（如有）

10.4.12 投标产品制造厂家自主创新、节能环保等方面的资质证书；（如有）

10.4.13 投标供应商质量管理体系和质量保证体系等方面的认证证书；（如有）

10.4.14 投标产品列入《节能产品政府采购品目清单》的相关证明材料（如有）；

10.4.15 投标产品列入《环境标志产品政府采购品目清单》的相关证明材料（如有）；

10.4.16 对本项目的技术服务类总体要求的理解；

10.4.17 项目总体架构及技术解决方案；

10.4.18 保证工期的施工组织方案及人力资源安排；



10.4.19 设备详细配置清单（格式见附件）；

10.4.20 技术规格偏离表（格式见附件）；

10.4.21 项目实施人员一览表（格式见附件）；

10.4.22 售后服务承诺书（格式见附件）；

10.4.23 服务质量承诺书（格式见附件）；

10.4.24 交货计划安排、项目组织实施方案；

10.4.25 项目安装、调试、验收方法或方案；

10.4.26 本采购文件第三章采购需求里要求提供的检验报告以及原材料的相关证明材料。（如有）

投标供应商需要说明的其他文件和说明。

10.5 价格文件的组成

10.5.1 投标函（格式见附件）；

10.5.2 开标一览表（格式见附件）；

10.5.3 分项报价表（格式见附件）；

10.5.4 投标供应商认为有必要提供的其他资料。

★注：法定代表人授权委托书必须由法定代表人签字或盖章并加盖单位公章。本项目参投分支机构负责人身份或其授权书法律效力参照“浙财采监[2013]24 号”文件执行。投标供应商法定代表人或其授权代表人未参加开标的，视同认可开标结果。

11.投标报价（本项目设有最高限价 1270 万元，高于最高限价为废标）为整个项目报价，包括产品购置费、软件开发费、平台对接费用、附件配件费、运输费、安装调试费、技术服务费、保修期内维护费、培训费、代理服务费和税金等一切费用。投标报价为投标供应商所能承受的最低、最终一次性报价。投标供应商的投标报价为整个采购项目的总报价，如有漏项，视同已包含在其总项目中，合同总价不做调整。

11.1 投标报价应以人民币为结算货币。

11.2 投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

11.2.1 投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

11.2.2 大写金额和小写金额不一致的，以大写金额为准；

11.2.3 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；



11.2.4 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。评标委员会应当要求供应商对修正后的报价予以确认并对供应商产生约束力，投标供应商不确认的，其投标无效。

★11.3 采购项目只允许有一个报价，有选择的报价将不予接受，并作无效标处理。

11.4 投标分项报价表填写时应详细注明该表列举的费用及分项清单。

12. 履约保证金：

12.1 在合同签订后，中标供应商向采购人交纳中标合同总价 1%的履约保证金；履约保证金交付方式：银行转账或银行、保险公司出具的保函等形式。

12.2 履约保证金退还：履约保证金以银行转账方式提交，在履约完成后无息退还；以履约保函方式提交，在履约完成后自动失效。

13. 投标有效期

13.1 投标文件从开标之日起，投标有效期为 90 天。

13.2 特殊情况下，在原投标有效期截止之前，采购人可要求投标供应商同意延长有效期，这种要求与答复均应以书面形式提交。

14. 投标偏离及建议

14.1 投标供应商如对采购项目的要求在技术和商务方面有偏离，均须在规范的偏离表中提出。

14.2 投标供应商可以在投标文件中对采购设备的技术规格要求提出推荐和替代意见，但所提出的意见应优于招标文件中提出的响应要求，并且使采购人满意。

14.3 投标供应商在投标文件中需说明本次投标产品的技术参数是否与官网上公开的技术参数一致，如不一致，明确哪些参数不一致，不一致的原因以及使用何种技术可以达到投标产品参数。

15、投标文件格式和装订

15.1 投标供应商应参照招标文件中第八章提供的“投标文件格式”填写并装订。

四、投标文件的递交

16. 投标文件的签署和盖章

16.1 投标供应商应按本投标须知规定，涉及签字或盖章地方，由投标供应商法定代表人或其法定代表人授权代表签章；若系授权代表签章，应将法定代表人授权投标



委托书装订在投标文件技术商务文件内。投标供应商单位名称应为全称，并加盖公章。

16.2 投标文件的任何一页不得涂改、行间插字或删除。如有错漏必需修改，修改处须由同一签署人签字并加盖公章。由于字迹模糊或表达不清引起的后果由投标供应商负责。

17.投标文件的密封和标记

17.1 投标供应商线上制作的投标文件，采用 CA 数字证书进行电子签章及加密。

17.2 投标供应商邮寄或现场递交的备份电子投标文件应密封封装，注明投标供应商名称、项目名称、项目编号等，并封口处加盖公章。

18.投标地点和时间

18.1 投标地点：政府采购云平台（<https://www.zcygov.cn/>）在线投标。

18.2 投标截止时间：**2023 年 04 月 11 日 10: 00。**

18.3 投标截止前，允许投标供应商补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标截止时间后上传的投标文件，将被政府采购云平台拒收。

五、关联企业投标

19.1 本招标文件所称关联企业,是指存在关联关系的企业;“关联关系”的界定适用《中华人民共和国公司法》第 216 条之规定。

19.2 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投标。

六、无效投标的具体情形

20.有以下情形之一将作无效标处理

20.1 投标文件未按招标文件要求签署、盖章的;

20.2 不具备招标文件中规定的资格要求的;

20.3 报价超过招标文件中规定的最高限价的;

20.4 投标文件含有采购人不能接受的附加条件的;

20.5 法律、法规和招标文件规定的其他无效情形。

七、政府采购政策落实

21. 采购项目需要落实的政府采购政策



21.1 本项目原则上采购本国生产的货物、工程和服务，不允许采购进口产品。除非采购人采购进口产品，已经在采购活动开始前向财政部门提出申请并获得财政部门审核同意，且在采购需求中明确规定可以采购进口产品，未明确视同不得采购进口产品（但如果因信息不对称等原因，仍有满足需求的国内产品要求参与采购竞争的，采购人、采购机构不会对其加以限制，仍将按照公平竞争原则实施采购）。

21.2 支持绿色发展

21.2.1 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理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。供应商须按采购文件要求提供相关产品认证证书。▲采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，供应商未按采购文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的，投标无效。

21.2.2 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，供应商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）》。

21.3 支持中小企业发展

21.3.1 中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。

符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

21.3.2 在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

21.3.2.1 在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

21.3.2.2 在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

21.3.2.3 在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。



21.3.3 对于未预留份额专门面向中小企业的政府采购货物或服务项目，以及预留份额政府采购货物或服务项目中的非预留部分标项，对小型和微型企业的投标报价给予扣除，用扣除后的价格参与评审。接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的政府采购货物或服务项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的，对联合体或者大中型企业的报价给予扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

21.3.4 符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）规定的条件并提供《残疾人福利性单位声明函》（附件 1）的残疾人福利性单位视同小型、微型企业；

21.3.5 符合《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68 号）规定的监狱企业并提供由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证明文件的，视同为小型、微型企业。

21.3.6 可享受中小企业扶持政策的供应商应按照采购文件格式要求提供《中小企业声明函》，供应商提供的《中小企业声明函》与实际情况不符的，供应商未按采购文件要求提供国家确定的认证机构出具的、处于有效期之内的产品认证证书的，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

21.3.7 中小企业享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

21.4 支持创新发展

21.4.1 采购人优先采购被认定为首台套产品和“制造精品”的自主创新产品。

21.4.2 首台套产品被纳入《首台套产品推广应用指导目录》之日起 3 年内，以及产品核心技术高于国内领先水平，并具有明晰自主知识产权的“制造精品”产品，自认定之日起 3 年内视同已具备相应销售业绩，参加政府采购活动时业绩分值为满分。

21.5 中小企业信用融资：为支持和促进中小企业发展，进一步发挥政府采购政策功能，省财政厅、浙江银监局、省金融办制定了《浙江省政府采购支持中小企业信用融资试点办法》浙财采监[2012]13 号)，所称的政府采购信用融资，是指银行业金融机构（以下简称银行）以政府采购诚信考核和信用审查为基础，凭借政府采购合同，按优于一般中小企业的贷款利率直接向申请贷款的投标人发放贷款的一种融资方式。投标人可登录浙江政府采购网(<https://zfcg.czt.zj.gov.cn/>)的中小企业信用融资栏目了



解相关信息。供应商可以通过浙江政府采购网(<https://zfcg.czt.zj.gov.cn/>)首页的“浙江政采贷”模块进入申请,还可以通过政府采购云平台(<https://www.zcygov.cn/>)首页的“金融服务”模块进入申请。

八、中止电子交易活动的情形

22. 出现以下情形, 导致电子交易平台无法正常运行, 或者无法保证电子交易的公平、公正和安全时, 中止电子交易活动:

22.1 电子交易平台发生故障而无法登录访问的;

22.2 电子交易平台应用或数据库出现错误, 不能进行正常操作的;

22.3 电子交易平台发现严重安全漏洞, 有潜在泄密危险的;

22.4 病毒发作导致不能进行正常操作的;

22.5 无法保证电子交易的公平、公正和安全的其他情况。

出现前款规定情形, 不影响采购公平、公正性的, 采购代理机构可以待上述情形消除后继续组织电子交易活动, 也可以决定某些环节以纸质形式进行; 影响或可能影响采购公平、公正性的, 重新采购。

九、电子投标特别提醒

23. 请所有投标供应商在政府采购云平台系统准时参加线上开标活动, 并且要求法定代表人或授权委托人全程在线。

24. 投标截止时间后, 采购代理机构将线上开启解密, 投标供应商需及时用 CA 锁在线解密, 解密时间为半小时, 逾期解密, 投标供应商自行承担风险。

25. 解密投标文件的 CA 锁必须跟制作投标文件的 CA 锁为同一个, 否则将导致解密失败。

26. 若解密失败, 且投标供应商未按要求提供备份电子投标文件, 将导致废标。

27. 中标供应商还需将**纸质版投标文件(正本 1 份、副本 4 份)**邮寄到金华景鹏工程咨询有限公司留档备用, 纸质版投标文件由资格证明文件、技术商务文件、价格文件三部分组成, 并且分别胶装成册。**纸质投标文件必须与上传到政府采购云平台系统的电子加密文件一致, 并且均需加盖单位公章。**



第五章开标和评标须知

1. 组织开标

1.1 采购代理机构按照规定的时间通过政府采购云平台系统组织开标、开启投标文件，所有投标供应商均应当准时在线参加。

1.2 投标截止时间后，投标供应商登录政府采购云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密。在线解密电子投标文件时间为开启解密后半个小时内；

1.3 评标委员会对投标文件进行评审；

1.4 在政府采购云平台系统上公布技术商务得分；

1.5 开启价格投标文件；

1.6 在政府采购云平台系统上公开报价开标情况；

1.7 评标委员会对报价情况进行评审；

1.8 在政府采购云平台系统上公布评审结果。

特别说明：政采云公司如对电子化开标及评审程序有调整的，按调整后的程序操作。

2. 组织评标程序和评标委员评审程序

2.1 组织评标程序

2.1.1 采购代理机构将按照招标文件规定的时间、地点和程序组织评标，各评审专家及相关人员应参加评审活动并接受核验、签到，无关人员不得进入评审现场。采购代理机构工作人员和采购单位监督人员一起负责检查备份电子投标文件密封的完整性并签字确认。

2.1.2 核验出席评审活动现场的评审小组各成员和相关监督人员身份，并要求其分别登记、签到，按规定统一收缴、保存其通讯工具，无关人员一律拒绝其进入评审现场。

2.1.3 介绍评审现场的人员情况，宣布评审工作纪律，告知评审人员应当回避情形；组织推选评审小组组长。

2.1.4 宣读提交投标文件的供应商名单，组织评审小组各位成员签订《政府采购评审人员廉洁自律承诺书》

2.1.5 根据需要简要介绍招标文件（含补充文件）制定及质疑答复情况、按书面陈述项目基本情况及评审工作需注意事项等，让评审专家尽快知悉和了解所评审项目的采购需求、评审依据、评审标准、工作程序等；提醒评审小组对客观评审项目应统一



评审依据和评审标准，对主观评审项目应确定大致的评审要求和评审尺度；对评审人员提出的有关招标文件、投标文件的问题进行必要的说明、解释或讨论。

2.1.6 做好评审现场相关记录，协助评审小组组长做好评审报告起草、有关内容电脑文字录入等工作，并要求评审小组各成员签字确认。

2.1.7 评审结束后，采购代理机构对评审小组各成员的专业水平、职业道德、遵纪守法等情况进行评价；同时按规定向评审专家发放评审费，并交还评审人员及其他现场相关人员的通讯工具。

2.1.8 在线询标期间，评审小组给予供应商提交澄清、说明或补正的时间不得少于半小时，供应商已经明确表示澄清、说明或补正完毕的除外。

2.2 评标委员会评审程序

2.2.1 在评审专家中推选评审小组组长

2.2.2 评审小组组长召集成员认真阅读招标文件以及相关补充、质疑、答复文件、项目书面说明等材料，熟悉采购项目的基本概况，采购项目的质量要求、数量、主要技术标准或服务需求，采购合同主要条款，投标文件无效情形，评审方法、评审依据、评审标准等。

2.2.3 评审人员对各供应商投标文件的有效性、完整性和响应程度进行审查，确定是否对招标文件作出实质性响应。

2.2.4 评审人员按招标文件规定的评审方法和评审标准，依法独立对符合性审查合格的供应商投标文件进行评估，综合比较并给予评价或打分，不受任何单位和个人的干预。

2.2.5 评审人员对各供应商投标文件非实质性内容有疑议或异议，或者审查发现明显的文字或计算错误等，及时向评审小组组长提出。经评审小组商议认为需要供应商作出必要澄清或说明的，应通知该供应商以书面形式作出澄清或说明。**供应商授权代表须通过政府采购云平台线上或指定的电子邮箱、传真号码等作出澄清、说明或者补正。**评审小组给予供应商提交澄清、说明或补正的时间不得少于半小时，供应商已经明确表示澄清、说明或补正完毕的除外。书面通知及澄清说明文件应作为政府采购项目档案归档留存。

2.2.6 评审人员需对采购代理机构人员唱票或统计的评审结果进行确认，现场监督员应对评审结果签署监督意见。如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。



2.2.7 评审小组根据评审汇总情况和招标文件规定确定中标候选供应商排序名单。采购人、经其书面授权的采购人代表或经其书面授权的评审小组按中标候选供应商排名顺序对供应商逐一进行资格审查，直至依法产生合格的中标供应商。

2.2.8 起草评审报告，所有评审人员须在评审报告上签字确认。

3. 对投标文件的审查和响应性的确定

3.1 开标后，评审人员组织审查投标文件是否完整，文件是否恰当地签署。

3.2 对于投标文件中不构成实质性偏差的不正规、不一致或不规则，可以接受，但这种接受不能损害或影响任何投标供应商的相对排序。

3.3 在详细评标之前，评审人员审查每份投标文件是否实质上响应了招标文件的要求。实质上响应的投标应该是与招标文件要求的全部条款、条件和规格相符，没有重大偏离的投标。对关键条文的偏离、保留或反对，**例如关于“★”条款及特别说明为强制性要求的偏离将被认为是实质上的偏离**。投标的响应性只根据投标文件的内容，而不寻求外部的证据。

3.4 实质上没有响应招标文件要求的投标将被拒绝。投标供应商不得通过修改或撤消不符合要求的偏离或保留从而使其投标成为实质上响应的投标。

如发现下列情况之一的，其投标将被拒绝或无效：

3.4.1 未按招标文件规定提供相关文件，如资格证明、身份证明等；提供虚假资料的（含中标后查实的）；联合体投标未附联合各方共同投标协议的。

3.4.2 投标文件不符合招标文件规定，未按规定格式填写，内容不全或关键字迹模糊、无法辨认的。涂改文件、伪造或编造投标文件的。

3.4.3 借用或冒用他人名义或证件投标的。

3.4.4 投标供应商逾期送达投标文件。

3.4.5 参投服务的技术或商务与招标文件偏离的部分，不能使采购人满意，或实质上不响应招标文件的。

3.4.6 技术商务标中体现或包含报价。

3.4.7 投标中不同投标供应商的投标文件出现雷同或相似（包括部分雷同或相似），对所有雷同或相似投标供应商按废标处理，采购人将保留进一步追究责任的权利。

3.4.8 投标供应商递交二份内容不同的投标文件，或在一份投标文件中对同一项目有二个或多个报价，且未声明哪个有效的。按照招标文件规定提交备选投标供应商案的除外。

3.4.9 投标供应商名称或组织结构与资格审查时不一致，投标供应商不以自己真正



身份参加竞标，以挂户或以他人名义参与竞标的。投标供应商参加政府采购活动前三年内在经济活动中有重大违法记录的。

3.4.10 投标供应商的报价超过限价的和其它不符合《政府采购法》或省、市有关政府采购法律、法规要求的。

4. 投标文件的澄清

在评标期间，采购代理机构可要求投标供应商对其投标文件进行澄清，但不得寻求、提供或允许对投标价格等实质性内容做任何更改。有关澄清的要求和答复均电子交易平台提交。

5. 对投标文件的评估和比较

5.1 由评标委员会对各投标文件的全部内容进行审阅，并确定各投标文件是否合格有效。凡是对招标文件的实质性要约内容不作响应的投标，将被视为不合格的投标，而不予接受。经过审标，对其投标文件中须要进行澄清的问题，将由评标委员会向投标供应商进行政府采购云平台线上询标，投标供应商应接受询标、澄清；其记录须经投标供应商授权代表审阅签章，并应视作投标文件的补充，对投标供应商具有约束力。评标过程中如发现有异常情况，由评委集体讨论决定。

5.2 若本项目采购响应（指投标或谈判、报价）截止时间止及评审期间，出现有效供应商不足 3 家的，将依法重新组织采购活动或按规定向同级财政部门说明情况，申请采用其他采购方式组织采购。

6. 评审纪律和原则

6.1. 评审专家必须公平、公正评审，遵纪守法，客观、廉洁地履行职责。

6.2. 评审专家在评审开始前，应关闭并上交随身携带的各种通信工具。

6.3. 评审专家在评审过程中，未经许可不得中途离开评审现场，不得迟到早退。

6.4. 评审专家和工作人员不得透露评审过程中的讨论情况和评审结果。

6.5. 评审时，评审专家须按招标文件规定的程序、条件和标准，对投标人投标文件的合规性、完整性和有效性进行审查、比较和评估，其中对投标人的资格条件、主要技术参数、商务报价和其他评审要素等，评审专家应逐项进行审查、比较，不得漏评少评。如发现与招标文件要求相偏离的，应对其偏离情形进行必要的核实，并在工作底稿中予以说明；如属于实质性偏离或符合无效投标文件的，可询问投标人，并允许投标人进行陈述申辩，但不允许其对偏离条款进行补充、修正或撤回。

6.6. 采购人、采购代理机构不得向评审委员会的评审专家作倾向性、误导性的解释或者说明。



6.7. 采购代理机构应当为评审专家提供必要的评审条件和相应的评审工作底稿，并严格按照规定程序组织评审专家有步骤地进行项目评审，对各评审专家的评审情况和评审意见进行合理性和合规性审查，对明显畸高、畸低的重大差异评审情况（其总评分偏离平均分 30%以上），提醒相关评审专家进行复核或书面说明理由。

6.8. 评审专家在评审过程中不得将自己的观点强加给其他评审专家，评审专家应自主发表见解，对评审意见承担个人责任。

6.9. 评审结束后，评审委员会应向采购代理机构提交项目评审报告。评审报告是采购人确定中标人的合法依据，评审委员会应当如实、客观地反映评审情况，按招标文件的评审办法和细则的规定推荐中标候选人，说明推荐理由，并重点对中标候选人的技术、服务和价格等情况进行评价和比较。如排名第一的投标人报价为最高报价的，评审报告中须对其报价的合理性等进行分析 and 特别说明。

6.10. 评审专家应当独立、客观、公正地提出评审意见，不得带有倾向性，不得影响其他评审专家评审，并在评审报告上签字；如对评审报告有异议的，可在报告上签署不同意见，并说明理由，否则将视为同意。

6.11. 评审专家应当遵守评审工作纪律，不得泄露评审文件、评审情况和评审中获悉的商业秘密。

评审委员会在评审过程中发现投标人有行贿、提供虚假材料或者串通等违法行为的，应当及时向财政部门报告。

6.12. 招标文件内容违反国家有关强制性规定的，评审委员会应当停止评审并向采购代理机构说明情况。

6.13. 评审专家应当配合采购人、采购代理机构答复投标人提出的质疑。

6.14. 评审专家应当配合财政部门的投诉处理工作。

6.15. 评审专家有如下行为之一的，责令改正，给予警告，可以并处一千元以下的罚款：

- ①明知应当回避而未主动回避的；
- ②在得知自己为评审专家身份后至评审结束前时段内私下接触投标人的；
- ③在评审过程中擅离职守，影响评审程序正常进行的；
- ④在评审过程有明显不合理或者不正当倾向性的；
- ⑤未按招标文件规定的评审方法和标准进行评审的。
- ⑥上述①至⑤行为影响中标结果的，中标结果无效。

6.16. 政府采购评审专家未按照招标文件规定的评审程序、评审方法和评审标准进



行独立评审或者泄露评审文件、评审情况的，由财政部门给予警告，并处 2000 元以上 2 万元以下的罚款；影响中标、成交结果的，处 2 万元以上 5 万元以下的罚款，禁止其参加政府采购评审活动。

政府采购评审专家与投标人存在利害关系未回避的，处 2 万元以上 5 万元以下的罚款，禁止其参加政府采购评审活动。

政府采购评审专家收受采购人、采购代理机构、投标人贿赂或者获取其他不正当利益，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，处 2 万元以上 5 万元以下的罚款，禁止其参加政府采购评审活动。

政府采购评审专家有上述违法行为的，其评审意见无效，不得获取评审费；有违法所得的，没收违法所得；给他人造成损失的，依法承担民事责任。

6.17 评审专家因回避、临时缺席或健康原因等特殊情况不能继续参加评审工作的，应按规定更换评审专家，被更换的评审人员之前所作出的评审意见不再予以采纳，由更换后的评审人员重新进行评审。无法及时更换专家的，要立即停止评审工作、封存评审资料，并告知供应商择期重新评审的时间和地点。

6.18 评审人员对有关招标文件、投标文件、样品、现场演示（如有）的说明、解释、要求、标准存在不同意见的，持不同意见的评审人员及其意见或理由应予以完整记录，并在评审过程中按照少数服从多数的原则表决执行。对招标文件本身不明确或存在歧义、矛盾的内容，应作对供应商而非采购人有利的解释；对因招标文件中有关产品技术参数需求表述不清导致供应商实质性响应不一致时，应终止评审，重新组织采购。评审人员拒绝在评审报告中签字又不说明其不同意见或理由的，由现场监督员记录在案后，可视为同意评审结果。

6.19 浙财采监【2013】24 号《关于规范政府采购供应商资格设定及资格审查的通知》第九条规定：如多家供应商提供相同品牌相同型号的产品参加同一政府采购项目竞争的，应当按一家供应商认定。评审时，应取其中通过资格审查后的报价最低一家为有效供应商；报价相同时，取技术分最高者；均相同时，由评审小组集体决定。

非单一产品采购项目中，作为关键核心部分的单一产品品牌、型号均相同且报价占项目总报价 50%以上（含本数，下同）的，视为提供的是同品牌同型号的产品；多家供应商中，有一家供应商的报价达到 50%以上，提供同品牌同型号产品的供应商均按一家供应商认定。

7. 保密



7.1 在开标、投标期间，投标供应商不得向评标委员会成员询问评标情况，不得进行旨在影响评标结果的活动。

7.2 为保证定标的公正性，在评标过程中，评标成员不得与投标供应商私人交换意见。在招标工作结束后，凡与评标情况有接触的任何人员不得也不应将评标情况扩散出评标成员之外。

7.3 评标委员会不向落标方解释未中标原因，不退还投标文件。

8. 定标

8.1 项目由评标委员会根据第六章《评标细则》规定推荐中标候选人。

8.2 采购结果由采购人代表签名确认。采购人未确定中标供应商且在规定时间内提出异议的，视为默认。

8.3 采购结果经采购人确认后，在浙江政府采购网和兰溪市公共资源交易专栏上发布中标公告，并向中标供应商签发书面《中标通知书》。如有投标供应商对评标结果提出质疑的，采购人可在质疑处理完毕后确定中标供应商。

8.4 《中标通知书》将作为签订合同的重要依据。

9、合同授予

9.1. 合同的签订

9.1.1 除不可抗力等特殊情况外，采购人原则上应当在中标通知书发出之日起 20 日内，与中标（成交）人按照采购文件确定的事项签订政府采购合同，并在签订之日起 2 个工作日内将政府采购合同在浙江政府采购网上公告。

9.1.2 中标（成交）人按规定的日期、时间、地点，由法定代表人或其授权代表与采购人代表签订合同。如中标（成交）人为联合体的，由联合体成员各方法定代表人或其授权代表与采购人代表签订合同。

9.1.3 如签订合同并生效后，供应商无故拒绝或延期，除按照合同条款处理外，列入不良行为记录一次，并给予通报。

9.1.4 中标（成交）人拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标或者成交候选人名单排序，确定下一候选人为中标（成交）人，也可以重新开展政府采购活动。

9.1.5 采购合同由采购人与中标（成交）人根据采购文件、磋商响应文件等内容通过政府采购电子交易平台在线签订，自动备案。



9.1.6 政府采购货物和服务项目不得收取质量保证金。政府采购工程以及与工程建设有关的货物、服务，采用招标方式采购的，按国家和省有关规定执行。

9.2. 履约保证金

拟签订的合同文本要求中标（成交）人提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的 1%。鼓励和支持供应商以履约保函形式提供履约保证金。

供应商可登录政采云平台-【金融服务】-【我的项目】-【已备案合同】以保函形式提供：1、供应商在合同列表选择需要投保的合同，点击[保函推荐]。2、在弹框里查看推荐的保函产品，供应商自行选择保函产品，点击[立即申请]。3、在弹框里填写保函申请信息。具体步骤：选择产品—填写供应商信息—选择中标项目—确认信息—等待保险/保函受理—确认保单一支付保费—成功出单。政采云金融专线 400-903-9583。

9.3 预付款

采购单位应当在政府采购合同中约定预付款，对中小企业合同预付款比例原则上不低于合同金额的 40%，不高于合同金额的 70%；项目分年安排预算的，每年预付款比例不低于项目年度计划支付资金额的 40%，不高于年度计划支付资金额的 70%；采购项目实施以人工投入为主的，可适当降低预付款比例，但不得低于 30%。对供应商为大型企业的项目或者以人工投入为主且实行按月定期结算支付款项的项目，预付款可低于上述比例或者不约定预付款。在签订合同时，供应商明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不适用前述规定。采购单位根据项目特点、供应商诚信等因素，可以要求供应商提交银行、保险公司等金融机构出具的预付款保函或其他担保措施。政府采购预付款应在合同生效以及具备实施条件后7个工作日内支付。政府采购工程以及与工程建设有关的货物、服务，采用招标方式采购的，预付款从其相关规定。

9.4 资金支付

采购单位应当及时组织项目验收，不得以政府部门审计作为支付供应商款项的条件。采购单位对于满足合同约定支付条件的，自收到发票后 7 个工作日内将资金支付到合同约定的供应商账户。采购单位不得以机构变动、人员更替、政策调整、单位放假、履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审



计等为由迟延付款。迟延支付中小企业款项的，供应商可要求采购单位支付逾期利息。

9.5 验收

9.2.1. 采购人组织对供应商履约的验收。大型或者复杂的政府采购项目，应当邀请国家认可的质量检测机构参加验收工作。验收方成员应当在验收书上签字，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用，并接受相应的处理。

9.2.2. 采购人可以邀请参加本项目的其他供应商或者第三方机构参与验收。参与验收的供应商或者第三方机构的意见作为验收书的参考资料一并存档。

9.2.3. 严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

9.2.4. 采购人原则上应当在履约验收之日起2个工作日内，将履约验收结果在浙江政府采购网上公告。

9.2.5. 验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金、退还履约保证金。

验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。



第六章 评标细则

根据《中华人民共和国政府采购法》、《政府采购货物和服务招标投标管理办法》、

开标后，采用综合评分法，评标委员会首先对投标文件的完整性、符合性、响应性等进行审查。凡不符合有关规定或不响应招标文件要求的投标文件将不进入评标范围。评标专家组以开标、审标、询标情况为基本依据，对有效的投标文件及其投标供应商按评标内容进行分析、评议，确定合格供应商，根据《政府采购货物和服务招标投标管理办法》（财政部令第 87 号）文件规定，本次招标采购技术商务分为 70 分，价格分为 30 分。先评技术商务标得分，对合格的供应商进行技术商务分计算。后再开价格文件，取合格供应商中投标价格最终最低的投标报价为评标基准价，对合格的供应商进行价格分计算，以二项总分最高为中标供应商（总得分相同的，优先采购节能产品、环境标志产品、中小企业产品、监狱企业产品、残疾人福利性单位产品；均相同的，按投标报价由低到高顺序排列；技术商务分与投标报价都相同的，抽签决定中标单位，如若供应商不参加抽签，则取消其中标候选人资格。）中标供应商因不可抗力不能履行政府采购合同的，采购人可以与排位在中标供应商之后第一位的中标候选人签订政府采购合同，以此类推或重新招标。

三、技术商务标评定（满分为 70 分）

（1）技术商务分设置为 70 分，分值分配见以下表格。评标委员会根据评分标准，对该标项各投标供应商的技术商务标进行审核和评论后，由各评标成员独立给分，打分时保留小数 2 位，每人一份评分表，并签名。在统计得分时，如果发现某一单项评分超过评分细则规定的分值范围，则该张评分表无效。投标供应商技术商务标最终得分为评标成员的有效评分的算术平均值。计算时保留小数 2 位。

（2）评分标准：技术商务部分（70 分）

序号	评分项目	分值	评分基本规则
一、资信商务部分（20 分）			
1	政策分	0-2 分	投标产品列入财库〔2019〕18 号文《环境标志产品政府采购品目清单》的得 1 分；列入财库〔2019〕19 号文《节能产品政府采购品目清单》的得 1 分。（提供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



			认证证书复印件及认证机构名录，否则不得分。)
2	管理体系	0-4 分	投标人具有 ISO9001 质量管理体系证书（含系统集成）、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证证书、ISO45001 职业健康安全管理体系认证证书、ISO27001 信息安全管理体认证、信息系统建设和服务能力优秀级认证（CS4），每项得 0.5 分，最高得 3 分；ITSS 信息技术服务运行维护标准符合性证书二级及以上证书得 1 分， (需提供有效期内证书的复印件加盖投标单位公章)
3	成功案例业绩	0-3 分	投标供应商提供自 2020 年 1 月 1 日以来完成过同类项目业绩，每提供 1 个得 1 分，最高得 3 分。（提供合同复印件加盖投标单位公章）
4	质保期	0-2 分	质保期至少 5 年，每增加半年得 0.5 分，最高得 2 分。
5	拟派团队人员	0-3 分	项目负责人具有人社厅颁发的信息系统项目管理师（高级）资质证书、国家信息安全测评注册信息安全专业人员证书（CISP 每个得 1.5 分； (需提供有效期内的证书复印件或相关证明材料及在本单位缴纳近三个社保证明，否则不得分)
		0-3 分	拟派团队成员具有与本项目相关专业高级工程师职称得 1 分；具有 PMP 项目经理、网络工程师、信息系统管理师、信息系统项目管理师（高级）资质证书每个得 0.5 分，最高得 2 分； (需提供有效期内的证书复印件或相关证明材料及在本单位缴纳近三个社保证明，否则不得分)
6	后续服务	0-3 分	投标人提供完整的、可行的后续服务方案（包括服务能力、服务措施、服务承诺等方面）和后续的技术实施保障措施每项得 1 分，最高得 3 分。 未提供技术支持和售后服务方案的，或未描述的，不得分。
二、技术部分（50 分）			
1	技术参数及配置	0-25 分	投标产品的基本功能、技术指标与需求的吻合程度和偏差情况，是否能够满足招标文件要求，全部满足招标文件要求的得满分；“★”项属于关键指标不允许出现偏离，否则视为无效标；“▲”项为重要指标，负偏离每项扣 3 分；其他参数指标负偏离每项扣 2 分，扣完为止。（技术参数中要求提供检测报告、截图等证明材料的，如未提供，则视作



			负偏离)
2	实施方案	0-3 分	根据实施方案的清晰和完整性、技术方案的先进性、技术方案的经济合理性、核心部件满足要求的情况及功能及技术指标，设备可维护性，设备稳定性等情况， 经济合理性得 0-1 分； 技术指标得 0-1 分； 设备可维护性得 0-1 分； 未提供方案，或未描述的，不得分。
3	质量、进度、安全保障措施	0-3 分	根据投标供应商对本项目保证质量的技术方案、质量保证措施等情况 质量保证措施得 0-1 分； 进度保障措施得 0-1 分 安全保障措施得 0-1 分； 保障措施不合理或未提供不得分
4	安装、验收方案	0-4 分	根据投标供应商提供项目的整个安装、调试方案等 安装方案得 0-2 分； 验收方案得 0-2 分； 未提供方案，或未描述的，不得分
5	应急响应能力	0-3 分	投标方案中是否给出合理有效的系统安全设计方案和应急预案方案，预案完整、科学合理等： 系统安全设计方案得 0-1.5 分； 应急预案方案 0-1.5 分 未提供预案或预案不完整或未描述的不得分
6	培训	0-2 分	根据投标供应商针对本项目制定的培训方案进行评价，培训方案应至少包括：①培训时间、地点；②培训的主要内容（至少包含使用及日常维护内容）；③培训目标、原则；④培训内容、方式；⑤预期培训效果等；以上内容每完整响应 1 项得 0.5 分，最高得 2 分。
7	演示	0-10 分	根据投标供应商所提供的功能演示进行评审，演示时间不得超过 15 分钟，以提供演示视频 U 盘的方式提交，要求在一般 PC 端能够播放，如不能播放视作未提供演示，不提供演示不得分。 一、远程运维功能演示（4 分）： 1) 演示项 1：演示远程组件支持 SOS 一键提单，云端自动生成工单。该功能提供视频演示，满足此功能得 2 分，不满足则不得分。



		2) 演示项 2: 演示远程组件调试过程的云端录像审计功能, 支持在线录像回放。提供视频演示, 满足此功能得 2 分, 不满足则不得分。 二、存储能力演示 (6 分): 1) 演示项 1: 在存储管理软件中演示可根据目前负载情况及现有配置情况, 预测未来若干天存储的性能趋势; 在存储管理软件中演示云存储高级性能管理功能, 可以对存储整体、LUN 应用集合进行性能实时监控, 展示其带宽、IOPS、时延的实时状态, 并对热点卷排序; 可针对性能问题给予分析并展示影响当前性能的因素, 快速精准进行性能管理。通过性能洞察快速定位环境中性能瓶颈应用及对应的主机; 满足此功能得 3 分, 不满足则不得分; 2) 演示项 2: 演示 VMware DataStore 性能视图功能, 可以在存储管理界面下展示至少 20 个的 DataStore 的性能视图, 并通过视图大小反应 DataStore 的工作负载压力, 且根据颜色来区分性能压力是否异常, 为用户提供直观的虚拟机性能管理能力。满足此功能得 3 分, 不满足则不得分。 注: (以视频方式进行演示, 事先将录制的 U 盘, 按要求密封送达, 不提供演示视频或视频无法播放的不得分。)
--	--	--

四、价格分 (满分为 30 分)

价格文件的开启: 技术商务入围投标供应商确定后, 将开启合格投标供应商的价格文件, 公开宣读并由投标供应商确认。对没有合格的投标供应商价格文件将不予开启。价格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终最低的投标报价为评标基准价, 其价格分为满分。(注: 对于小型和微型、监狱企业、残疾人福利性单位提供产品的价格给予 10% 的扣除, 用扣除后的价格参与评审。企业需提供证明文件详见第四章投标供应商须知第十条关于中小企业、监狱企业、残疾人福利性单位参与政府采购活动的规定, 并且不重复享受。)

根据《政府采购货物和服务招标投标管理办法》(财政部令第 87 号) 第六十条规定: “评标委员会认为投标供应商的报价明显低于其他通过符合性审查投标供应商的报价, 有可能影响产品质量或者不能诚信履约的, 应当要求其在评标现场合理的时间内



提供书面说明，必要时提交相关证明材料；投标供应商不能证明其报价合理性的，评标委员会应当将其作为无效投标处理”。

投标供应商的价格分按照下列公式计算：

投标报价得分=（评标基准价/投标报价）×30%×100

五、总分计算方法（满分为 100 分）

计算公式：投标供应商的最终得分=技术商务得分+价格得分（所有分值四舍五入，保留到小数点后 2 位。）



第七章兰溪市中医院数据中心系统项目合同

甲方：签订地点：浙江省兰溪市

乙方：签订时间：年月日

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关政府采购法律、法规及省、市有关规定，甲乙双方按照兰溪市中医院数据中心系统项目（采购编号：jhjp-lxszyy20230310012）采购结果，签订本合同：

一、合同货物

序号	货物名称	制造商、产地	品牌和型号	数量及单位	单价（元）	总价（元）
合计： (大写):						

二、供货时间、地点：乙方必须于合同签订之日起 **45** 个日历天内（具体以医院实际进度为准），将上述清单所列的货物送至甲方指定地点免费安装、调试完毕，且验收合格。并承担运输过程中发生的一切费用。

三、质量标准：

1、乙方所提供的货物必须是原厂生产、全新未使用过的(包括零部件)，并完全符合原厂质量检测标准(以说明书为准)和国家质量检测标准以及合同规定的性能要求。

2、设备出现质量问题，乙方应负责三包(包修、包退、包换)。由于使用单位保管不当造成的质量问题，乙方亦应负责修理，但费用由使用单位负担。每台设备上均应订铭牌(内容包括制造单位、设备名称、型号规格、出厂日期等)。

四、付款方式：

1.合同生效以及具备实施条件后 **7** 个工作日内支付合同金额的 **40%**，余款在项目验收合格后支付。

2.乙方在结算合同价款时需提供发票；

五、履约保证金：



1、在合同签订后，乙方向甲方缴纳中标合同总价 1%的履约保证金；履约保证金以支票、汇票、本票或者金融机构、保险机构出具的保函等非现金形式提交。

2、履约保证金退还：履约保证金以支票、汇票、本票提交的，在履约完成后退还，履约保证金以保函方式提交的，在履约完成后自动失效。

六、验收：

根据中华人民共和国现行技术标准，按招标文件以及有关技术评定标准等规范，由甲方统一组织验收。

1. 采购人组织对供应商履约的验收。验收方成员应当在验收书上签字，并承担相应的

2. 采购人可以邀请参加本项目的其他供应商或者第三方机构参与验收。参与验收的供应商或者第三方机构的意见作为验收书的参考资料一并存档。

3. 严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付挂钩。履约验收的各项资料应当存档备查。

4. 验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金。

验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。

七、违约责任：

1、违反本合同约定，造成本合同不能履行或不能完全履行，由违约方承担违约责任，违约方应按合同法赔偿对方经济损失。

2、甲方无故逾期验收和办理合同价款支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3、乙方未按采购方要求的时间提供货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，从履约保证金中扣除。逾期超过约定日期 10 个工作日不能履行交货的，甲方可解除本合同。乙方因逾期履行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。

4、乙方达不到项目要求，乙方应负责根据合同及甲方的要求采取相应的处理措施，并承担由此发生的一切损失和费用，整改延误的时间不作为整个项目工期延期的理由。

5、由于甲方的使用单位延期的原因要求延期交货时，甲方使用单位应按规定承付货款，并承担供方所提供的代为保管费用(按有关仓储规定另议)。

八、质量保证及售后服务

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。

2.乙方提供的货物在保修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：由甲乙双方协议定价。

(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、货款利息及银行手续费等）。

3.如在使用过程中发生质量问题，乙方在接到甲方通知后在小时内到达甲方现场。

4.在保修期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

5.上述的货物免费保修期为年，因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

九、货物包装、发运及运输

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。

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。

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。

4.货物在交付甲方前发生的风险均由乙方负责。

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、不可抗力事件处理



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。

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。

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。

十一、合同相关文件:有关本次采购项目的招标文件以及相关的函件如答疑函、承诺函等均为本合同不可分割的一部份。若“本次采购项目的招标文件以及相关的函件、如答疑函、承诺函”与本合同有出入时,以“本次采购项目的招标文件以及相关的函件如答疑函、承诺函”为准。

十二、合同在执行过程中出现的未尽事宜,双方在不违背本合同和采购(招标)文件的原则下,协商解决,协商结果以书面形式盖章记录在案,作为本合同的附件,具有同等效力。

十三、合同争议处理方式:本合同在履行中若发生争议,双方应协商解决。协商不成时,依法向兰溪市人民法院起诉。

本合同一式六份,甲、乙双方及金华景鹏工程咨询有限公司各执两份。

合同附件和本合同均具有同等法律效力。

本合同有效期限:自签订之日起生效。



甲方	乙方	
单位名称（章）：	单位名称（章）：	合同见证单位：
单位地址：	单位地址：	经办人：
法定代表人或委托代理人：	法定代表人或委托代理人：	（单位盖章）：
电话：	电话：	
开户银行：	开户银行：	
账号：	账号：	年月日
邮政编码：	邮政编码：	

注：此合同样本仅作参考，甲、乙双方可根据采购项目的实际情况进行修改。



第八章投标文件格式

资格证明文件

项目名称：兰溪市中医院数据中心系统项目

项目编号：**jhjp-lxszyy20230310012**

投标供应商名称：（公章）

投标供应商地址：

年月日



资格证明文件：

- （1）经有关部门年检通过且在有效期内的《营业执照副本》或《事业单位法人证》复印件；
- （2）符合参加政府采购活动应当具备的一般条件的承诺函；
- （3）中小企业声明函（如有）（格式见附件）；
- （4）残疾人福利性单位声明函（如有）（格式见附件）；
- （5）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（如有）；
- （6）提供招标公告中符合投标供应商特定条件要求的有效资质证书复印件（如有）；

说明：以上材料均需加盖公司公章。



符合参加政府采购活动应当具备的一般条件的承诺函

致：兰溪市中医院：

我方参与 XXX 项目【项目编号：XXX】政府采购活动，郑重承诺：

（一）具备《中华人民共和国政府采购法》第二十二条第一款规定的条件：

- 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，在经营活动中没有重大违法记录；
- 6、具有法律、行政法规规定的其他条件。

（二）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、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

（三）不存在以下情况：

- 1、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参加同一合同项下的政府采购活动的；
- 2、为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后再参加该采购项目的其他采购活动的。

投标供应商名称（盖章）：

日期：



中小企业声明函（货物）

本公司（联合体）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（联合体）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（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称），属于（招标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¹，属于（中型企业、小型企业、微型企业）；

2. （标的名称），属于（招标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。

投标供应商名称（公章）：

日期：

注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。



残疾人福利性单位声明函

本单位郑重声明，根据《财政部民政部中国残疾人联合会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（由本单位承担工程/提供服务），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）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标供应商名称（公章）：

日期：

注：本函为残疾人福利性单位提供。



技术商务文件

项目名称：兰溪市中医院数据中心系统项目

项目编号：**jhjp-lxszyy20230310012**

投标供应商名称：（公章）

投标供应商地址：

年月日



技术商务文件：

- 1) 投标声明书(格式见附件)；
- 2) 法定代表人身份证明书及身份证复印件(格式见附件)；
- 3) 法定代表人授权委托书原件和委托代理人身份证复印件(格式见附件)（委托代理时需提供）
- 4) 提供有效的营业执照副本或事业单位法人证复印件并需加盖单位公章；
- 5) 提供采购公告中符合投标供应商特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料（如有）；
- 6) 投标供应商同类项目实施情况一览表(格式见附件)（投标供应商同类项目实施情况一览表、合同复印件、用户验收报告、用户评价等）；
- 7) 资信及商务响应表(格式见附件)；
- 8) 投标供应商的基本情况（主要产品、技术力量、生产规模、经营业绩等）；
- 9) 对本项目的技术服务类总体要求的理解；
- 10) 项目总体架构及技术解决方案；
- 11) 保证工期的施工组织方案及人力资源安排；
- 12) 设备详细配置清单(格式见附件)；
- 13) 技术规格偏离表(格式见附件)；
- 14) 项目实施人员一览表(格式见附件)；
- 15) 服务质量承诺书(格式见附件)；
- 16) 投标供应商需要说明的其他文件和说明。

说明：具体的响应文件组成按第四章投标须知及第六章评标细则的要求。



技术商务自评分索引

序号	评分项目	分值	评分基本规则
一、资信商务部分（20 分）			
1	政策分	0-2 分	投标产品列入财库〔2019〕18 号文《环境标志产品政府采购品目清单》的得 1 分；列入财库〔2019〕19 号文《节能产品政府采购品目清单》的得 1 分。（提供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复印件及认证机构名录，否则不得分。）
2	管理体系	0-4 分	投标人具有 ISO9001 质量管理体系证书（含系统集成）、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证证书、ISO45001 职业健康安全管理体系认证证书、ISO27001 信息安全管理体认证、信息系统建设和服务能力优秀级认证（CS4），每项得 0.5 分，最高得 3 分；ITSS 信息技术服务运行维护标准符合性证书二级及以上证书得 1 分， （需提供有效期内证书的复印件加盖投标单位公章）
3	成功案例业绩	0-3 分	投标供应商提供自 2020 年 1 月 1 日以来完成过同类项目业绩，每提供 1 个得 1 分，最高得 3 分。（提供合同复印件加盖投标单位公章）
4	质保期	0-2 分	质保期至少 5 年，每增加半年得 0.5 分，最高得 2 分。
5	拟派团队人员	0-3 分	项目负责人具有人社厅颁发的信息系统项目管理师（高级）资质证书、国家信息安全测评注册信息安全专业人员证书（CISP 每个得 1.5 分； （需提供有效期内的证书复印件或相关证明材料及在本单位缴纳近三个社保证明，否则不得分）
		0-3 分	拟派团队组成员具有与本项目相关专业高级工程师职称得 1 分；具有 PMP 项目经理、网络工程师、信息系统管理师、信息系统项目管理师（高级）资质证书每个得 0.5 分，最高得 2 分； （需提供有效期内的证书复印件或相关证明材料及在本单位缴纳近三个社保证明，否则不得分）
6	后续服务	0-3 分	投标人提供完整的、可行的后续服务方案（包括服务能力、服务措施、服务承诺等方面）和后续的技术实施保障措施每项得 1 分，最高得 3 分。 未提供技术支持和售后服务方案的，或未描述的，不得分。



二、技术部分（50 分）			
1	技术参数及配置	0-25 分	投标产品的基本功能、技术指标与需求的吻合程度和偏差情况，是否能够满足招标文件要求，全部满足招标文件要求的得满分；“★”项属于关键指标不允许出现偏离，否则视为无效标；“▲”项为重要指标，负偏离每项扣 3 分；其他参数指标负偏离每项扣 2 分，扣完为止。（技术参数中要求提供检测报告、截图等证明材料的，如未提供，则视作负偏离）
2	实施方案	0-3 分	根据实施方案的清晰和完整性、技术方案的先进性、技术方案的经济合理性、核心部件满足要求的情况及功能及技术指标，设备可维护性，设备稳定性等情况， 经济合理性得 0-1 分； 技术指标得 0-1 分； 设备可维护性得 0-1 分； 未提供方案，或未描述的，不得分。
3	质量、进度、安全保证措施	0-3 分	根据投标供应商对本项目保证质量的技术方案、质量保证措施等情况 质量保证措施得 0-1 分； 进度保证措施得 0-1 分 安全保证措施得 0-1 分； 保证措施不合理或未提供不得分
4	安装、验收方案	0-4 分	根据投标供应商提供项目的整个安装、调试方案等 安装方案得 0-2 分； 验收方案得 0-2 分； 未提供方案，或未描述的，不得分
5	应急响应能力	0-3 分	投标方案中是否给出合理有效的系统安全设计方案和应急预案方案，预案完整、科学合理等： 系统安全设计方案得 0-1.5 分； 应急预案方案 0-1.5 分 未提供预案或预案不完整或未描述的不得分
6	培训	0-2 分	根据投标供应商针对本项目制定的培训方案进行评价，培训方案应至少包括：①培训时间、地点；②培训的主要内容（至少包含使用及日常维护内容）；③培训目标、原则；④培训内容、方式；⑤预期培训效果等；以上内容每完整响应 1 项得 0.5 分，最高得 2 分。



7	演示	0-10 分	根据投标供应商所提供的功能演示进行评审，演示时间不得超过 15 分钟，以提供演示视频 U 盘的方式提交，要求在一般 PC 端能够播放，如不能播放视作未提供演示，不提供演示不得分。 一、远程运维功能演示（4 分）： 1）演示项 1：演示远程组件支持 SOS 一键提单，云端自动生成工单。该功能提供视频演示，满足此功能得 2 分，不满足则不得分。 2）演示项 2：演示远程组件调试过程的云端录像审计功能，支持在线录像回放。提供视频演示，满足此功能得 2 分，不满足则不得分。 二、存储能力演示（6 分）： 1）演示项 1：在存储管理软件中演示可根据目前负载情况及现有配置情况，预测未来若干天存储的性能趋势；在存储管理软件中演示云存储高级性能管理功能，可以对存储整体、LUN 应用集合进行性能实时监控，展示其带宽、IOPS、时延的实时状态，并对热点卷排序；可针对性能问题给予分析并展示影响当前性能的因素，快速精准进行性能管理。通过性能洞察快速定位环境中性能瓶颈应用及对应的主机；满足此功能得 3 分，不满足则不得分； 2）演示项 2：演示 VMware DataStore 性能视图功能，可以在存储管理界面下展示至少 20 个的 DataStore 的性能视图，并通过视图大小反应 DataStore 的工作负载压力，且根据颜色来区分性能压力是否异常，为用户提供直观的虚机性能管理能力。满足此功能得 3 分，不满足则不得分。 注：（以视频方式进行演示，事先将录制的 U 盘，按要求密封送达，不提供演示视频或视频无法播放的不得分。）
---	----	--------	--



投标声明书

致：兰溪市中医院

（投标供应商名称）系中华人民共和国合法企业，经营地址。

我（姓名）系（投标供应商名称）的法定代表人，我方愿意参加贵方组织的项目的投标，为便于贵方公正、择优地确定中标供应商及其投标产品和服务，我方就本次投标有关事项郑重声明如下：

- 1、我方向贵方提交的所有投标文件、资料都是准确的和真实的；
- 2、我方不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。
- 3、我方诚意提请贵方关注：有关该型号产品的生产、供货、售后服务以及性能等方面的重大决策和事项有：

4、我方最近三年内的被公开披露或查处的违法违规行为有：

5、以上事项如有虚假或隐瞒，我方愿意承担一切后果和责任。

投标供应商名称（公章）：

法定代表人或授权委托人（签字或盖章）：

时间：年月日



法定代表人身份证明书

单位名称：

单位性质：

地址：

成立时间：年月日

经营期限：

姓名：性别：年龄：职务：

系（投标供应商名称）的法定代表人。

特此证明。

投标供应商名称：（公章）

日期：年月日



法定代表人授权书

本授权书声明：注册于的公司的在下面签字的(法定代表人姓名、职务)代表本公司授权（单位）的在下面签字的（被授权人的姓名、职务）为本公司的唯一合法代理人，就项目的投标及合同的执行完成和保修，以本公司名义处理一切与之有关的事务。**被授权人身份证复印件：**

法定代表人（签字或盖章）：

被授权人（签字或盖章）：

投标供应商名称（公章）：

投标供应商地址：

时间：年月日



投标供应商同类项目实施情况一览表

投标供应商全称：

序号	采购单位名称	项目名称	合同金额 (万元)	采购单位联系人及 联系电话	合同（材料） 所在页码	备注
.....						

投标供应商名称（公章）：

法定代表人或授权委托人（签字或盖章）：

时间：



资信及商务响应表

投标供应商全称：标项：

项目	招标文件要求	是否 响应	投标供应商的承诺或说明

投标供应商名称（公章）：

法定代表人或授权委托人（签字或盖章）：

日期：



设备详细配置清单

序号	货物名称	品牌型号	数量	技术规格说明	产地

投标供应商名称（公章）：_____

法定代表人或授权委托人（签字或盖章）：_____

此表可在不改变格式的情况下自行制作

备注：该表需详细填写，置于技术商务文件中，用于技术商务文件评审。



技术规格偏离表

投标供应商名称（盖章）： 采购编号：

序号	招标文件规范要求	投标文件对应规范	是否响应	偏离	说明

注：对每个需求的响应必须遵循如下规则：

- 1、重复该需求；
 - 2、用“是/否”响应来表明该需求是否被满足（描述性需求）；
- 。

投标供应商名称（公章）：

法定代表人或授权委托人（签字或盖章）：

日期：



项目实施人员一览表

序号	姓名	职位	持何种资格证	发证时间	从事本工作时间

注：在填写时，如本表格不适合投标供应商的实际情况，可根据本表格格式自行制表填写



服务质量承诺书

内容要求：

投标供应商根据本项目的工作内容、服务要求、特点等，合理、科学、慎重对以下内容作出承诺：

1、服务承诺：具体服务承诺方案、优惠条件，需详细描述和承诺

2、服务验收标准：

3、本项目考核时应达到的效果和指标：

投标供应商名称（公章）：

法定代表人或授权委托人(签字或盖章)：

日期：

注：格式仅供参考，投标供应商可根据项目实际情况承诺！



价格文件

项目名称：兰溪市中医院数据中心系统项目

项目编号：**jhjp-lxszyy20230310012**

投标供应商名称：（公章）

投标供应商地址：

年月日



价格文件：

- 1： 投标函（格式见附件）；
- 2： 开标一览表（格式见附件）；
- 3： 分项报价表（格式见附件）；
- 4： 其他投标供应商认为有必要提供的资料。



投标函

致：兰溪市中医院

_____（投标供应商全称）授权_____（全名、职务）为全权代表参加贵方组织的_____（招标项目名称、采购编号）招标的有关活动。为此提交下述文件。

1、技术商务投标书；

2、价格投标书；

3、资格证明投标书；

4、其他：

5、据此函，签字代表宣布同意如下：

1) 所附开标一览表中规定的应提供和支付的货物和服务投标总价为(人民币)_____，即_____ (大写)。

2) 投标供应商已详细审查全部招标文件，我们完全理解并同意放弃对这方面有不明及误解的权利。

3) 投标供应商将按招标文件规定履行合同责任和义务。

4) 其投标自开标之日起有效期 90 个日历天。

5) 如果在规定的开标时间后，投标供应商在投标有效期内撤回投标，将接受贵方按政府采购法律、法规进行处罚。

6) 投标供应商同意提供按照贵方可能要求的与其投标有关的一切数据或资料，理解贵方不一定要接受最低价的投标或收到的任何投标。

7) 与本投标有关的一切正式往来通讯请寄：

投标供应商名称(公章)：_____

法定代表人或授权委托人（签字或盖章）：_____

地址：_____ 邮编：_____

电话：_____ 传真：_____

投标日期：_____年____月____日



开标一览表

项目名称	
投标报价 (总价, 元)	(人民币, 小写):
	(人民币, 大写):
质保期	5 年
备注	

投标供应商名称（公章）：_____

法定代表人或授权委托人（签字或盖章）：

日期：_____



分项报价表

序号	产品名称	制造商、产地	品牌	产品型号	单价（元）	数量及单位	小计（元）
.....							
合计（元）							
总计（元）：							

投标供应商名称（公章）：_____

法定代表人或授权委托人（签字或盖章）：

日期：_____



备份电子投标文件/演示文件的密封

备份电子投标文件/演示文件包装封面格式：

备份电子投标文件/演示文件

项目名称：

项目编号：

投标供应商名称：（公章）

投标供应商地址：

法定代表人或授权委托人签字：

在 年 月 日 时 分之前不得启封（开标时间）

年 月 日