



黄石城发工程咨询有限公司

鄂东医养集团网络安全升级续保服务项目

招 标 文 件

项目编号：CFG CZX2026-094

项目名称：鄂东医养集团网络安全升级续保服务项目

招 标 人：湖北鄂东医养集团有限公司

黄石城发工程咨询有限公司

二〇二六年七月

目 录

第一章 招标公告	2
第二章 投标人须知	4
第三章 采购需求及技术要求	9
第四章 评标方法及标准	42
第五章 合同条款	45
第六章 投标文件基本格式	51

第一章 招标公告

黄石城发工程咨询有限公司受湖北鄂东医养集团有限公司的委托，拟对其鄂东医养集团网络安全升级续保服务项目进行公开招标，欢迎符合资格条件的投标单位参加投标。

一、项目概况：

1、项目名称：鄂东医养集团网络安全升级续保服务项目

2、项目编号：CFG CZX2026-094

3、项目内容：对湖北鄂东医养集团本部及下属医疗机构的网络安全设备（包括但不限于防火墙、漏洞扫描、容灾备份、终端杀毒、安全审计等设备）进行系统升级、服务维保、安全运维等内容。具体以第三章“采购需求及技术要求”为准。

4、招标控制价：170 万元。超过本报价为无效报价。

5、免费质保期：原有设备 1 年、新购设备 3 年，自招标人验收通过次日起记（授权未到期项目以到期后重新授权激活验收日为准）。

二、投标人资格要求：

1、投标人须为在中国境内注册的企业，具备有效营业执照，且经营范围须满足本项目实际需求。若投标人为不具备独立法人资格的分公司，须提供总公司（或具有管辖权的上级公司）针对本项目的唯一授权书，经有效授权后，总公司（或上级公司）的资质、资格、业绩等条件均对分公司有效。

2、投标人近三年（2023 年 6 月 1 日至今）至少完成过一例合同金额 150 万元及以上的信息安全项目实施案例，要求提供中标通知书或合同复印件。

3、根据《关于在招标投标活动中对失信被执行人实施联合惩戒的通知》（[2016]285 号）规定，投标人须通过“信用中国”对本企业进行信用查询，若在“失信惩戒对象”名单中的，其投标无效，查询结果以开标当天在“信用中国”网站查询结果为准。

4、投标人近三年内企业无涉及重大资产的不良诉讼，履约情况良好，近三年无重大违法情况（提供没有重大违法记录的书面声明），且目前未处于投标资格被取消状态；

5、本次招标不接受联合体投标。

三、报名登记及招标文件的获取

凡有意参加供应商，请于2026年7月23日至2026年8月12日在黄石市公共资源交易信息网上注册网员，具体操作参见《黄石公共资源交易信息网—办事指南—会员

网上注册指南》，完成网员注册后，通过互联网使用账号密码登录“黄石市其他项目交易系统”，明确所投项目后下载招标文件。

四、投标文件递交截止及开标时间、地点

1、时间：2026年8月13日9时00分整

2、本次项目采取网上递交及网络开标的方式进行(详见招标文件)，截止时间后递交的投标文件不予接收。即投标人在招标文件上规定的截止时间前，将投标文件转换成PDF格式并加密上传到(303183947@qq.com)邮箱。其中投标人递交投标文件时一定要在“邮件主题”上标注参与项目的名称+投标人名称。

3、递交方式：本次项目采取网上递交及网络开标的方式进行(详见招标文件)，由于本次开标采用网络开标，采用的会议软件为“天翼云会议”，请各投标人(即参会人员)提前用带视频功能的手机或电脑下载“天翼云会议”，并提前自行测试，防止意外出现。黄石城发工程咨询有限公司在投标文件递交截止时间后，将本次开标会的会议时间、会议ID及密码以邮件回传给在规定时间内递交了投标文件的投标人的投标邮箱。投标人不要使用163、162邮箱(该类型邮箱下载限速，影响开标进程)，也不要将文件压缩。

五、评标办法

本次招标评标办法采用综合评估法。

六、发布公告的媒介

本次招标公告在黄石市公共资源交易信息网发布

七、联系方式

招标人：湖北鄂东医养集团有限公司 代理机构：黄石城发工程咨询有限公司

地 址：黄石市黄石港区青山桥102号 地 址：开·铁区黄石创业中心A座

邮 编：435000 邮 编：435000

联 系 人：李部长 联 系 人：张工

电 话：13971767274 电 话：0714-6516620/15272050691

2026年7月23日

第二章 投标人须知

投标人须知前附表

条款号	条款名称	编列内容
1	招标人	名称：湖北鄂东医养集团有限公司 联系人：李部长 电话：13971767274
2	招标代理机构	名称：黄石城发工程咨询有限公司 地址：开·铁区黄石创业中心A座 联系人：张工 电话：0714-6516620/15272050691 邮箱：303183947@qq.com
3	招标项目名称	鄂东医养集团网络安全升级续保服务项目
4	项目建设地点	同招标公告
5	项目建设规模	同招标公告
6	资金来源及比例	企业自筹，100%
7	资金落实情况	已落实
8	招标范围	同招标公告
9	服务期限	同招标公告
10	是否接受联合体投标	不接受联合体投标
11	投标人提出书面问题时间	递交投标文件截止之日__10__日前
12	分包	☒ 不允许
13	偏差	☒ 不允许 ☐ 允许，偏差范围：_____ 偏差幅度：_____
14	投标人要求澄清招标文件的时间	递交投标文件截止之日__15__日前

条款号	条款名称	编列内容
15	报价方式	金额报价
16	最高投标限价	☐ 无 ☒ 有，本项目采用金额报价，控制价金额为 1700000 元。 投标人投标报价不能超过招标控制价，否则作废标处理。
17	投标有效期	自投标人提交投标文件截止之日起计算 90 日
18	投标保证金	☒ 不提交
19	退还投标保证金及利息	/
20	履约保证金	☒ 不提交 ☐ 提交，履约保证金的形式： ☒ 银行保函 _____ ☒ 保证保险 _____ ☒ 其他形式 _____ 履约保证金的金额：合同总价的 10 %
21	投标人基本情况表 应附资料	营业执照副本（事业单位法人证书）、资质证书副本（如有）、质量管理体系认证证书（如有）等证件的扫描件
22	近年财务状况的年份要求	近 2 年，即 2023 年至 2024 年或 2024 年至 2025 年
23	近年完成的类似项目情况表 应附资料 and 具体时间要求	提供合同证明的扫描件或复印件（复印件需加盖单位公章）的签字盖章页、签署日期页、合同金额页等关键信息页，并同时提供发票证明、验收证明。
	“类似项目”	近 3 年，即 2023 年 6 月 1 日至投标截止日期前一日 “类似项目”是指：2023 年 6 月 1 日至投标截止日期前一日完成过 1 项合同金额 150 万元及以上的信息安全类项目实施案例
24	是否允许递交备选投标方案	☒ 不允许 ☐ 允许，递交备选投标方案的具体要求_____。

条款号	条款名称	编列内容
25	中标人提供的纸质版投标文件份数	份数： <u>一正二副</u> ，中标人提交的纸质投标文件应当与投标时的电子投标文件内容一致。
26	投标文件递交	1.时间：2026 年 8 月 13 日 9 时整 2.递交方式：网上递交；PDF 格式加密电子投标文件一份；PDF 格式加密投标报价一份；PDF 格式不加密法定代表人身份证明书及法定代表人授权书各一份以及报名费转账记录递交至 303183947@qq.com 邮箱，投标文件递交截至时间后递交的投标文件不予接收，投标文件递交的时间以邮箱收件时间为准。
27	投标文件及份数	PDF 格式加密电子投标文件一份；PDF 格式加密投标报价一份；PDF 格式不加密法定代表人身份证明书及法定代表人授权书各一份，报名费转账记录一份
28	签字和（或）盖章要求	投标文件中提交的相关材料全部按照招标文件要求加盖公章或签字。
29	投标文件邮件标题写明	（投标人名称）“项目名称投标文件”字样；
30	评标委员会的组建	评标委员会构成： <u>5</u> 人，其中招标人代表 <u>1</u> 人，专家 <u>4</u> 人； 评标专家确定方式： <u>从湖北省综合评标专家总库相应专业中随机抽取产生。</u>
31	是否授权评标委员会确定中标人	否，推荐中标候选人数量：3 家。
32	确定中标人的标准	评标委员会根据综合评分情况，确定评审得分最高的投标人为中标人。若评审最高分有并列，确定其中报价得分高的投标人为中标人；若评审最高且报价分最高有并列，确定技术指标优的为中标人。
33	中标公示	在中标通知书发出前，招标人将中标人的情况在黄石市公共资源交易网予以公示，公示期不少于 3 日。
34	开标	投标人在开标规定时间前半小时进入“天翼云会议”会议室，并将称呼改为“XX 公司+姓名”后参与本次视频开标。代理机构在开标前 15 分钟，组建本次开标会微信群，每家投标人的法人授权委托代表“公司名称+姓名”实名进入。具体流程如下： 1. 将开标倒计时投屏至会议界面。 2. 宣布本次开标会开始，强调会议纪律及要求。除主持人和联合主持人会议麦克风打开外，其他参会人员麦克风保持静音，需发言时自行打开。 3. 确认本次开标会有效投标人。如有投标保证金的，将投

条款号	条款名称	编列内容
		<p>标保证金到账和匹配情况投屏至会议界面,确认有效投标人。无投标保证金的,将代理机构企业邮箱打开并投屏至会议界面,根据文件递交截止时间确认有效投标人。</p> <p>4. 下载投标文件。根据投标保证金到账时间顺序或邮箱中邮件递交时间顺序,依次下载投标人投标文件。下载过程全程投屏至会议界面。在此过程中,投标人代表应对下载其投标文件的数量通过微信群确认并告之解密密码。代理机构在本地电脑上新建该项目投标文件夹,再在这个文件夹内建立每家投标人子文件夹,将投标文件下载至此,将投标人代表告之的解密密码标注在对应的文件名上。</p> <p>5. 验证投标人身份。代理机构按顺序逐个打开投标人投标文件,将投标人法人授权委托书页投屏至会议界面,同时对应的投标人代表打开摄像头,左手持本人身份证至头部的左下方,代理机构截屏保存。如无异议,逐个确认及截屏。</p> <p>6. 唱标。代理机构按顺序逐个打开投标人投标文件,将其投标文件中的报价页投屏至会议界面并唱标,投标人代表应在微信群中确认投屏的报价无误。如无异议,逐个唱标。</p> <p>7. 代理机构再次询问各投标人代表,对此次开标会有无异议。如无异议,书面手写开标确认书,附授权委托人身份证原件拍照上传至本次开标会微信群。</p> <p style="text-align: right;">项目开标确认书</p> <p>黄石市城发工程咨询有限公司: 本人对 _____项目的投标、开标和唱标过程无异议。</p> <p style="text-align: right;">(附法人授权委托人身份证原件) XXXX【投标人名称】 (法人授权委托人签名) XXXX 年 X 月 X 日</p> <p>8、宣布开标结束,进入评标程序。</p>
35	投标人参加开标会要求	本项目采取网络开标,投标人无需到开标现场,但法定代表人或授权委托人须携带身份证原件参加网络开标。详见本章“投标人须知正文部分”;
	开标会时间	2026 年 8 月 13 日 9 时 00 分整,本次开标采用不见面开标 (天翼云会议) 软件下载网址: https://cloudmeeting.189.cn/downloadhd.html
36	报名费	<p>本次招标文件资料费 500 元,开标前缴纳至代理机构指定帐户并注明所投标段,售后不退,未缴纳费用文件将不予接收。</p> <p>户名:黄石城发工程咨询有限公司 帐号: 714903123910101 开户行: 招商银行股份有限公司黄石分行营业部</p>
	招标代理服务费	本次招标有招标代理服务费。根据招标人和招标代理机构委托代理合同的约定,本项目招标代理服务费用由中标人支付。

条款号	条款名称	编列内容
		<p>支付标准：招标代理费用按照《湖北省招标代理服务收费参考标准(试行)》(鄂建文(2023)35 号)计取，不足 4000 元按 4000 元计，以上费用中标人应当在中标通知书发出时，向招标代理机构一次性支付；</p> <p>户名：黄石城发工程咨询有限公司</p> <p>帐号：714903123910101</p> <p>开户行：招商银行股份有限公司黄石分行营业部</p>
37	付款方式	<p>1、中标方完成所有续保设备设施授权激活，可向招标人提交验货申请，经招标人验货通过后，招标人向中标方支付合同总价款的 20%。</p> <p>2、中标方完成所有新购设备设施安装完成后，可向招标人提交验货申请，经招标人验货通过后，招标人向中标方支付合同总价款的 20%。</p> <p>3、中标方完成网络安全总体需求调研、实施及系统加固等全部工作，并达到项目验收条件后，可向招标人提交验收申请。经招标人验收通过后，招标人向中标方支付合同总价款的 50%。</p> <p>4、自验收通过次日起进入免费质保期（授权未到期项目以到期后重新授权激活验收日为准），中标方应按要求提供合格网络安全服务（续保设备免费质保期一年，新购设备免费质保期三年），免费质保期满一年后，中标方向招标人开具剩余两年免费质保期等额银行保函（额度为本合同内新购设备设施总价的 10%），同时向招标人提交付款申请，经招标人审核通过后，招标人向中标方支付合同剩余尾款。</p> <p>5、发票要求：招标人每次付款前，中标方均应提供等额、合法、有效的增值税专用发票（新购硬件设备税率 13%，其他部分税率 6%），否则招标人有权顺延付款，且不承担违约责任。</p>

投标人须知正文部分

一、总则

1、项目基本信息

- 1.1 项目概况：见投标人须知前附表；
- 1.2 招标人：见投标人须知前附表；
- 1.3 招标代理机构：见投标人须知前附表；
- 1.4 项目名称：见投标人须知前附表；
- 1.5 项目地点：见投标人须知前附表；

2、招标范围、方式、时间要求及质量要求

- 2.1 项目规模：见投标人须知前附表。
- 2.2 招标范围：见投标人须知前附表。
- 2.3 招标方式：见投标人须知前附表。

2.4 资格审查方式：本项目采用资格后审的方法确定合格投标人，合格投标人必须为能通过资格后审的投标人。投标人须按投标资格证明文件要求提交资格审查资料且不得对招标文件中提供的样本格式内容进行修改，以证明其有符合规定要求的投标合格条件和履行合同的能力。评标委员会将依据资格后审文件的要求，对投标申请人进行资格审查，未通过资格后审的投标人投标文件不予评审，作废标处理。

3、投标人资格要求：

- 3.1 投标人应具备承担本项目的资质条件、能力及信誉，详见招标公告；

3.2 投标人不得存在下列情形之一”

- (1) 为本项目提供招标代理服务的；
- (2) 被责令停业的；
- (3) 被暂停或取消投标资格的（指被本招标项目所在地县级及以上行业主管部门或其他行政主管部门暂停或取消投标资格或禁止进入该区域市场且处于有效期内）；
- (5) 财产被接管或冻结的；
- (6) 在最近三年内有骗取中标或严重违约等重大问题的；

3.3 投标人存在下列情形之一的，相关投标均无效：

- (1) 与招标人存在利害关系影响招标公正性的；
- (2) 法定代表人为同一人或者存在控股、管理关系的不同单位，参加同一标段投标的。

4、投标费用

4.1 投标人在投标过程中的一切费用，不论中标与否，均由投标人自负。凡参加投标者，在黄石市公共资源交易信息网上注册网员并下载招标文件，投标人未按规定下载招标文件的，其投标文件招标人将不予接收。

4.2 招标文件费 500 元，投标人在开标时间之前转账至招标代理机构指定帐户（未交招标文件费的将做无效投标处理），招标代理机构指定银行帐号为：

户名：黄石城发工程咨询有限公司

帐号：714903123910101

开户行：招商银行股份有限公司黄石分行营业部

5、保密

参与招标投标活动的各方应对招标文件和投标文件中的技术等秘密保密，违者应对由此造成的后果承担法律责任。

6、语言文字

除专用术语外，与招标投标有关的语言均使用中文。必要时专用术语应附有中文注释。

7、计量单位

所有计量均采用中华人民共和国法定计量单位。

8、踏勘现场

8.1 投标人自行踏勘现场。

8.2 投标人踏勘现场发生的费用自理。

8.3 除采购人的原因外，投标人自行负责在踏勘现场中所发生的人员伤亡和财产损失。

8.4 投标人在踏勘现场中了解的情况，仅供投标人在编制投标文件时参考，采购人不
对投标人据此作出的判断和决策负责。

9、分包

除投标人须知前附表另有规定外，本招标项目不允许分包。

二、招标文件

10、招标文件的组成

10.1 招标文件除以下内容外，招标人在招标期间发出的答疑、纪要和其它补充修改函件等，均是招标文件的组成部分，对投标人起约束作用。

招标文件包括下列主要内容：

- （1）招标公告；
- （2）投标人须知；
- （3）项目概况及要求；
- （4）评标办法；
- （5）合同条款及格式；
- （6）投标文件格式；
- （7）其他补充文件。

10.2 投标人购取招标文件后，应仔细检查招标文件的所有内容，如有残缺应在领到招标文件后 2 日内向招标人提出，否则，由此引起的投标损失自负；投标人同时应认真审阅

招标文件中所有的事项、格式、条款和规范要求等，如果投标人的投标文件没有按照招标文件要求提交全部资料或者投标文件没有对招标文件做出实质性响应，其风险应由投标人自行承担并根据有关条款规定，其投标有可能被拒绝。

10.3 发售招标文件的时间及地点见投标人须知前附表。招标文件售价见投标人须知前附表。

10.4 招标文件的澄清、修改、答疑

10.4.1 招标人对已发出的招标文件确需进行澄清或者修改的，应当在招标文件规定的提交投标文件截止时间至少 15 日前，以书面形式在黄石市公共资源交易网通知所有招标文件收受人。

10.4.2 不论招标人以书面形式向投标人发出的任何资料文件，还是投标人以书面形式提出的任何问题，均应以书面形式予以签收确认。任何口头上的修改、澄清、答疑一律视为无效。

10.4.3 当招标文件、修改补充通知、澄清、答疑内容相互矛盾时，以最后发出的修改补充通知、澄清、答疑或修改文件为准。

10.4.4 为了使投标人在编制投标文件时，充分响应招标文件的修改、澄清及答疑的内容，招标人可根据情况适当延长提交投标文件的截止时间，并在补充文件中明确。

三、投标文件

11、投标文件的组成

11.1 投标人编写的投标文件应包括但不少于下列部分，投标人保证所提供的全部资料真实可靠，对其提交的全部资料的真实性、合法性承担法律责任，并接受招标代理机构对其中任何资料进一步核实的要求。

11.1.1 投标文件目录；

11.1.2 投标资格审查文件；

11.1.3 投标函；

11.1.4 投标报价表；

11.1.5 投标人业绩证明材料

11.1.6 招标文件要求提供或投标人认为需要提供的其它材料。

12、投标报价

投标报价是指招标文件中说明的全部工作范围以及内容的报价。

投标人投标函中的大写报价或投标报价（算术错误修正后的报价）大于招标控制价的，其投标将被否决。

13、投标有效期

13.1 自投标文件截止时间起至投标人须知前附表规定的时间内。凡符合本招标文件要求的投标文件均有效。

13.2 特殊情况下，在原投标有效期截止之前，招标代理机构或招标人可要求投标人延长投标有效期。这种要求与答复均应以书面形式提交，投标人可拒绝招标代理机构或招标人的这种要求，其投标保证金可以被退还，但其投标在原投标有效期期满后将不再有效。同意延长投标有效期的投标人将不会被要求和允许修正其投标，而只会被要求相应地延长其投标保证金的有效期。在这种情况下，有关投标保证金的退还规定将在延长了的有效期内继续有效。

14、投标保证金

14.1 投标人须知前附表规定提交投标保证金的，投标人在递交投标文件的同时，应按投标人须知前附表规定的形式、金额、递交截止时间、递交方式提交投标保证金，并作为其投标文件的组成部分。联合体投标的，其投标保证金由牵头人递交，并应符合投标人须知前附表的规定。

14.2 投标人不按招标文件要求提交投标保证金的，其投标将被否决。

14.3 招标人最迟在与中标人签订合同后 5 日内，向未中标的投标人和中标人退还投标保证金。招标人同时退还投标保证金的银行同期存款利息。投标保证金及利息的计息标准和退还方式见投标人须知前附表。

14.4 有下列情形之一的，投标保证金将不予退还：

- (1) 投标人在规定的投标有效期内撤销或修改其投标文件；
- (2) 中标人在收到中标通知书后，无正当理由拒签合同、在签订合同时向招标人提出附加条件或未按招标文件规定提交履约保证金。

15、履约保证金

中标人须向招标人提交履约保证金。履约保证金在合同履行完成后退还中标人，不计利息，履约保证金退还时按来款渠道退回。

16、投标文件的编制

16.1 投标人应当对投标文件逐页标注页码并编制详细目录

16.2 投标人应完整地填写招标文件中提供的《投标函》、《报价一览表》等招标文件中规定的所有内容。

16.3 投标人必须保证投标文件所提供的全部资料真实可靠，并接受招标方对其中任何资料进一步核实的要求。

16.4 如果因为投标人投标文件填报的内容不详，或没有提供招标文件中所要求的全部资料及数据，由此造成的后果，其责任由投标人承担。

16.5 因本次招标采用电子开标，所有投标人的投标文件须按上述要求制作完成后，扫描成加密的 PDF 文档，密码在网络开标时（视频会议方式）提供进行现场解密。

17、投标文件的数量和签署

17.1 投标人应编制 PDF 格式电子投标文件一份。

17.2 投标文件须按招标文件要求盖章。

17.3 中标人须按招标人要求提供纸质版投标文件。

四、投标

18、投标文件的送达

18.1 投标人应将 PDF 格式的电子投标文件按规定时间发送至指定邮箱，如果电子投标文件未按要求发送的，其投标文件视为无效投标。

19、投标文件递交截止时间

19.1 投标人须在投标人须知前附表规定的投标文件递交截止时间前发送成功电子投标文件。在本招标文件规定的投标文件递交截止时间后收到的，招标人将视为无效投标。

19.2 招标人将按投标须知前附表规定的时间准时开标。

20、投标文件的补充、修改与撤回

20.1 投标人在投标人须知前附表中规定的投标截止时间前，可以补充、修改或者撤回已提交的投标文件。补充、修改的内容作为投标文件的组成部分，应当按本招标文件的规定进行编制、标志（在文件标题上标明“修改”或“撤回”字样，并注明修改或撤回的时间）、发送和保管。

20.2 在投标截止时间之后，投标人不得补充、修改投标文件。

五、开标、评标、定标

21、开标

本项目开、评标流程会有所调整，但整个开标过程会按照公开、公平、公正、诚实的原则进行。开、评标时，请投标人的联系人务必保持手机畅通、网络通畅、有可操作的办公电脑，以确保在开、评标过程中，招标代理机构可以随时联系到投标人。因投标人自身原因在开、评标过程中造成的一切后果，均由投标人自行负责。

21.1 开标会由招标代理机构主持，按投标人须知前附表规定的开标时间和方式进行，届时将采用“天翼云会议”软件，以网络开标的方式进行开标直播，并在开标时间接收投标人加密电子投标文件（PDF 格式）的解密密码，进行开标。请各投标人的法定代表人或授权委托人准备好身份证原件，以便在开标时招标人对其进行身份核实。

注：请各投标人（即参会人员）提前用带视频功能的手机或电脑下载“天翼云会议”软件，并将“您的名称”改为“XX 公司+姓名”参与本次视频开标（请提前自行测试，防止出现意外）。投标人进入“天翼云会议”的会议 ID、会议密码等，主持人在开标前 30 分钟发送至各投标人用以投标的邮箱，请各投标人关注，如邮箱内未收到相关信息请及时与招标代理公司联系。开标前代理机构建项目开标微信群，群号会发送至各投标人投标邮箱。

21.2 本次开标具体流程为：

21.2.1 2026 年 月 日 08 时 30 分进入“天翼云会议”；

21.2.2 2026 年 月 日 09 时截止投标，并将招标人接收投标文件的收件邮箱投屏，用

以公布各投标人投标文件递交的情况；（投标人递交至招标人邮箱的电子文件共四份：1、PDF 格式加密电子投标文件一份；2、PDF 格式加密电子投标报价表一份；3、未加密 PDF 格式法定代表人证明书及法定代表人授权委托书电子文件（原件扫描件）一份 4、报名费缴纳凭证。加密文件请使用同样的密码。

21.2.3 招标人验证投标人代表身份，以及明确相关事宜（是否存在异议）；

21.2.4 投标人协助招标代理机构明确自己的投标文件，由招标代理机构下载至本地文件夹，并标注；

21.2.5 投标文件全部下载完成后，招标代理机构将按照投标文件递交的顺序依次请投标人提供电子文件的解密密码；

21.2.6 唱标人依次解密电子文件并进行唱标；

21.2.7 唱标结束后，主持人将在微信群里发送“开标确认书”，用以让各投标人确认各自唱标结果无误并对整个开标流程无异议。请各投标人准备 A4 白纸，手写或打印“开标确认书”后签字，拍照上传至微信群。

开标确认书格式为：

_____项目开标确认书

黄石城发工程咨询有限公司：

本人对_____项目的投标、开标和唱标过程无异议。

（附法人授权委托书身份证原件）

XXXX【投标人名称】

（法人受权委托人签名）

XXXX 年 X 月 X 日

21.2.8 主持人宣布开标结束，进入评标程序。

21.3 招标人对开标过程进行记录，开标结束后，由招标人进行签字确认，并存档备查。

21.4 在开标时，当投标文件出现下列情形之一的，为无效投标文件，招标人不予受理，作废标处理：

21.4.1 投标文件未按招标文件要求递交或撤回的。（投标人递交投标文件的时间以招标代理指定收件邮箱收到邮件的时间为准。）

21.4.2 投标文件格式未按照招标文件的要求的。

22、评标

22.1 评标委员会

评标委员会的组成：评标委员会依照有关法律法规组建，负责评标活动。评标委员会由招标人代表一名和评审专家四名共五人组成。评标委员会负责人(评委组长)由评标委员

会成员推荐产生。

评标过程的保密：开标后，直至授予中标人合同为止，凡属于对投标文件的审查、澄清、评价和比较有关的资料以及中标候选人的推荐情况、与评标有关的其他任何情况均严格保密。中标人确定后，招标人不对未中标人就评标过程以及未能中标原因作出任何解释。未中标人不得向评标委员会成员或其他有关人员索问评标过程的情况和材料。

22.2 投标文件初步评审

22.2.1 经审查符合本须知有关规定的投标文件，提交评标委员会进行初步评审。

22.2.2 初步评审包括对投标文件的符合性评审、投标文件计算错误的修正。

22.2.3 符合性评审是指评标委员会审查每一投标文件是否对招标文件提出的所有实质性要求和条件作出响应，有无显著的差异或保留。未能在实质上响应的投标，应作废标处理。

22.2.4 评标委员会按规定否决不合格投标或者界定为废标的投标文件不再进入详细评审。

22.2.5 投标文件计算错误的处理

投标文件中的大写金额与小写金额不一致时，以大写金额为准，总价金额与单价金额不一致时，以单价金额为准，除非评标委员会认为单价有明显的小数点错误，此时应以合价为准，并修改单价。对不同文字文本投标文件的解释发生异议时，以中文文本为准。

按上述修正错误的原则及方法调整或修正投标文件的投标报价，投标人同意后，调整后的投标报价对投标人起约束作用。如果投标人不接受修正后的报价，则按废标处理。

22.3 评标委员会在评审过程中，投标文件有下列情形之一的，由评标委员会审定后，作为废标处理：

22.3.1 委托代理人没有合法有效委托书原件；

22.3.2 投标文件中未提供有效资格证明材料、企业资质证书、组织机构代码证（或三证合一）等；

22.3.3 投标文件未按招标文件要求加盖投标人公章及法定代表人（或法定代表人授权的单位负责人）或委托代理人未签字或盖章的；

22.3.4 投标人未按招标文件的要求缴纳投标保证金的；

22.3.5 投标文件投标报价高于招标控制价的；

22.3.6 不同投标人的投标文件相互混装的；

22.3.7 不同投标人的投标保证金从同一单位或者个人账户转出的；

22.3.8 其他不符合资格后审要求的；

22.4 详细评审

详细评审按第四章“评标办法”执行。

23、投标文件澄清

23.1 在评标过程中，在招标投标监督人员在场的情况下，评标委员会可以用书面形式要求投标人对投标文件中含义不明确，对同类问题表述不一致或者有明显文字和计算错误的内容作必要的澄清、说明或者补正。投标人应在评标结束前用书面形式进行澄清、说明或者补正，其澄清、说明或者补正内容，不得超出投标文件范围或者改变投标价格等实质性内容。澄清方式为网络方式并录像。

23.2 书面答复须经投标人法定代表人或其委托代理人签字或盖章，签字或盖章的书面答复将视为投标文件的组成部分（以邮件方式递交）。提交投标文件截止时间后，投标人对投标报价或其他实质性内容修正的函件和增加的任何优惠条件，一律不得作为评标、定标的依据。

23.3 在投标文件的审查、澄清、评价和比较以及合同签订过程中，投标人对招标人或招标代理机构和评标委员会成员施加影响的任何行为，都将导致取消其中标资格。

24、 定标

24.1 招标人授权评标委员会确定评标排序第一的中标候选人为中标人。

24.2 评标委员会在评标过程中，评标委员会否决不合格投标或者界定为废标后因有效投标人不足 3 个的，可以继续评标；

24.3 完成评标后，评标委员会根据综合评分情况，确定评审得分最高的投标人为中标人。若评审最高分有并列，确定其中报价分最高的投标人为中标人；若评分最高且报价分最高有并列，确定技术指标优的为中标人，并编写评标报告。

24.4 中标人的经营、财务状况发生较大变化或者存在违法行为，招标人认为可能影响其履约能力的，应当在发出中标通知书前由原评标委员会按照招标文件规定的标准和方法审查确认。

24.5 招标人自收到评标报告之日起 3 日内，在投标人须知前附表规定的媒介上公示中标人，公示期不少于 3 日历天。

24.6 投标人或者其他利害关系人对评标结果有异议的，可在公告期届满之日起 3 日内提出，招标人自收到异议之日起 3 日内作出答复。异议与答复应采取书面形式。质疑书应当包括下列主要内容：

质疑人的名称、地址、电话等；质疑人法人签章和单位公章；具体的质疑事项和请求；与质疑事项相关的证明材料；提起质疑的日期。

24.7 中标通知

评标结果公示期满后，无投标人或者其他利害关系人投诉，或者投诉处理完毕的，在本章规定的投标有效期内，招标人以书面形式或电子文件形式向中标人发出中标通知书。

六、合同授予

25、合同的签订

25.1 招标人将按照评标委员会推荐的中标候选人，依排名顺序依次确定中标人。排名

第一的中标候选人放弃中标、因不可抗力提出不能履行合同、或在规定的时间内因自身原因未能与采购人签订合同，招标人可以确定排名第二的中标候选人为中标人。排名第二的中标候选人因上述的同样原因不能签订合同的，招标人可以确定排名第三的中标候选人为中标人；招标人也可以重新招标。

25.2 签约合同价的确定原则如下：

投标报价表中的投标报价为签约合同价。

25.3 中标人在收到中标通知书后三十日内与招标人签订服务合同。

25.4 中标人无正当理由不签订合同的，招标人有权取消其中标资格并没收投标保证金，给招标人造成的损失超过投标保证金数额的，应当对超过部分给予赔偿。

26、 重新招标、不再招标和终止招标

26.1 重新招标

有下列情形之一的，招标人将重新招标：

- (1) 投标文件递交截止时间止，投标人少于 3 个的；
- (2) 经评标委员会评审后否决所有投标的。
- (3) 除非已经产生中标候选人，在投标有效期内同意延长投标有效期的投标人少于 3 个的；
- (4) 所有中标候选人均未与招标人签订合同的；
- (5) 法律、法规规定的其他情形。

26.2 终止招标

因不可抗力等原因，招标人终止招标的，将及时发布公告，或者以书面形式通知被邀请的或者已经获取招标文件的潜在投标人。

27、纪律和监督

27.1 对招标人的纪律要求

招标人不得泄漏招标投标活动中应当保密的情况和资料，不得与投标人串通损害国家利益、社会公共利益或者他人合法权益。

27.2 对投标人的纪律要求

投标人不得相互串通投标或者与招标人串通投标，不得向招标人或者评标委员会成员行贿谋取中标，不得以他人名义投标或者以其他方式弄虚作假骗取中标；投标人不得以任何方式干扰、影响评标工作。

27.3 对评标委员会成员的纪律要求

评标委员会成员不得与任何投标人或者与招标结果有利害关系的人进行私下接触，不得收受投标人、中介人、其他利害关系人的财物或者其他好处，不得向他人透漏对投标文件的评审和比较、中标候选人的推荐情况以及评标有关的其他情况。在评标活动中，评标委员会成员不得应当回避而不回避，不得擅离职守，影响评标程序正常进行，不得向招标

人征询其确定中标人的意向，不得接受任何单位或者个人明示或者暗示提出的倾向或者排斥特定投标人的要求，不得对依法应当否决的投标不提出否决意见，不得暗示或者诱导投标人作出澄清、说明或者接受投标人主动提出的澄清、说明；不得使用第四章“评标办法”没有规定的评审因素和标准进行评标。

27.4 对与评标活动有关的工作人员的纪律要求

与评标活动有关的工作人员不得收受他人的财物或者其他好处，不得向他人透漏对投标文件的评审和比较、中标候选人推荐情况以及评标有关的其他情况。在评标活动中，与评标活动有关的工作人员不得擅自离职守，影响评标程序正常进行。

27.5 投诉

本次招标投标活动及其相关当事人应当接受有关行政监督部门依法实施的监督。

投标人和其他利害关系人认为本次招标活动违反法律、法规和规章规定的，有权自知道之日起 10 日内向有关行政监督部门投诉，其中对招标文件的内容（包括招标控制价）、开标、评标结果进行投诉的，应当按本章的规定先向招标人提出异议后，方可向有关行政监督部门投诉，异议答复期不计算在规定的投诉时效期限内。投标人和其他利害关系人的投诉应按照规定进行。

第三章 采购需求及技术要求

一、升级续保部分

序号	产品名称	产品型号	单位	数量	技术要求	系统授权到期时间	备注
1、黄石市第二医院网络安全升级续保清单							
1	绿盟防火墙	NFNX3-HD4100	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-9-29	
2	绿盟防火墙	NFNX3-HD4100	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-12-29	
3	绿盟防火墙	NFNX5-HD6300	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-9-29	
4	绿盟防火墙	NFNX5-HD6300	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-9-29	
5	绿盟防火墙	NFNX3-HD4100	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-12-29	
6	绿盟防火墙	NFNX3-HD4100	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-9-29	
7	绿盟防火墙	NFNX5-HD6300	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-9-30	
8	绿盟防火墙	NFNX5-HD6300	套	1	包含 IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-9-30	
9	绿盟网络安全漏洞扫描系统	RSASNX3-X	套	1	包含系统+web 漏洞特征库模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2026-1-15	
10	天融信数据库审计	TopAudit	台	1	可进行软件升级、硬件维修、特征库、规则库升级等。	2026-5-23	

11	EDR (DMZ 区)	TopEDR (V1.0.2.2 .14)	套	1	<p>(1) 服务管理端要求: 1 个 Windows Server 系统 1 年服务 (外网), 包含: 硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>(2) 服务器客户端要求: 防病毒功能授权, 含升级许可。支持基因识别、虚拟沙盒等引擎, 可以精准查杀勒索、木马、蠕虫等各类病毒; 提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持 Windows, 支持远程桌面功能。</p> <p>(3) PC 客户端要求: 防病毒功能授权, 含升级许可。支持基因识别、虚拟沙盒等引擎, 可以精准查杀勒索、木马、蠕虫等各类病毒; 提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持 Windows, 支持远程桌面功能。</p>	2025-11-13	
12	EDR (内网 区)	TopEDR (V1.0.2.2 .14)	套	1	<p>(1) 服务管理端要求: 1 个 Windows Server 系统 1 年服务 (外网), 包含: 硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>(2) 服务器客户端要求: 防病毒功能授权, 含升级许可。支持基因识别、虚拟沙盒等引擎, 可以精准查杀勒索、木马、蠕虫等各类病毒; 提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持 Windows, 支持远程桌面功能。</p> <p>(3) PC 客户端要求: 防病毒功能授权, 含升级许可。支持基因识别、虚拟沙盒等引擎, 可以精准查杀勒索、木马、蠕虫等各类病毒; 提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持 Windows, 支持远程桌面功能。</p>	2025-11-13	
13	信服易备容灾备份	XS-ES2Z	台	1	<p>(1) 硬件维保: 原厂备件更换服务 (7×24 小时响应, 4 小时内到场)。</p> <p>(2) 软件支持: 信服易备系统版本升级、补丁更新及技术服务。</p> <p>(3) 定期巡检: 每季度 1 次现场巡检, 包含设备健康检查、性能优化建议等。</p>	2025-10-29	
14	信服易备容灾备份	XS-ES4T	台	1	<p>(1) 硬件维保: 原厂备件更换服务 (7×24 小时响应, 4 小时内到场)。</p> <p>(2) 软件支持: 信服易备系统版本升级、补丁更新及技术服务。</p> <p>(3) 定期巡检: 每季度 1 次现场巡检, 包含设备健康检查、性能优化建议等。</p>	2025-10-29	

15	集团 DMZ 区千兆防火墙	深信服 AF-1000 B1300	台	1	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。（已开通应用控制、漏洞攻击防护、僵尸网络、内容安全等基础安全功能，云脑-云智最新威胁防御规则库订阅服务 云脑-云鉴未知威胁与杀毒订阅服务等）	2025-11-30	
16	集团 DMZ 区千兆防火墙	深信服 AF-1000 B1300	台	1	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。（已开通应用控制、漏洞攻击防护、僵尸网络、内容安全等基础安全功能，云脑-云智最新威胁防御规则库订阅服务 云脑-云鉴未知威胁与杀毒订阅服务等）	2025-11-30	
17	集团 DMZ 区 WAF 防火墙	深信服 WAF-1000 B1400	台	1	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。	2025-12-5	
18	外网上网行为管理	深信服 AC-1000 B1100	台	1	包含：软件升级、硬件维修、应用识别、URL 库升级、上网安全授权等。	2025-10-12	

2、黄石市第四医院网络安全升级续保清单

1	EDR（内网区）	TopEDR (V1.0.2.2 .14)	套	1	<p>（1）服务管理端要求：1 个 Windows Server 系统 1 年服务（外网），包含：硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>（2）服务器客户端要求：防病毒功能授权，含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持 Windows，支持远程桌面功能。</p> <p>（3）PC 客户端要求：防病毒功能授权，含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持 Windows，支持远程桌面功能。</p>	2025-11-11	
2	信服易备容灾备份	XS-ES8T	台	1	<p>（1）硬件维保：原厂备件更换服务（7×24 小时响应，4 小时内到场）。</p> <p>（2）软件支持：信服易备系统版本升级、补丁更新及技术咨询服务。</p> <p>（3）定期巡检：每季度 1 次现场巡检，包含设备健康检查、性能优化建议等。</p>	2025-10-29	

3	深信服外网出口防火墙	AF 8.0.26	台	1	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。	2025-12-1	
4	深信服内网出口防火墙	AF 8.0.26	台	1	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。	2025-12-1	

3、黄石市第五医院网络安全升级续保清单

1	EDR（内网区）	TopEDR（V1.0.2.2.14）	套	1	<p>（1）服务管理端要求：1个Windows Server系统1年服务（外网），包含：硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>（2）服务器客户端要求：防病毒功能授权，含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p> <p>（3）PC客户端要求：防病毒功能授权，含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p>	2025-11-16	
2	数据库审计	TopAudit	台	1	可进行软件升级、硬件维修、特征库、规则库升级等。	2026-5-23	
3	信服易备容灾备份	XS-ES2T	台	1	<p>（1）硬件维保：原厂备件更换服务（7×24小时响应，4小时内到场）。</p> <p>（2）软件支持：信服易备系统版本升级、补丁更新及技术服务。</p> <p>（3）定期巡检：每季度1次现场巡检，包含设备健康检查、性能优化建议等。</p>	2025-10-29	

4、黄石市十五冶医院网络安全升级续保清单

1	信服易备容灾备份	XS-ES8C	台	1	<p>（1）硬件维保：原厂备件更换服务（7×24小时响应，4小时内到场）。</p> <p>（2）软件支持：信服易备系统版本升级、补丁更新及技术服务。</p> <p>（3）定期巡检：每季度1次现场巡检，包含设备健康检查、性能优化建议等。</p>	2025-10-29	
2	深信服网络防火墙	AF-1000 B1200	台	1	包含IPS+防病毒模块，可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。	2025-12-2	

备注：涉及序列号等信息的，中标后提供。

二、新增采购部分（交付硬件设备须为 2026 年 1 月 1 日（含）以后出厂的新品，提供《6-1 新购设备承诺函》，否则该设备所涉的所有技术规格及性能参数，在评审时一律按无效响应处理。）

5、鄂东医养集团数据中心网络安全升级加固新增

序号	设备名称	指标	技术要求	备注
1	下一代防火墙（2 台）	硬件配置	≥1U 机型，含交流冗余电源，≥1*RJ45 串口，≥1*RJ45 管理口，≥2*USB 接口，10*GE 电口（含 2 对 Bypass），≥4 个 combo 口，≥2 个接口扩展槽位，1T 国产固态硬盘，SFPP 万兆多模光纤接口模块，≥2*10GE 接口（300M,850nm,LC 接口，含原厂光模块），≥2 个万兆 SFPP 插槽整机吞吐量≥8G（含原厂多模万兆光模块），应用层吞吐量≥1G,最大并发连接数≥50 万,新建连接数≥2 万。防病毒模块，入侵防护模块，含传统防火墙、流量管理、IPSec VPN。	
		功能要求	支持虚拟线，二层透明，三层，混合，旁路监听，单臂接入方式。	
			支持三层接口、三层子接口、环回接口、VPN 接口。	
			▲支持工业系统类应用协议识别，例如：OPC、EC、MODBUS、航天云网-NDICS、FOCAS、PCWORX 等工控协议；物联网类应用协议识别，例如：西门子 MindSphere 平台、GB/T32960、JT808、JT809、JT905、CoAP、小米 N 音响、米家小白智能摄像机、Yeelight。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告，并加盖原厂公章。	
			▲针对防火墙策略，支持基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟流量报文的处理计算，获得策略的命中信息，并可对命中的策略信息进行编辑，实现防火墙策略命中情况的仿真模拟测算。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告，并加盖原厂公章。	
			▲支持对非 IP 协议类型的流量进行访问控制，例如 IPX、Apple Talk。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告，并加盖原厂公章。	
			▲支持对基于 HTTP、FTP、POP3、SMTP、IMAP 协议的多线程下载行为，以及有密码的压缩包进行下载限制。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告，并加盖原厂公章。	
			▲策略可按匹配顺序、策略分组、新建顺序、安全区分组等不同维度的查看方式，在按匹配顺序查看下，可以通过拖拽实现优先级的调整，也可以输入具体的策略序号、置顶或者置底等方式进行调整。提供功能截图并加盖原厂公章。	
			提供基于源/目的 IP 地址、安全区、应用、应用组、协议/端口、时间、安全模板的精细粒度的安全访问控制，时间精确到秒级。	
			▲支持对应用进行二级分类，类型包括媒体类、协作类、一般网络应用、商业系统等，子类包括音频流、游戏、普通商业、工业系统、物联网、文件传输、知名网站、即时通信、图片视频、社	

2	WAF 防火墙 (2 台)		交网络等，提供功能截图并加盖原厂公章。	
			支持内置/自定义 ISP 路由库，实现 ISP 链路间路由负载均衡。	
		质保服务	含 3 年规则升级及原厂服务。	
		厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件。	
			厂商需具备符合 ISO 22301:2019 标准的业务连续性管理体系认证证书，提供有效证书的厂商盖章复印件。	
			厂商具备中国电子信息行业联合会颁发的《信息系统建设和服务能力评估资质证书-CS4 级别》，提供有效证书的厂商盖章复印件。	
		产品资质	产品厂商具备中国软件评测中心和中国计算机行业协会数据安全专业委员会联合颁发的《数据安全服务能力评定资格证书》（数据安全评估二级），提供有效证书的厂商盖章复印件。	
			为保证数据的安全与可靠，产品厂商应具备《隐私信息管理体系认证》证书，提供有效证书的厂商盖章复印件。	
			产品具备《多核分布式安全操作系统》，提供有效证书的厂商盖章复印件。	
		硬件配置	≥2U, 含交流冗余电源模块, ≥2*USB 接口, ≥1*RJ45 串口, ≥2*GE 管理口。≥6*GE 电口 (BYPASS), ≥4*千兆光口 (含原厂千兆多模光模块), ≥2 个接口扩展插槽位, 硬盘 4T, 2 个万兆 SFP 插槽, 支持万兆多模光纤接口模块、万兆单模光纤接口模块。整机吞吐量 10Gbps。	
		功能要求	▲支持紧急模式：支持配置 CPU 使用率、内存使用率、并发连接数阈值，当 CPU 使用率，内存使用率或并发连接数超过设置阈值时，WAF 自动进入紧急模式，已经代理的连接正常代理，对新增的请求直接转发；当恢复到阈值以内时，自动退出紧急模式。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告，并加盖原厂公章。	
			部署灵活，支持透明桥部署，串联部署，路由旁路部署，镜像模式，反向代理模式以及插件式等部署模式	
			▲会话追踪，通过浏览器标识和会话标识实现对会话的跟踪，记录完整的黑客攻击过程，做到场景复现。提供第三方测试报告，以及功能截图并且加盖厂家公章	
			▲支持对 XML 文件进行基础合规检测，覆盖“节点个数、节点深度、节点名称长度”等；支持基于自定义的 schema 文件对 XML 文件进行更加细致的合规检测，能根据定义好的 schema 文件检测节点类型、属性类型等。支持基于 WSDL 文件来检测 webservicess 请求的 soap 流量是否符合规则。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告，并加盖原厂公章。	

			<p>▲支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell 及 Ruby shell，同时可支持源 IP 封禁、Session 封禁和 UA 封禁。提供功能截图并且加盖厂家公章</p>	
			支持非法下载防护，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等）。	
			支持暴力破解防护，支持 GET/POST 两种请求方法检测；支持 Form/Ajax/JsonP 三种验证方式；支持验证码机制，可有效防止误报。	
			支持 Cookie 安全机制，通过 cookie 加密或 cookie 签名的方法对访问服务器后保留在客户端的 cookie 进行安全防护。	
		质保服务	含 3 年规则升级及原厂服务。	
		产品资质	产品厂商具备中国软件评测中心和中国计算机行业协会数据安全专业委员会联合颁发的《数据安全服务能力评定资格证书》（数据安全评估二级），提供有效证书的厂商盖章复印件。	
			为保证数据的安全与可靠，产品厂商应具备《隐私信息管理体系认证》证书，提供有效证书的厂商盖章复印件。	
			参与起草了《信息安全技术 WEB 应用防火墙安全技术要求与测试评价方法》GB/T 32917-2016，提供截图证明。	
		厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件。	
			厂商需具备符合 ISO 22301:2019 标准的业务连续性管理体系认证证书，提供有效证书的厂商盖章复印件。	
			厂商具备中国电子信息行业联合会颁发的《信息系统建设和服务能力评估资质证书-CS4 级别》，提供有效证书的厂商盖章复印件。	
3	零信任安全系统（1 台）	硬件配置	性能参数：要求产品采用国产 cpu,支持国产操作系统；SSL 加密流量（Mbps）≥300，并发用户数（个）≥600；IPSEC 加密最大流量（Mbps）≥100，IPSEC 理论并发隧道数（Tunnel）≥1000；硬件参数：规格：1U，内存≥16G，硬盘容量≥128G SSD，接口≥6 千兆电口，≥4 千兆光口 SFP（含原厂千兆多模光模块）。售后服务：提供≥3 年原厂维保服务。	
		软件授权	要求提供零信任接入授权数量≥200 套，零信任访问控制管理系统软件授权数量≥1 套，安全沙箱授权数量≥200 套。	

功能要求		<p>身份认证：为满足身份安全要求，应支持多因素认证，至少包括：账号密码认证、短信认证、证书认证、动态令牌认证、扫码认证，以及对接统一认证平台实现单点登录等认证方式。可配置的异常环境包括但不限于：账号首次登录、账号在该终端首次登录、闲置账号登录、弱密码登录、异常时间登录、非常用地点登录等。</p>	
		<p>权限及访问控制：为满足组织灵活的管理要求，支持配置动态访问规则，可配置化的 ACL 规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置，针对不同操作系统设定单独或多系统访问控制策略。动态访问控制策略支持“与”、“或”条件嵌套，并可通过单一条件或条件组的方式灵活组合嵌套，可支持多种条件变量设置，当检测到不符合安全条件时，支持如短信增强认证、告警等灵活的补救动作，实现灰度处置，有效平衡员工访问体验和安全保障</p>	
		<p>DNS 解析：支持以私有 DNS 发布企业资源，无需额外购买 DNS 服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有 DNS 解析地址。</p>	
		<p>客户端自动选路：为了提升终端用户访问体验，对于多线路接入单网关访问业务的场景，支持时延优先的选路模式，支持周期性探测线路时延和多次探测确认恶化后切换。多网关接入访问业务的场景，支持最低时延+相对时延阈值随机选择策略。（需提供产品功能截图证明）</p>	
		<p>沙箱场景配置：▲沙箱功能应支持通过功能配置的变更，适配对应使用环境和场景： 1）支持在互联网办公 PC 对隧道应用的网络访问进行权限隔离，仅通过沙箱空间允许对隧道应用的访问和数据留存加密。 2）支持在内网办公 PC 对互联网网络访问进行权限隔离，仅通过上网沙箱应用进行互联网访问。（需提供产品功能配置截图）</p>	
		<p>PC 端沙箱：▲为了满足 PC 端数据防泄密需求，零信任平台需支持在 PC 终端上基于沙箱技术生成隔离的安全工作空间（非容器类型），且无需再额外搭建服务端设备、组件。PC 沙箱应支持统信 UOS、麒麟 Kylin 等主流系统。（需提供公安部计算机信息系统安全产品质量监督检验中心出具的检测报告）</p>	
		<p>沙箱文件加密：▲支持以文件为单位，对工作应用产生的数据进行加密保存；文件加密支持“一文一密”即每个文件独立密钥，以确保沙箱组件被卸载、模块驱动被摘除的情况下，终端用户仍无法明文取出文件。（需提供第三方权威检测机构出具的带 CNAS 标识的检测报告证明）</p>	
		<p>SPA 单包授权：▲为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持 UDP+TCP 组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口。安全码支持共享码和一人一码及一次一码三种模式，可通过短信分发安全码。一人一码模式下，当实际登录用户跟分发 SPA 安全码绑定的用户不一致时，零信任系统可以产生安全告警。一次一码模式下激活码被用户使用并正常登录零信任系统后转换为安全</p>	

			码加密存储，换码成功后激活码失效，控制台日志须体现用户首次登录后的换码过程。（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）	
		质保服务	含 3 年规则升级及原厂服务。	
		产品资质	提供国家版权局颁发的含有“零信任”字样的《计算机软件著作权登记证书》（需提供有效证明材料并加盖公章）	
			无漏洞证明： 为证明所投产品的自身安全性，应具备国家计算机网络应急技术处理协调中心出具的安全众测无漏洞证明文件。（需提供有效证明材料并加盖公章）	
			所投零信任产品应在《IDC 中国零信任网络访问解决方案市场份额，2024》中位列前茅，并出具由 IDC 盖章确认的证明文件，	
		厂商资质	厂商为国家信息安全漏洞共享平台（CNVD）用户组及技术组成员单位	
4	应用、数据容灾备份安全防护系统（5 套）	配置要求	▲支持黄石市第二、四、五、十五冶医院现用灾备系统，完全兼容，实现有效网络安全防护。	需包含现场网络安全服务
		功能要求	内置勒索病毒、挖矿、APT 组织等安全事件的专题规则库并定期更新，可配置勒索病毒主动防护策略，实现勒索病毒的监控与隔离；同时匹配漏洞扫描、安全基线设置等高级防护功能，确保备份及恢复环境安全可靠。	
		行为防护	可检测并阻断攻击者利用 powershell 访问互联网行为，可检测并阻断攻击者利用 psexec 工具执行命令行为，可检测并阻断缓冲区溢出漏洞攻击行为，可检测并阻断攻击者利用 powershell 从远端加载恶意文件攻击，可检测并阻断攻击者反射注入 dll 恶意行为。	
		恶意程序防护	可检测并阻断系统内存密码盗窃行为，可检测并阻断攻击者利用代理工具进行内外网穿透行为，可检测并阻断攻击者利用非系统进程尝试劫持 EXE 执行过程行为，可检测并阻断攻击者利用非系统进程尝试劫持自启动过程行为，可检测并阻断攻击者更改系统引导文件行为，可检测并阻断攻击者更改系统可执行文件行为。	
		质保服务	含 3 年规则升级及原厂服务。	
		产品资质	产品具有《国家信息安全测评信息技术产品安全测评证书》（级别 EAL3+）（提供有效证明复印件并加盖公章）	
		厂商资质	产品制造商具备国家信息安全测评信息安全服务资质证书安全开发类二级。（提供有效证书复印件并加盖公章）	

		现场服务	提供日常网络、计算、存储和安全设备的巡检，处理日常运营问题，协助完成突发故障和事件处置，做好管理台账以及每季一次汇报/每年度一次汇报和建议工作。（现场服务详细要求可见本项目服务要求章节）	
5	光纤交换机（2台）	硬件配置	≥32Gb，≥24 端口交换机，≥24 端口激活，含≥24 个 16Gb/s 短波模块，全光纤支持级联，单电源（固定），机架套件	
		功能要求	采用≥16Gb 光纤通道技术，支持广泛的光纤通道和多功能/融合协议、收发器及线缆产品组合。提供存储网络环境中关键业务数据和应用所需的可扩展性、灵活性、性能、安全性和互操作性，以满足日益复杂的存储环境的需求。	
		质保服务	含 3 年原厂服务。	

三、服务要求

本项目服务要求分为**基本服务要求**、**实施期服务要求**、**免费质保期服务要求**和**收费维保期服务要求**，均要求投标人无条件承诺满足，出具书面承诺函，加盖投标人公章，不承诺或承诺不合格，可取消投标人资格，具体要求如下：

一、基本服务要求

1. 功能不重复收费。本项目所采购的设备设施的功能，必须完全包含技术要求文件所列的功能，这些功能在交货至采购方时必须完全开通且为正式版，采购方无需再额外购买授权。尤其强调凡是参数里文字载明了“实现”、“支持”、“具备”、“能够”、“包含”、“提供”、“配置”、“自带”、“配备”等字眼，表示交货时必须开通所对应的功能且为正式版，采购方无需再额外购买授权。

2. 利旧集成。凡是采购方已有的设备，包括但不限于标明“利旧集成”、“利旧、升级并集成”等字眼的，由供方按采购方要求负责提供集成服务，费用包含在本项目中标价范围内，采购方不再另行付费。

二、实施期服务内容

1. 到货时间。合同签订后 25 天内全部到货。

2. 安装部署。到货后 15 天内完成安装、上架和部署运行。

3. 需求调研。供方需对采购方主生产机房、容灾机房、备份机房进行现场勘察，了解现有的设备设施情况，并充分了解采购方在计算、存储、网络、网络安全等各方面的需求，编制需求调研报告。

4. 实施方案。根据需求调研报告，供方需编制项目实施方案，要求该方案中包括但不限于下列子方案：底层网络架构设计、数据中心整体设计、容灾备份体系设计、安全体系建设规划、技术解决方案、进度计划、供方实施团队安排、部署调试方案、培训方案、技术移交方案、测试上线方案、试运行期故障问题处理方案等，经采购方确认后即实施。对于不清楚事项，应多于采购方进行有效沟通，避免出现信息不对等情况出现。

5. 组织实施。按照确认过的项目实施方案，供方组织己方实施团队，按进度要求组织实施，包括新设备设施的部署调试，和采购方已有设备实施的利旧集成部署调试。实施过程中严格遵守采购方有关制度规定，保质保量、按进度推进项目。

6. 功能测试。设备设施部署完成后，采购方、供方共同对设备设施进行功能测试，检核是否达到招标文件和合同要求的目标。达成目标经采购方确认后，即进入项目试运行阶段，供方须做好试运行阶段故障的处理和设备设施配置的完善，确保至验收前不存在问题。

7. 组织培训。按照项目实施方案，组织对采购方操作人员、系统管理员、维护人员等各类运维人员进行专项培训，确保采购方人员可以正确使用、维护设备系统。培训效果须经采购方确认，未达成目的则供方负责继续组织培训。

8. 技术移交。供方应向采购方移交各类技术文档和手册资料，包括但不限于项目方案、网络拓扑图、部署架构图、设备操作文档、配置文档、检修手册、运维手册等资料，资料类型包括书面纸质版和电子版，且须经采购方确认。

9. 等保测评。本项目实施目标包括满足采购方数据中心、信息系统达到三级等保测评要求。

10. 项目验收。项目试运行期满三个月，供方向采购方提交验收申请，并附

详细验收报告，验收报告要求响应项目实施方案，对其中各项内容、功能实现情况、试运行阶段问题处理情况、采购方提出的其他要求等任务的完成情况进行详细阐述，并提供详实佐证资料。经采购方确认后，方通过验收。

11. 其他服务：

(1) 系统迁移与重装。项目实施期内，对于采购方系统需要进行迁移的，供方提供技术服务，确保采购方应用系统环境重新搭建、数据导入、网络切换等各项工作顺利完成。

(2) 设备运行维护保障。对设备进行维护保障，确保正常安全稳定运行，保障我方业务顺利开展。

(3) 网络安全。对于采购方在漏洞检测、渗透测试、等保测评、网络攻防演练、网络安全事故处理等过程中发现或出现的各种网络安全隐患，供方应无条件免费提供技术支持进行处理和完善。供方必须严格遵守中华人民共和国网络安全法、数据安全法的规定，开展项目实施工作。

(4) 网络畅通。配合采购方及运营商，对采购方连接二医院、四医院、五医院、十五冶医院、国安医院等所有直属单位的裸纤、本地电路接入网络和安全设备等提供技术支持，确保网路畅通。

(5) 配件要求。本项目采购范围包含所有配件，包括设备的各种组成部分，如光模块、光口、端口、接口、光缆、网线、辅材等，且必须符合兼容要求和质量要求。

(6) 布线理线。供方负责采购方机房的所有布线、理线施工，且走线符合国家标准和规范，插口、线路均有标识，且有详细记录台账，项目交付时一并移交采购方。

(7) 配件与新机更换要求。对于本次采购的新设备设施，若出现故障，供方在规定时间内响应、修复或更换；对于需要更换零配件的，由供方在7个工作日内免费提供并及时进行更换；对于更换零配件仍然无法解决故障问题的，由供方于20个工作日内免费提供全新设备进行更换，保障我方业务正常开展。

(8) 系统维护要求。供方对本项目范围内提供的系统的质量负责，凡是出现系统故障的，供方无条件负责进行及时的、高质量的维护，不得推诿。

(9) 机房搬迁要求。若实施过程中，需要对采购人现有机房设备设施进行搬迁，包括计算存储、数据通信、网络安全及其它机房设备设施等，由供方负责搬迁至采购人指定的新机房中，并负责做好应用系统环境重新搭建、数据导入、网络切换等各项工作，不影响采购方业务。

12. 实施期服务内容包括但不限于上述内容，凡是与本项目正常安全稳定运行有关的实施内容均包含在内，具体以采购方实际情况为准，

上述服务均由供方提供，所涉费用均包含在本项目合同总价范围内，不再另行增加。

三、免费质保期服务内容

本项目免费质保期，自正式通过采购方验收之日起算，免费质保期供方提供服务内容包括但不限于下列内容：

1. 本项目新采购的安全设备设施，免费质保期 3 年，在免费质保期内，享受免费维修、免费更换配件等服务，免费更换配件仍无法修复的，则免费更换新机。

2. 本项目内续保的安全设备设施，免费质保期 1 年，在免费质保期内，设备自身软硬件故障均由供方承担费用，采购方不另外付费。

3. 供方服务能力要求。在全国有完善的售后服务体系，有 400 客服中心，在黄石本地及武汉等周边城市设有售后服务站。供方能够提供故障维修和预防性维护服务，通过此项服务来保证设备处于良好的运行状态。供方能够组织成立专门的售后技术服务队伍，提供集中、统一的规划、设计、支持、服务。

4. 供方人员技术支持要求。当用户方实施系统升级优化、故障分析时，供方可以提供专职工程师现场技术支持服务。必要时根据最终用户要求，提供产品原厂售后工程师现场技术支持服务。当出现故障时，维护服务响应时间为 7×24 小时，供方在接到现场服务需求后立即响应，硬件故障到达现场后 1 个小时内解决，软件问题到达现场后 2 个小时内解决，需要更换部件的，一般当日解

决，特殊情况不超过 3 天。

5. 备品备件保障要求。供方能够提供充足的零配件，以确保设备维修所需更换的零配件。在湖北黄石及武汉等周边城市设有备品备件库，对备品、备件实行分级库管理，以便及时替换故障设备，保证系统正常运转。

6. 维护保障要求。在本项目免费质保期内，供方负责进行所有的故障处理，对于需要更换零配件的，由供方在 7 个工作日内免费提供并及时进行更换；对于更换零配件仍然无法解决故障问题的，由供方于 20 个工作日内免费提供全新设备进行更换，保障我方业务正常开展。供方接到用户的备件或新设备更换需求后，供方按现场服务响应时间要求，及时派工程师携带有关备品备件抵达用户现场，保证更换备件或新设备为原厂全新备件。

7. 巡检维护要求。在运行维护服务期内，服务工程师每月对所有供货设备设施进行全面的巡检和预防性维护，对整个设备各部件进行清洁、除尘，对设备各性能进行检查和调整，对隐患部件进行更换等，做好文字记录并存档。并提供服务规范文件，按服务规范向贵方最终用户提供服务和技术支持。

8. 安全设备维护服务要求：

对现有数据中心网络安全设备提供现场的技术支持，对防火墙等安全类设备提供远程或现场的技术支持，对各安全类设备提供管理服务，包括硬件、软件升级、病毒库升级、使用单位、使用人、IP 地址等。

9. 网络安全服务。对于采购方在漏洞检测、渗透测试、等保测评、网络攻防演练、网络安全事故处理等过程中发现或出现的系统安全问题，供方应无条件免费提供技术支持进行处理和完善。供方必须严格遵守中华人民共和国网络安全法、数据安全法的规定，开展质保期服务工作。

10. 培训服务要求。根据信息安全技术的发展和不同层面的信息安全人才需求，针对组织决策者、管理者、工作人员、运维人员、安全管理员等从网络、终端、日常工作生活、移动安全等维度进行信息安全意识培训、信息安全技术培训。内容涵盖：信息安全事件与安全威胁、日常安全和必备安全习惯、信息安全基础、

常见操作系统安全、网络安全设备、抗拒绝服务攻击技术、Web 应用安全之常见威胁、常见漏洞、热点安全事件（如：0day、勒索、挖矿等）。

11. 重要时期安全保障。主要针对企业重要 IT 系统资产、包括主机、网络、应用等系统运行维护场景。针对互联网 IT 服务业务、IT 资产为服务对象。服务内容包括：信息安全通告、信息安全咨询、对外服务检查、WEB 站点渗透测试、安全漏洞扫描、主机安全检查、网站安全监测服务、安全值守服务、安全日志分析、应急响应服务。该服务每年不得少于四次。

12. 数据容灾备份安全防护系统服务要求。供方承诺数据容灾备份设备出现安全事故，由供方承担安全责任事故的全部责任。

13. 其他服务。无条件免费支持我方医养集团及直属单位内网络运维，包括调整优化、配置优化等，并对可能出现的网络成环、网络拥塞等问题及时进行处理，确保我方网络安全畅通运行。

上述服务均由供方提供，所涉费用均包含在本项目合同总价范围内，不再另行增加

四、收费维保期服务内容

1. 项目免费质保期满前三个月内，我方可自由选择与项目承包商签订收费维保服务，以一年为一个收费维保周期。

2. 要求供方提供与免费质保期一致的所有服务（收费维保期服务不包含新机更换服务，但包含故障零配件免费更换服务）。

3. 所有费用均包含在该收费维保期维保费用中，我方不再增加其他费用。

五、供方提供内网安全扫描服务

1. 服务内容概述。资产安全识别：识别业务系统资产，并通过可视化平台展示出来；暴露面检测：对资产暴露程度进行检测；漏洞脆弱性检测：对系统漏洞和 WEB 漏洞进行检测；高危 0day 事件告警：出现 0day 漏洞第一时间告警。

2. 服务频率。每年提供具体服务，具体的系统由业主方实际需求为准，提供 3 年服务。

3. 服务要求:

资产安全识别: 端口、服务、操作系统探测, 设备类型探测, 如: 交换机、负载均衡和防火墙等, WEB 容器探测, 如: Apache、tomcat、Weblogic、WebSphere、Nginx 等, WEB 服务语言探测, 如: PHP、JSP、ASP、ASPX、.NET 等, WEB 开发框架探测, 如: Django、Rails、ThinkPHP、Struts 等, WEB 应用探测, 如: BBS、CMS 和 BLOG 等, WEB 前端框架探测, 如: jQuery、Bootstrap、HTML5 等, 0day 漏洞应急响应, 通过对资产的识别, 精准定位爆发的 0day 或 Nday 漏洞, 缩短应急响应时间。

关键资产系统域名发现: 自动发现客户所填入域名的相关所有子域名。

开放端口监测: 检测网站服务器端口开放情况, 比如数据库端口、FTP 服务端口等。

网站后台暴露: 检测网站管理后台向互联网开放。

WAF 防御检测: 可检测用户的网站是否存在 WAF 防护。

WEB 漏洞扫描: 覆盖通用漏洞和常规漏洞。支持 SQL 注入、XSS、安全配置错误、已知漏洞组件包含、敏感信息泄露等常见的漏洞的检测。

系统漏洞检测: 各种系统漏洞、协议漏洞, 如: CVE 漏洞、MS 漏洞等。

信息泄露检测: 检测网站源码、数据库备份文件、SVN 文件、系统重要配置、日志文件向外网泄露。

弱口令检测: 对服务器对外提供的 rdp,ssh 等远程服务进行弱口令检测。

通用性字典弱口令检测, 如: top500,top10000 等; 行业性字典弱口令探测, 如: 运营商行业、教育行业等。

高危 0day 实时检测: 出现 0Day 漏洞时, 主动对所监控用户业务做扫描发现, 如有影响范围大、破坏性高的重要网络安全事件和安全漏洞快速预警通告和检测, 检测结果第一时间推送到客户。

服务成果要求包含但不限于以下文档: 《风险评估报告》、《每日评估报告》、《每月运营报告》。

六、供方提供应急响应服务

1. 服务内容概述。为采购方提供信息安全事件应急响应和处置服务，在发生信息破坏事件（篡改、泄露、窃取、丢失等）、大规模病毒事件、网站漏洞事件等信息安全事件时，提供应急响应专家协助处置。事件处理结束后，应根据要求完成相关报告。提供合理的应急响应服务支持流程和处置流程。

事件范围：WEB 入侵：挂马、篡改、暗链、WEBSHELL；系统入侵：系统异常、RDP 爆破、SSH 爆破、主机漏洞；病毒木马：远控、后门、勒索软件；信息泄露：拖库、数据库登录（弱口令）；网络异常：频繁发包、批量请求、DOS 攻击。

2. 服务频率。业主方出现紧急状况、事故时，在接到业主通知或诉求的第一时间，集成商或原厂商予以响应，提供解决方案和技术支持。提供 3 年服务。

3. 服务要求：如采购人发生信息安全事件，服务商应在采购人通知后的 30 分钟内进行响应，以工程师远程协助或到采购人现场的方式，两小时内到达现场协助进行事件处理。

4. 服务内容应包含以下阶段：

（1）应急响应小组应了解应急服务对象的各项业务功能及其之间的相关性，确定支持各种业务功能的相关信息系统资源及其他资源，明确相关信息的保密性、完整性和可用性要求；

（2）对服务对象的信息系统，包括应用程序，服务器，网络及任何管理和维护这些系统的流程进行评估，确定系统所执行的关键功能，并确定执行这些关键功能所需要的特定系统资源；

（3）应急响应小组采用定性或定量的方法，对业务中断、系统宕机、网络瘫痪等突发安全事件造成的影响进行评估；

（4）应急响应小组协助服务对象建立适当的应急响应策略，应提供在业务中断、系统宕机、网络瘫痪等突发安全事件发生后快速有效的恢复信息系统运行的方法；

（5）应急响应小组为服务对象提供相关的培训服务，以提高服务对象的安

全意识，便于相关责任人明确自己的角色和责任，了解常见的安全事件和入侵行为，熟悉应急响应策略。

检测阶段：接到事故报警后在服务对象的配合下对异常的系统进行初步分析，确认其是否真正发生了信息安全事件，制定进一步的响应策略，并保留证据。

输出：《检测结果记录》

抑制阶段：及时采取行动限制事件扩散和影响范围，限制潜在的损失与破坏，同时要确保封锁方法对涉及相关业务影响最小。输出：《抑制处理记录表》。

根除阶段：对事件进行抑制之后，通过对有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。输出《根除处理记录表》。

恢复阶段：恢复安全事件所涉及到的系统，并还原到正常状态，使业务能够正常进行，恢复工作应避免出现误操作导致数据的丢失。

总结阶段：通过以上各个阶段的记录表格，回顾安全事件处理的全过程，整理与事件相关的各种信息，进行总结，并尽可能的把所有信息记录到文档中。

应急处理总结的具体工作包括但不限于：事件发生的现象总结；事件发生的原因分析；系统的损害程度评估；事件损失估计；采取的主要应对措施；相关的工具文档（如专项预案、方案等）归档。

事故报告：应急服务提供者应向服务对象提供完备的网络安全事件处理报告；应急服务提供者应向服务对象提供网络安全方面的措施和建议；

上述总结报告的具体信息参考《应急响应报告表》

（6）交付文档

安全事件处置完成，系统得到恢复。

找到安全事件发生原因并提供安全解决方案。

提供交付物。

《XX 系统（事件）应急响应报告》。

得到采购方相关负责人的书面确认。

七、供方提供安全加固服务

1. 服务内容概述。系统漏洞加固：根据主机扫描结果，针对不同版本的应用系统及网络安全漏洞加固，对漏洞进行补丁或配置加固，防止入侵。安全配置加固建议：根据配置核查结果，针对不同版本的应用系统及安全配置加固，提供网络层加固整改建议。安全策略分析：分析策略对保护业务的有效性。加固追踪：提供主机漏洞、网站漏洞、配置加固等方面的安全加固情况，跟踪加固进度，通过平台展示安全加固率，便于监测安全加固工作情况与效率，推动安全加固工作的开展。

2. 服务频率。每年提供具体服务，具体需求以业主方实际需求为准，提供 3 年服务。

3. 服务要求。漏洞加固服务。服务商根据安全漏洞扫描结果，开展查漏补缺的安全整改优化服务，提供应用系统加固协助服务、服务器操作系统加固服务、数据库安全加固协助服务、中间件安全加固协助服务、网络设备安全加固服务、安全整改建议，并撰写安全整改报告等。

对存在风险的安全加固，进行梳理、答疑以及加固方案输出。并配和对补丁修补，并优化和加强账号口令、日志、网络性能、文件系统、权限控制、服务进程等安全特征的管理。如：补丁、文件系统、帐号管理、网络及服务、注册表、共享、应用软件、审计/日志、紧急恢复，使系统可以长期保持在高度可信的状态。

服务成果要求包含但不限于下列文档：《信息安全安全整改报告》、《安全优化实施方案》、要求实时展示各单位/系统的漏洞加固率。

配置加固服务：服务提供商根据安全配置核查结果，略开展配置完善优化服务，提供应用系统配置加固协助服务、服务器操作系统配置加固服务、数据库配置安全加固协助服务、中间件配置安全加固协助服务、网络设备配置安全加固服务、安全设备配置安全加固服务安全整改建议，并撰写安全整改报告等报告。

服务成果要求包含但不限于下列文档：《信息安全安全整改报告》、《配置加固实施方案》、安全策略分析服务。

通过工具扫描和人工测试，根据整体安全策略目标，分析网络安全产品策略合理性，并提供改进建议。

服务成果要求包含但不限于以下文档：《信息安全整改报告》、《安全策略分析报告》。

八、供方提供现场网络安全服务：

1. 提供日常网络、计算、存储和安全设备的巡检，处理日常运营问题，协助完成突发故障和事件处置，做好管理台账以及每季一次汇报/每年度一次汇报和建议工作。

2. 网络维护技术服务

- (1) 负责常用软件的安装及应用，解决常见终端故障；
- (2) 负责维护网络交换系统，能够解决常见网络故障；
- (3) 负责终端病毒防护，对常见计算机病毒及网络木马有一定处理能力；
- (4) 负责防火墙、漏洞扫描等网络安全防护设备，能够处理常见的网络安全故障。

(5) 负责超融合/虚拟化平台运维及操作、系统备份、常见故障处置；

(6) 负责系统运维，常见数据库的操作维护；

3. 技术力量服务总体要求

(1) 现场人员共 1 人，负责网络维护技术服务，服务期不少于 1 年；工作时间由采购单位安排，不少于 5 天×24 小时，因工程施工、突发事件等情况需加班的，应无条件执行；

(2) 现场人员对用户终端进行操作时，涉及对终端的文件操作，须征得用户同意；

(3) 现场人员出现故障不能当场解决的，向用户解释清楚原因，做好记录，与用户协商好解决时间；

(4) 采购单位为现场服务人员提供工作条件，但与其之间不存在任何劳动关系和劳务关系；

(5) 发生人员变更时需提前 30 天通知采购单位，采购单位审批后方可办理交接手续；

(6) 现场人员具备良好的学习能力，沟通处理能力，服务态度良好。

4.7×24 小时值守服务。为保障医院后台支撑系统的正常运行，以及端业务服务的连续性，投标方需要提供 7×24 小时值守的能力（现场或远程不限），确保设备和系统在发生故障时间，能第一时间发现和告警，第一时间告知相关责任人，以便得到妥善的处置，不影响医院业务系统正常运行。

5. 考核要求

由采购单位对现场人员每月进行一次能力评估考核，连续 3 月考核不合格人员，供方承诺无条件更换现场人员，且现场服务时间重新计算。如出现 2 次现场人员更换，考核人员仍未达标，则采购单位无条件取消现场人员服务合同，同时核减现场人员费用。

履约服务考核表

序号	名 称	服务要求	考核惩罚	备注
1	驻场服务 服务期限 1 年	提供日常网络、计算、存储和安全设备的巡检，处理日常运营问题，协助完成突发故障和事件处置，做好管理台账以及每季一次汇报/每年度一次汇报和建议工作。	对现场人员每月进行一次能力评估考核，连续3月考核不合格人员，供方承诺无条件更换现场人员，且现场服务时间重新计算。如出现2次现场人员更换，考核人员仍未达标，则采购单位无条件取消现场人员服务合同，扣除合同总金额的10%。	
		网络维护技术服务 (1) 负责常用软件的安装及应用，解决常见终端故障； (2) 负责维护网络交换系统，能够解决常见网络故障； (3) 负责终端病毒防护，对常见计算机病毒及网络木马有一定处理能力； (4) 负责防火墙、漏洞扫描等网络安全防护设备，能够处理常见的网络安全故障。 (5) 负责超融合/虚拟化平台运维及操作、系统备份、常见故障处置； (6) 负责系统运维，常见数据库的操作维护；		
		技术力量服务总体要求 (1) 驻场人员共1人，负责网络维护技术服务，服务期不少于1年；工作时间由采购单位安排，因工程施工、突发事件等情况需加班的，应无条件执行； (2) 驻场人员对用户终端进行操作时，涉及对终端的文件操作，须征得用户同意； (3) 驻场人员出现故障不能当场解决的，向用户解释清楚原因，做好记录，与用户协商好解决时间； (4) 采购单位为驻场服务人员提供工作条件，但与其之间不存在任何劳动和劳务关系； (5) 发生人员变更时需提前30天通知采购单位，采购单位审批后方可办理交接手续； (6) 驻场人员具备良好的学习能力，沟通处理能力，服务态度良好。		
2	免费质保 期服务内容	网络安全服务： 发现漏洞，质保期内，无条件解决； 培训服务要求： 根据客户要求来定，一年不少于1次； 重要时期安全保障： 每年不少于4次。 考核内容： 1、网络安全服务：服务报告 2、培训服务：培训记录 3、重要时期安全保障：值守报告	1. 每发生1次未履约问题，扣除合同总金额的0.04%。 2. 扣款上限：全年累计扣款总额不超过项目总合同金额2%。	

3	网络安全服务	<p>安全扫描服务：服务频率一年两次。每年提供具体服务，具体的系统由业主方实际需求为准。</p> <p>考核内容： 《风险评估报告》、《每日评估报告》、《每月运营报告》。</p>	<p>3 出现数据泄露、勒索病毒爆发、上级监管书面通报等特大安全责任事故，采购人有权单方解除安全服务合同，剩余全部安全服务费不予支付，并有权向中标方追索损失。</p>	
		<p>应急响应服务：业主方出现紧急状况、事故时，在接到业主通知或诉求的第一时间，集成商或原厂商予以响应，提供解决方案和技术支持。</p> <p>考核内容： 紧急状况处理效率、质量等。</p>		
		<p>安全加固服务：服务频率一年两次。每年提供具体服务，具体需求以业主方实际需求为准。</p> <p>考核内容： 《信息安全整改报告》、《安全优化实施方案》</p>		
		<p>网络服务：提供日常网络、计算、存储和安全设备的巡检，处理日常运营问题，协助完成突发故障和事件处置，做好管理台账以及每季一次汇报/每年度一次汇报和建议工作。发现漏洞，维保期内，无条件解决</p> <p>考核内容： 《网络安全服务报告》4次/年</p>		
		<p>7×24小时值守服务：为保障医院后台支撑系统的正常运行，以及端业务服务的连续性，投标方需要提供7×24小时值守的能力</p> <p>考核内容： 《7*24小时值守报告》</p>		

第四章 评标方法及标准

一、资格审查合格标准

序号	评审因素	评审标准
1	投标人资质要求	投标人须为在中国境内注册的企业，具备有效营业执照，且经营范围须满足本项目实际需求。若投标人为不具备独立法人资格的分公司，须提供总公司（或具有管辖权的上级公司）针对本项目的唯一授权书，经有效授权后，总公司（或上级公司）的资质、资格、业绩等条件均对分公司有效。
2	业绩要求	投标人近三年（2023年6月1日至今）至少完成过一例合同金额150万元及以上的信息安全项目实施案例，要求提供中标通知书或合同复印件。
3	信用中国	根据《关于在招标投标活动中对失信被执行人实施联合惩戒的通知》([2016]285号)规定，投标人须通过“信用中国”对本企业进行信用查询，若在“失信惩戒对象”名单中的，其投标无效，查询结果以开标当天在“信用中国”网站查询结果为准；提供网页查询截图。
4	信誉情况	投标人近三年内企业无涉及重大资产的不良诉讼，履约情况良好，近三年无重大违法情况（提供没有重大违法记录的书面声明），且目前未处于投标资格被取消状态；提供企业声明加盖公章。
5	是否接受联合体	本项目不接受联合体投标

二、评标方法

评标程序：由评标委员会组对各投标单位的投标文件进行资格和符合性审查，评委只对审查合格、实质性响应招标文件要求的投标文件进行评审和比较。

评分内容	评审因素	分值	评分标准
价格部分 (30分)	价格评审	30	<p>1. 评标小组只对符合性审查合格的响应文件进行价格评议，报价分采用低价优先法计算，即满足投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。</p> <p>2. 其他供应商的价格分按照下列公式计算： 报价得分=(评标基准价 / 投标报价) × 30 × 100%。 计算时保留两位小数。</p> <p>3. 注：投标报价高于采购预算价的作废标处理。评标小组认为供应商的报价明显低于其他通过符合性审查投标人的报价，有可能影响货物质量或者不能诚信履约的，应当要求其在投标现场合理的时间内提供书面说明，必要时提交</p>

			相关证明材料；投标人不能证明其报价合理性的，评标小组应当将其作为无效投标处理。
商务部分 (30 分)	类似业绩	6	除资格业绩外，投标人近三年（2023 年 6 月 1 日至今）每提供一个合同金额 150 万及以上信息安全类项目相关业绩，得 3 分，最高得 6 分。 (需提供合同原件扫描件)；
	项目团队	6	投标人拟投入本项目的项目经理须为投标人正式员工： 1、具备信息系统项目管理师证书、通信工程师证书，每提供一个证书得 3 分，最高得 6 分。 证明材料：提供证书和近三个月社保缴纳证明，并加盖投标人公章，未提供不得分。
		6	投标人拟投入本项目的项目组成人员（不包括项目经理）须为投标人正式员工。在此基础上： 1、具备信息系统项目管理师证书的，得 2 分。 2、具备高级通信工程师的，得 2 分。 3、具备 CISP 注册信息安全工程师，得 2 分。 证明材料：提供项目组成人员证书扫描件和近三个月社保缴纳证明，并加盖投标人公章，未提供不得分。
	企业实力	12	投标人具有中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质（安全集成）证书、信息安全服务资质（应急处理）证书、CCRC 信息安全服务资质（安全运维）证书、CCRC 信息安全服务资质（灾难备份与恢复）证书、CCRC 信息安全服务资质（风险评估），证书级别为一级，每提供 1 个得 4 分；证书级别为二级或三级，每提供 1 个得 2 分。同类证书不重复得分，最高得 12 分。（投标人需提供证书复印件并加盖公章，否则视为未提供）
技术部分 (40 分)	技术要求	24	1. 标“▲”项为关键技术参数，投标人需提供相关佐证资料，未提供的视为负偏离，每负偏离一项扣 2 分。 2. 其余为一般技术参数，若需要提供相关佐证资料的，投标人需按要求提供，不提供或不满足视为负偏离，每负偏离一项扣 1 分。 3. 全部按要求提供的，本项得 24 分；若本项出现多项负偏离时，可累计扣完本项 24 分为止。 注：未提供《6-1 新购设备承诺函》，本项不得分。
	应急响应	4	电话/远程响应：10 分钟以内得 1 分，30 分钟以内得 0.5 分，超过 30 分钟不得分； 技术人员到达现场：30 分钟以内得 1 分，1 小时以内得 0.5 分，2 小时以内得 1 分，超过 2 小时不得分； 核心业务恢复时限：4 小时以内得 2 分，8 小时以内得 1 分，超过 8 小时不得分。 注：提供《6-2 应急响应承诺函》，未提供本项不得分。

	应急响应和重大事件保障	2	投标人须对运维服务制定应急响应及重大事件保障机制，对重大故障及重大保障制定专门的应急预案，包括人员和资源配置。应急响应机制完整、可行、合理得 1.6-2 分，一般得 1.2-1.5 分，不可行或未提供的不得分。
	质量工期保证	2	投标人提供施工进度表和合理性施工方案，质量工期保证措施完整、可行、合理得 1.6-2 分，一般得 1.2-1.5 分，不可行或未提供的不得分。
	售后故障服务	8	投标人针对本项目提供详细的系统故障处理方案，获得原厂售后服务承诺及支持，包括但不限于故障紧急处理预案、故障处理原则、流程时效及工作要求、预防机制等，有且售后服务相关能力满足项目需求。服务方案优秀得 6.4-8 分，一般得 4.8-6.3 分，差或未提供的不得分。

评分计分办法和有关规定：

- 1、各参与投标单位的最终得分为各评委所评定分数相加后的算术平均值。
- 2、各项统计、评分结果均按四舍五入方法精确到小数点后二位。

三、定标

1、定标：在通过资格审查、符合性审查，综合得分最高的投标人推荐为中标人，并以其报价作为中标价。

2、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，且按照技术部分评审得分最高的投标人为排名第一的中标候选人。

3、中标单位因不可抗力或者自身原因不能履合同的，采购人可以与排在中标单位之后第一位的中标候选单位签订采购合同，以此类推。

第五章 合同条款

（此为中标后签订模板，此合同书仅供签订正式合同时参考用，正式合同书应包括此参考格式之内容）

甲方：

乙方：

根据公开招标结果，甲方同意将项目交由乙方完成。根据诚实信用、平等互利原则，经甲乙双方友好协商，就下列合同内容达成一致协议，合同条款如下：

一、定义和解释。（除另有说明外，下列名词定义和解释按本条所述）

1. 项目名称：
2. 建设单位：
3. 实施单位：

二、法律。合同双方应遵守《中华人民共和国民法典》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《计算机软件保护条例》及国家有关法律规定。

三、合同范围

乙方负责对合同附件所列清单上的硬件的购买、运输、交货、安装、现场调试、测试、验收、售后服务等。

四、文件的相互关系和书面通知、变更通知

1. 构成合同文件的各部分是相互补充的，具有同等法律效力。甲方对合同文件的有关事项发生疑问时，乙方应当负责释疑，如乙方的解释不符合甲方签署本合同的目的，则乙方同意按甲方的理解来确定该事项。

2. 乙方如认为甲方的实施要求或其他非乙方的行为影响了合同成本或交付期限，须立即以书面形式向甲方提出，甲方应在核实无误后向乙方发出调整通知。在乙方因其自身的失误、疏忽或未能按合同要求履行义务的情况下，甲方不发变更通知，交付期限按合同约定履行。

3. 除非甲方书面同意，乙方不得擅自对项目做任何变更。

五、合同价格

1. 合同总价。本合同总价_____元人民币，大写人民币_____元整。
2. 本合同总价包含项目设备采购、运输、安装上架、项目实施、调试配置、

测试、上线运行、验收、质保期服务等费用。

合同总价为甲方付给乙方合同范围内的基本价格，该费用为包干价。包括乙方向甲方提供的所有项目设备采购、运输、安装上架、项目实施、调试配置、测试、上线运行、验收、各项服务、质保期服务、培训等所有费用，及所有完成系统建设所需的相关手续、税金等各项直接、间接费用。甲方无需再向乙方支付其他任何费用。

3. 本合同价格包括政府有关部门向乙方所征收的与合同有关的所有税费及管理费。

4. 本合同价格包括乙方人员到现场的交通、食宿、项目实施及服务的一切费用。

六、付款方式

1. 本合同中甲乙双方之间发生的一切费用以人民币转账或电汇支付。

2. 费用支付方式：

见招标文件。

3. 符合上述付款条件时，乙方应依法向甲方提供合法合规发票，否则甲方有权拒绝付款。

七、货品到货

1. 本合同范围内的货品均在甲方要求的现场交货。

2. 本项目以正式部署上线运行完成日期视为交货日期。

八、工期

1. 乙方应在合同签订之日起45个日历天内完成本项目内设备设施、信息系统全部实施工作，由乙方提供符合本项目招标文件要求的服

2. 甲方应为乙方项目交付提供必要并符合乙方交付要求的物理条件，包括但不限于：机房配套设施等。

九、验收

1. 项目实施完成后，乙方按招标文件、投标文件及本合同等正式文件的约定，结合具体实施情况，实事求是、全面详实编写项目验收报告，并正式书面向甲方提交。

2. 甲方组织验收小组对项目进行验收，验收合格后完成验收报告确认手续。如验收不合格，乙方应在 10 个工作日内完成整改并申请复验，复验仍不通过，

甲方有权单方面解除合同，乙方应向甲方退回所有已付款项并承担合同总金额5%的违约金。

3. 验收标准如下：

(1) 本项目建设、上线和运维达到甲方招标文件所规定的要求。

(2) 从本项目上线试运行三个月的时期内，乙方要保障本项目的正常稳定可靠安全运行。

(3) 项目验收合格，乙方提交完整的安装竣工资料 2 套。并按档案管理编目和装订。

十、安装与培训

1. 现场安装。乙方应按合同规定派遣技术人员到现场进行本项目安装、调试和测试，根据合同附件要求进行网络改造。

2. 培训。乙方根据系统的要求，合理安排甲方人员进行培训。试运行期间乙方应对甲方本项目故障实时响应，并实时解决，以确保本项目正常稳定运行。若故障无法解决，乙方应在 2 小时内安排专人到甲方现场解决。乙方同时做好详细培训规划，免费对甲方使用人员进行针对性培训，确保使用人员对本项目的理解、掌握并能熟练运用和维护；若本项目系统升级，也提供相应的免费培训。

十一、版权归属

乙方自主开发的软件知识产权属乙方，但甲方在本项目中可以使用，甲方使用后形成的数据库归甲方所有，乙方不得使用、不得向第三方披露。本项目在甲方进行的个性化定制开发部分知识产权归甲方所有，未经甲方同意，乙方不得擅自使用上述定制化软件，并不得向第三方披露，否则乙方应当承担全部侵权责任。

十二、质保及售后

1. 本项目免费质保期限，续费设备____年、新购设备____年，从甲方书面确认本项目正式验收之日起算。

2. 甲方在质保期免费享有乙方提供的服务，具体见附件。

3 质保期过后，甲乙双方协商签订维保协议。本项目每年维保费用为本合同价的____%。乙方承诺，每年维保服务内容不得少于免费质保期内服务内容。

十三、违约责任

1. 甲方应提供适当的工作环境和场地，为乙方履行合同提供方便；乙方应保证项目质量，按时完工。乙方由于未履行其合同范围内的业务以致严重影响项目

实施、提供的与硬件不能满足合同规定的技术性能保证值，经调整更换后仍不能实现的、所交项目不符合合同规定经调整重修后仍不符合合同要求的、中途无故退出，发生上述情况之一，即视为乙方违约。乙方违约时，甲方有权利通知乙方单方解除本合同，乙方应向甲方退回所有已付款项并向甲方支付本合同总金额 5% 的违约金。

2. 若乙方提前交付，由于提前交付而产生的一切责任与风险由乙方承担。由于甲方原因造成工期延迟，则将工期顺延。

3. 乙方保证合同硬件的完整性，由于乙方的原因，造成合同或其他安装材料等的遗漏由乙方负责免费补齐。甲方应保证提供乙方符合本项目上线的配套环境，如甲方提供的交付环境无法满足要求，甲方有义务在 30 个自然日内负责完成。

4. 若由于乙方原因造成工期延误，每延误一天，应向甲方支付合同总价的 0.05% 的违约金；若延误工期三十日以上，则视为乙方违约单方面终止合同，乙方除向甲方退还已收取的全部费用外，乙方负责赔偿由此对甲方产生的一切经济损失。

5. 若乙方未提供本合同内约定的质保期售后服务，由此造成的甲方一切经济损失，由乙方承担赔偿责任。

6. 免费质保期或收费维保期过后，若甲方选择续签维保协议，而乙方拒绝，乙方向甲方支付本合同总金额 5% 的违约金，由此造成的甲方一切经济损失，由乙方承担赔偿责任。

7. 乙方若私自篡改甲方本项目数据信息，乙方应向甲方支付本合同总金额 5% 的违约金，并承担由此造成的负面影响、经济损失赔偿责任。

8. 乙方应保证提交的产品或成果未侵犯任何第三方权利，否则由此引发的纠纷或责任均由乙方承担。

9. 如乙方未按本协议履行售后及质保等相关义务，每违约一次应向甲方支付违约金 5000 元，如连续或累计违约达到 3 次的，除应向甲方按合同总金额 10% 向甲方支付违约金，甲方有权另行委托第三方履行，由此产生的费用由乙方负担。

10. 乙方不得将本项目以任何形式转包或分包交由第三方完成，否则视为乙方违约，甲方有权利通知乙方单方解除本合同，乙方应向甲方退回所有已付款项并向甲方支付本合同总金额 5% 的违约金。

十四、不可抗力

签订合同后，由于不可抗力不能履行合同时，双方对由此产生的损失，不得提出索赔要求。由于不可抗力使合同无法如约履行时，经双方协商允许变更或解除合同。

十五、税务

乙方根据合同供货清单，根据中华人民共和国现行税法、地方性法规和法令，按甲方要求，向甲方开具符合国家法律规定税率的增值税专用发票，乙方负责支付自己需缴纳的税款和其它费用。

十六、争议的解决方式

因履行本合同发生争执，由当事人协商解决，协商不成的，任何一方有权向甲方所在地有管辖权的人民法院提起诉讼。

十七、保密

甲乙双方应对对方提出的技术资料及价格，以及本合同履行过程中知悉的相关信息、文件、资讯等均负有保密的义务。非经对方同意，不得向任何第三方泄露。如未经对方同意，擅自披露和使用的，应承担因此造成的损失的赔偿责任。

十八、合同终止

1. 双方应按照合同的规定，全面履行完合同义务直至合同终止。
2. 甲乙双方均不得随意解除合同，如果一方根本违约另一方需解除合同，双方应磋商给违约方申辩理由及补正的机会；如仍需解除合同，双方应结清本协议约定的费用。双方有权追究在合同终止前的违约责任。
3. 乙方在收到甲方的合同终止书后，应立即终止合同执行，但双方有权追究在合同终止前的违约索赔。

十九、合同生效及其它

1. 合同自乙方履约金到账且双方代表人签字和单位盖章之后生效。
2. 合同书由合同条款与合同附件组成，具有同等法律效力。
3. 本合同一式捌份，甲方、乙方各执贰份，具有同等效力。经双方盖章后生效。
4. 合同未尽事宜由双方另行协商解决。

（以下页面为合同签订页，无正文）

甲方签章：

代 表：

签字日期：

乙方签章：

代 表：

签字日期：

合同附件：

附件 1：甲方本项目招标文件

附件 2：乙方本项目投标文件

第六章 投标文件格式

1、投标函

_____（招标人名称）：

根据你方招标项目编号为 _____ 的 _____ 招标文件，经踏勘项目现场和研究上述招标文件的投标须知、合同条款及其他有关文件后我方愿以人民币 _____ 元（大写 _____）的投标报价参与本次投标，并郑重声明同意如下：

（1）我方根据招标文件的规定，承担完成合同的责任和义务。

（2）我方已详细审核招标文件，确认招标文件中所需要我们提供的服务在需求、技术、质量和服务等方面不存在唯一性或歧视的条款。

（3）我方已详细审核招标文件，我方知道必须放弃提出含糊不清或误解问题的权利。

（4）我方同意在投标人须知规定的开标日期起遵循本投标文件，并在投标人须知规定的投标有效期满之前均具有约束力，并有可能中标。

（5）如果在投标截止时间后的投标有效期内撤回投标或者有其他违约行为，我方的投标保证金可被贵方全部没收。

（6）同意向贵方提供贵方可能要求的与本投标有关的任何数据或资料。

（7）我方按照合同约定履行义务，完成中标项目服务，绝不将中标项目转让（转包或变相转包）给他人，由我单位直接承包管理，否则招标人有权单方解除合同。

与本投标有关的正式通讯地址为：

地址：_____ 邮政编码：_____

电话：_____ 传真：_____

开户银行名称：_____

开户银行帐号：_____

法定代表人或委托代理人（签名或盖章）：_____

投标人（盖公章）：_____

日期：_____年 _____月 _____日

2、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_____（投标人单位名称）的法定代表
人。

特此证明。

投标人：_____（盖章）

日 期：_____年_____月_____日

3、法定代表人授权委托书

本授权书声明：注册于（国家或地区的名称和供应商名称）的（法定代表人姓名、职务）代表本公司授权（被授权人的姓名、职务）为本公司的合法代理人，代表本公司参加 （项目名称） 投标，并处理一切与之有关的事务。

本授权书于_____年____月____日签字生效，特此声明。

供应商（盖章）：_____

法定代表人（签名或盖章）：_____

委托代理人（签名或盖章）：_____

委托日期：_____年____月____日

附：委托代理人身份证复印件

4. 投 标 报 价 表

一、升级续保部分

序号	设备设施名称	规格型号	单位	数量	报价（元）	备注
（一）黄石市第二医院网络安全升级续保清单						
1	绿盟防火墙	NFNX3-HD4100	套	1		
2	绿盟防火墙	NFNX3-HD4100	套	1		
3	绿盟防火墙	NFNX5-HD6300	套	1		
4	绿盟防火墙	NFNX5-HD6300	套	1		
5	绿盟防火墙	NFNX3-HD4100	套	1		
6	绿盟防火墙	NFNX3-HD4100	套	1		
7	绿盟防火墙	NFNX5-HD6300	套	1		
8	绿盟防火墙	NFNX5-HD6300	套	1		
9	绿盟网络安全漏洞扫描系统	RSASNX3-X	套	1		
10	天融信数据库审计	TopAudit	台	1		
11	EDR(DMZ区)（1套服务管理端，80个服务器杀毒客户端、30个PC端杀毒客户端，均为WINDOWS系统）	TopEDR（V1.0.2.2.14）	套	1		
12	EDR(内网区)（1套服务管理端，200个服务器杀毒客户端、600个PC端杀毒客户端，均为WINDOWS系统）	TopEDR（V1.0.2.2.14）	套	1		
13	信服易备容灾备份	XS-ES2Z	台	1		
14	信服易备容灾备份	XS-ES4T	台	1		
15	集团DMZ区千兆防火墙	深信服 AF-1000 B1300	台	1		
16	集团DMZ区千兆防火墙	深信服 AF-1000 B1300	台	1		
17	集团DMZ区WAF防火墙	深信服 WAF-1000 B1400	台	1		
18	外网上网行为管理	深信服 AC-1000 B1100	台	1		
（二）黄石市第四医院网络安全升级续保清单						
1	EDR(内网区)（1套服务管理端，50个服务器杀毒客户端、300个PC端杀毒客户端，均为WINDOWS系统）	TopEDR（V1.0.2.2.14）	套	1		

2	信服易备容灾备份	XS-ES8T	台	1		
3	深信服外网出口防火墙	AF 8.0.26	台	1		
4	深信服内网出口防火墙	AF 8.0.26	台	1		
(三) 黄石市第五医院网络安全升级续保清单						
1	EDR(内网区) (1套服务管理端, 50个服务器杀毒客户端、450个PC端杀毒客户端, 均为WINDOWS系统)	TopEDR (V1.0.2.2.14)	套	1		
2	数据库审计	TopAudit	台	1		
3	信服易备容灾备份	XS-ES2T	台	1		
(四) 黄石市十五冶医院网络安全升级续保清单						
1	信服易备容灾备份	XS-ES8C	台	1		
2	深信服网络防火墙	AF-1000 B1200	台	1		
合计(元)						

二、新增采购部分

序号	设备设施名称	规格型号	单位	单价(元)	数量	总报价(元)	备注
1	WAF 防火墙		台		2		
2	下一代防火墙		台		2		
3	零信任安全系统		台		1		含现场网络安全服务
4	应用、数据容灾备份安全防护系统		套		5		
5	光纤交换机		台		2		
合计(元)							

三、总报价汇总

- 1、总报价_____元(大写_____元)。
- 2、其中其中升级续保部分总计_____元(大写:_____);新增采购部分总计_____元(大写:_____);

5. 技术参数响应表

序号	产品名称	产品型号	技术要求	响应内容	证明材料页码数
1、黄石市第二医院网络安全升级续保清单					
1	绿盟防火墙	NFNX3-HD4100	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
2	绿盟防火墙	NFNX3-HD4100	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
3	绿盟防火墙	NFNX5-HD6300	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
4	绿盟防火墙	NFNX5-HD6300	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
5	绿盟防火墙	NFNX3-HD4100	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
6	绿盟防火墙	NFNX3-HD4100	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
7	绿盟防火墙	NFNX5-HD6300	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
8	绿盟防火墙	NFNX5-HD6300	包含 IPS+防病毒模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		
9	绿盟网络安全漏洞扫描系统	RSASN3-X	包含系统+web 漏洞特征库模块, 可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		

10	天融信数据库审计	TopAudit	可进行软件升级、硬件维修、特征库、规则库升级等。		
11	EDR（DMZ区）	TopEDR（V1.0.2.2.14）	<p>（1）服务管理端要求：1个Windows Server系统1年服务（外网），包含：硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>（2）服务器客户端要求：防病毒功能授权,含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p> <p>（3）PC客户端要求：防病毒功能授权,含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p>		
12	EDR（内网区）	TopEDR（V1.0.2.2.14）	<p>（1）服务管理端要求：1个Windows Server系统1年服务（外网），包含：硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>（2）服务器客户端要求：防病毒功能授权,含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p> <p>（3）PC客户端要求：防病毒功能授权,含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p>		

13	信服易备容灾备份	XS-ES2Z	(1) 硬件维保：原厂备件更换服务（7×24 小时响应，4 小时内到场）。 (2) 软件支持：信服易备系统版本升级、补丁更新及技术咨询服务。 (3) 定期巡检：每季度 1 次现场巡检，包含设备健康检查、性能优化建议等。		
14	信服易备容灾备份	XS-ES4T	(1) 硬件维保：原厂备件更换服务（7×24 小时响应，4 小时内到场）。 (2) 软件支持：信服易备系统版本升级、补丁更新及技术咨询服务。 (3) 定期巡检：每季度 1 次现场巡检，包含设备健康检查、性能优化建议等。		
15	集团 DMZ 区千兆防火墙	深信服 AF-1000 B1300	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。（已开通应用控制、漏洞攻击防护、僵尸网络、内容安全等基础安全功能,云脑-云智最新威胁防御规则库订阅服务 云脑-云鉴未知威胁与杀毒订阅服务等）		
16	集团 DMZ 区千兆防火墙	深信服 AF-1000 B1300	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。（已开通应用控制、漏洞攻击防护、僵尸网络、内容安全等基础安全功能,云脑-云智最新威胁防御规则库订阅服务 云脑-云鉴未知威胁与杀毒订阅服务等）		
17	集团 DMZ 区 WAF 防火墙	深信服 WAF-1000 B1400	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。		
18	外网上网行为管理	深信服 AC-1000 B1100	包含：软件升级、硬件维修、应用识别、URL 库升级、上网安全授权等。		

2、黄石市第四医院网络安全升级续保清单

1	EDR（内网区）	TopEDR (V1.0.2.2.14)	<p>（1）服务管理端要求：1个Windows Server系统1年服务（外网），包含：硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>（2）服务器客户端要求：防病毒功能授权,含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p> <p>（3）PC客户端要求：防病毒功能授权,含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p>		
2	信服易备容灾备份	XS-ES8T	<p>（1）硬件维保：原厂备件更换服务（7×24小时响应，4小时内到场）。</p> <p>（2）软件支持：信服易备系统版本升级、补丁更新及技术咨询服务。</p> <p>（3）定期巡检：每季度1次现场巡检，包含设备健康检查、性能优化建议等。</p>		
3	深信服外网出口防火墙	AF 8.0.26	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。		
4	深信服内网出口防火墙	AF 8.0.26	包含：软件升级、硬件维修、防病毒模块升级、入侵防护模块升级。		

3、黄石市第五医院网络安全升级续保清单

1	EDR（内网区）	TopEDR (V1.0.2.2.14)	<p>（1）服务管理端要求：1个Windows Server系统1年服务（外网），包含：硬件维修、防病毒模块升级、入侵防护模块升级。</p> <p>（2）服务器客户端要求：防病毒功能授权,含升级许可。支持基因识别、虚拟沙盒等引擎，可以精准查杀勒索、木马、蠕虫等各类病毒；提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持Windows，支持远程桌面功能。</p> <p>（3）PC客户端要求：防病毒功能授</p>		
---	----------	-------------------------	---	--	--

			权,含升级许可。支持基因识别、虚拟沙盒等引擎,可以精准查杀勒索、木马、蠕虫等各类病毒;提供病毒防御、系统防御以及网络防御等主动防御功能。客户端系统默认支持 Windows,支持远程桌面功能。		
2	数据库审计	TopAudit	可进行软件升级、硬件维修、特征库、规则库升级等。		
3	信服易备容灾备份	XS-ES2T	(1) 硬件维保: 原厂备件更换服务(7×24 小时响应,4 小时内到场)。 (2) 软件支持: 信服易备系统版本升级、补丁更新及技术服务。 (3) 定期巡检: 每季度 1 次现场巡检,包含设备健康检查、性能优化建议等。		

4、黄石市十五冶医院网络安全升级续保清单

1	信服易备容灾备份	XS-ES8C	(1) 硬件维保: 原厂备件更换服务(7×24 小时响应,4 小时内到场)。 (2) 软件支持: 信服易备系统版本升级、补丁更新及技术服务。 (3) 定期巡检: 每季度 1 次现场巡检,包含设备健康检查、性能优化建议等。		
2	深信服网络防火墙	AF-1000 B1200	包含 IPS+防病毒模块,可进行软件升级、硬件维修、防病毒模块升级、入侵防护模块升级等。		

备注: 涉及序列号等信息的, 中标后提供。

二、新增采购部分(交付硬件设备须为 2026 年 1 月 1 日(含)以后出厂的新品,提供相关承诺函,否则该设备所涉的所有技术规格及性能参数,在评审时一律按无效响应处理。)

5、鄂东医养集团数据中心网络安全升级加固新增

序号	设备名称	指标	技术要求	响应内容	证明材料页码数
1	下一代防火墙(2台)	硬件配置	≥1U 机型,含交流冗余电源,≥1*RJ45 串口,≥1*RJ45 管理口,≥2*USB 接口,10*GE 电口(含 2 对 Bypass),≥4 个 combo 口,≥2 个接口扩展槽位,1T 国产固态硬盘,SFP 万兆多模光纤接口模块,≥2*10GE 接口(300M,850nm,LC 接口,含原厂光模块),≥2 个万兆 SFP 插槽整机吞吐量≥8G(含原厂多模万兆光模块),应用层吞吐量≥1G,		

			最大并发连接数≥50 万,新建连接数≥2 万。防病毒模块,入侵防护模块,含传统防火墙、流量管理、IPSec VPN。		
			支持虚拟线,二层透明,三层,混合,旁路监听,单臂接入方式。		
			支持三层接口、三层子接口、环回接口、VPN 接口。		
			▲支持工业系统类应用协议识别,例如: OPC、EC、MODBUS、航天云网-NDICS、FOCAS、PCWORX 等工控协议;物联网类应用协议识别,例如: 西门子 MindSphere 平台、GB/T32960、JT808、JT809、JT905、CoAP、小米 N 音响、米家小白智能摄像机、Yeelight。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告,并加盖原厂公章。		
			▲针对防火墙策略,支持基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等,模拟流量报文的处理计算,获得策略的命中信息,并可对命中的策略信息进行编辑,实现防火墙策略命中情况的仿真模拟测算。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告,并加盖原厂公章。		
		功能要求	▲支持对非 IP 协议类型的流量进行访问控制,例如 IPX、Apple Talk。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告,并加盖原厂公章。		
			▲支持对基于 HTTP、FTP、POP3、SMTP、IMAP 协议的多线程下载行为,以及有密码的压缩包进行下载限制。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告,并加盖原厂公章。		
			▲策略可按匹配顺序、策略分组、新建顺序、安全区分组等不同维度的查看方式,在按匹配顺序查看下,可以通过拖拽实现优先级的调整,也可以输入具体的策略序号、置顶或者置底等方式进行调整。提供功能截图并加盖原厂公章。		
			提供基于源/目的 IP 地址、安全区、应用、应用组、协议/端口、时间、安全模板的精细粒度的安全访问控制,时间精确到秒级。		
			▲支持对应用进行二级分类,类型包括媒体类、协作类、一般网络应用、商业系统等,子类包括音频流、游戏、普通商业、工业系统、物联网、文件传输、知名网站、即时通信、图片视频、社交网络等,提供功能截图并加盖原厂公章。		
			支持内置/自定义 ISP 路由库,实现 ISP 链路间路由负载均衡。		

2		质保服务	含 3 年规则升级及原厂服务。		
		厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书, 提供有效证书的厂商盖章复印件。		
			厂商需具备符合 ISO 22301:2019 标准的业务连续性管理体系认证证书, 提供有效证书的厂商盖章复印件。		
			厂商具备中国电子信息行业联合会颁发的《信息系统建设和服务能力评估资质证书-CS4 级别》, 提供有效证书的厂商盖章复印件。		
		产品资质	产品厂商具备中国软件评测中心和中国计算机行业协会数据安全专业委员会联合颁发的《数据安全服务能力评定资格证书》(数据安全评估二级), 提供有效证书的厂商盖章复印件。		
			为保证数据的安全与可靠, 产品厂商应具备《隐私信息管理体系认证》证书, 提供有效证书的厂商盖章复印件。		
			产品具备《多核分布式安全操作系统》, 提供有效证书的厂商盖章复印件。		
		硬件配置	≥2U, 含交流冗余电源模块, ≥2*USB 接口, ≥1*RJ45 串口, ≥2*GE 管理口。≥6*GE 电口 (BYPASS), ≥4*千兆光口 (含原厂千兆多模光模块), ≥2 个接口扩展插槽位, 硬盘 4T, 2 个万兆 SFP 插槽, 支持万兆多模光纤接口模块、万兆单模光纤接口模块。整机吞吐量 10Gbps。		
		WAF 防火墙 (2 台) 功能要求	▲支持紧急模式: 支持配置 CPU 使用率、内存使用率、并发连接数阈值, 当 CPU 使用率, 内存使用率或并发连接数超过设置阈值时, WAF 自动进入紧急模式, 已经代理的连接正常代理, 对新增的请求直接转发; 当恢复到阈值以内时, 自动退出紧急模式。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告, 并加盖原厂公章。		
			部署灵活, 支持透明桥部署, 串联部署, 路由旁路部署, 镜像模式, 反向代理模式以及插件式等部署模式		
			▲会话追踪, 通过浏览器标识和会话标识实现对会话的跟踪, 记录完整的黑客攻击过程, 做到场景复现。提供第三方测试报告, 以及功能截图并且加盖厂家公章		
			▲支持对 XML 文件进行基础合规检测, 覆盖“节点个数、节点深度、节点名称长度”等; 支持基于自定义的 schema 文件对 XML 文件进行更加细致的合规检测, 能根据定义好的 schema 文件检测节		

			点类型、属性类型等。支持基于 WSDL 文件来检测 webservicess 请求的 soap 流量是否符合规则。提供功能截图证明及国家认可的含有 CNAS 的第三方检测报告，并加盖原厂公章。		
			▲支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell 及 Ruby shell，同时可支持源 IP 封禁、Session 封禁和 UA 封禁。提供功能截图并且加盖厂家公章		
			支持非法下载防护，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等）。		
			支持暴力破解防护，支持 GET/POST 两种请求方法检测；支持 Form/Ajax/JsonP 三种验证方式；支持验证码机制，可有效防止误报。		
			支持 Cookie 安全机制，通过 cookie 加密或 cookie 签名的方法对访问服务器后保留在客户端的 cookie 进行安全防护。		
		质保服务	含 3 年规则升级及原厂服务。		
		产品资质	产品厂商具备中国软件评测中心和中国计算机行业协会数据安全专业委员会联合颁发的《数据安全服务能力评定资格证书》(数据安全评估二级)，提供有效证书的厂商盖章复印件。		
			为保证数据的安全与可靠，产品厂商应具备《隐私信息管理体系认证》证书，提供有效证书的厂商盖章复印件。		
			参与起草了《信息安全技术 WEB 应用防火墙安全技术要求与测试评价方法》GB/T 32917-2016，提供截图证明。		
		厂商资质	厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书，提供有效证书的厂商盖章复印件。		
			厂商需具备符合 ISO 22301:2019 标准的业务连续性管理体系认证证书，提供有效证书的厂商盖章复印件。		
			厂商具备中国电子信息行业联合会颁发的《信息系统建设和服务能力评估资质证书-CS4 级别》，提供有效证书的厂商盖章复印件。		

3	零信任安全系统(1台)	硬件配置	性能参数：要求产品采用国产cpu,支持国产操作系统；SSL加密流量(Mbps)≥300,并发用户数(个)≥600；IPSEC加密最大流量(Mbps)≥100,IPSEC理论并发隧道数(Tunnel)≥1000；硬件参数：规格：1U,内存≥16G,硬盘容量≥128G SSD,接口≥6千兆电口,≥4千兆光口 SFP(含原厂千兆多模光模块)。售后服务：提供≥3年原厂维保服务。		
		软件授权	要求提供零信任接入授权数量≥200套,零信任访问控制管理系统软件授权数量≥1套,安全沙箱授权数量≥200套。		
		功能要求	身份认证： 为满足身份安全要求,应支持多因素认证,至少包括：账号密码认证、短信认证、证书认证、动态令牌认证、扫码认证,以及对接统一认证平台实现单点登录等认证方式。可配置的异常环境包括但不限于：账号首次登录、账号在该终端首次登录、闲置账号登录、弱密码登录、异常时间登录、非常用地点登录等。		
			权限及访问控制： 为满足组织灵活的管理要求,支持配置动态访问规则,可配置化的ACL规则引擎,可以灵活地将终端环境、用户身份、处置动作等进行配置,针对不同操作系统设定单独或多系统访问控制策略。动态访问控制策略支持“与”、“或”条件嵌套,并可通过单一条件或条件组的方式灵活组合嵌套,可支持多种条件变量设置,当检测到不符合安全条件时,支持如短信增强认证、告警等灵活的补救动作,实现灰度处置,有效平衡员工访问体验和安全保障		
			DNS解析： 支持以私有DNS发布企业资源,无需额外购买DNS服务即可使用域名访问内网资源,支持管理员自主配置是否允许从具体网络区域(局域网/互联网)接入时使用此私有DNS解析地址。		
			客户端自动选路： 为了提升终端用户访问体验,对于多线路接入单网关访问业务的场景,支持时延优先的选路模式,支持周期性探测线路时延和多次探测确认恶化后切换。多网关接入访问业务的场景,支持最低时延+相对时延阈值随机选择策略。(需提供产品功能截图证明)		
			沙箱场景配置： ▲沙箱功能应支持通过功能配置的变更,适配对应使用环境和场景： 1) 支持在互联网办公PC对隧道应用的网络访问进行权限隔离,仅通过沙箱空间允许对隧道应用的访问和数据留存加密。 2) 支持在内网办公PC对互联网网络访问进行权		

			限隔离，仅通过上网沙箱应用进行互联网访问。 (需提供产品功能配置截图)		
			PC 端沙箱： ▲为了满足 PC 端数据防泄密需求，零信任平台需支持在 PC 终端上基于沙箱技术生成隔离的安全工作空间（非容器类型），且无需再额外搭建服务端设备、组件。PC 沙箱应支持统信 UOS、麒麟 Kylin 等主流系统。（需提供公安部计算机信息系统安全产品质量监督检验中心出具的检测报告）		
			沙箱文件加密： ▲支持以文件为单位，对工作应用产生的数据进行加密保存；文件加密支持“一文一密”即每个文件独立密钥，以确保沙箱组件被卸载、模块驱动被摘除的情况下，终端用户仍无法明文取出文件。（需提供第三方权威检测机构出具的带 CNAS 标识的检测报告证明）		
			SPA 单包授权： ▲为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持 UDP+TCP 组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口。安全码支持共享码和一人一码及一次一码三种模式，可通过短信分发安全码。一人一码模式下，当实际登录用户跟分发 SPA 安全码绑定的用户不一致时，零信任系统可以产生安全告警。一次一码模式下激活码被用户使用并正常登录零信任系统后转换为安全码加密存储，换码成功后激活码失效，控制台日志须体现用户首次登录后的换码过程。（需提供产品功能截图及第三方权威检测机构出具的带 CNAS 标识的检测报告证明）		
	质保服务		含 3 年规则升级及原厂服务。		
	产品资质		提供国家版权局颁发的含有“零信任”字样的《计算机软件著作权登记证书》(需提供有效证明材料并加盖公章)		
			无漏洞证明： 为证明所投产品的自身安全性，应具备国家计算机网络应急技术处理协调中心出具的安全众测无漏洞证明文件。(需提供有效证明材料并加盖公章)		
	厂商资质		所投零信任产品应在《IDC 中国零信任网络访问解决方案市场份额，2024》中位列前茅，并出具由 IDC 盖章确认的证明文件，		
			厂商为国家信息安全漏洞共享平台（CNVD）用户组及技术组成员单位		

4	应用、数据容灾备份安全防护系统（5套）	配置要求	支持黄石市第二、四、五、十五冶医院现用灾备系统，完全兼容，实现有效网络安全防护。	含现场网络安全服务	
		功能要求	内置勒索病毒、挖矿、APT 组织等安全事件的专题规则库并定期更新，可配置勒索病毒主动防护策略，实现勒索病毒的监控与隔离；同时匹配漏洞扫描、安全基线设置等高级防护功能，确保备份及恢复环境安全可靠。		
		行为防护	可检测并阻断攻击者利用 powershell 访问互联网行为，可检测并阻断攻击者利用 psExec 工具执行命令行为，可检测并阻断缓冲区溢出漏洞攻击行为，可检测并阻断攻击者利用 powershell 从远端加载恶意文件攻击，可检测并阻断攻击者反射注入 dll 恶意行为。		
		恶意程序防护	可检测并阻断系统内存密码盗窃行为，可检测并阻断攻击者利用代理工具进行内外网穿透行为，可检测并阻断攻击者利用非系统进程尝试劫持 EXE 执行过程行为，可检测并阻断攻击者利用非系统进程尝试劫持自启动过程行为，可检测并阻断攻击者更改系统引导文件行为，可检测并阻断攻击者更改系统可执行文件行为。		
		质保服务	含 3 年规则升级及原厂服务。		
		产品资质	产品具有《国家信息安全测评信息技术产品安全测评证书》（级别 EAL3+）（提供有效证明复印件并加盖公章）		
		厂商资质	产品制造商具备国家信息安全测评信息安全服务资质证书安全开发类二级。（提供有效证书复印件并加盖公章）		
		现场服务	提供日常网络、计算、存储和安全设备的巡检，处理日常运营问题，协助完成突发故障和事件处置，做好管理台账以及每季一次汇报/每年度一次汇报和建议工作。（现场服务详细要求可见本项目服务要求章节）		
5	光纤交换机（2台）	硬件配置	≥32Gb，≥24 端口交换机，≥24 端口激活，含 ≥24 个 16Gb/s 短波模块，全光纤支持级联，单电源（固定），机架套件		
		功能要求	采用 ≥16Gb 光纤通道技术，支持广泛的光纤通道和多功能/融合协议、收发器及线缆产品组合。提供存储网络环境中关键业务数据和应用所需的可扩展性、灵活性、性能、安全性和互操作性，以满足日益复杂的存储环境的需求。		

		质保服务	含 3 年原厂服务。		
--	--	------	------------	--	--

6. 承诺函

6-1 新购设备承诺函

_____（招标人名称）：

我方_____（单位名称）针对鄂东医养集团网络安全升级续保服务项目招标文件的要求，郑重承诺如下：若我方被确定为本项目中标人，我方按清单要求所交付的新购硬件设备均为 2026 年 1 月 1 日（含）以后出厂的新品。

违约责任：若我方违反上述承诺，我方愿承担以下责任：

- （1）向招标人支付合同总金额5%的违约金；
- （2）无条件配合更换符合要求的硬件设备，因交付延期对招标人造成的经济损失、社会恶劣影响等，我方对此承担全部责任；
- （3）招标人有权从应付给我方的款项中直接扣除上述费用；
- （4）我方自愿接受列入不良行为记录名单的处理。

投标人：_____（盖单位章）

法定代表人或其委托代理人：_____（签字或盖章）

_____ 年 ____ 月 ____ 日

6-2 应急响应承诺函

_____（招标人名称）：

我方_____（单位名称）_____针对鄂东医养集团网络安全升级续保服务项目招标文件关于应急响应时间的要求，发生紧急事件时，郑重承诺如下：

- 1、电话/远程响应：____分钟以内；
- 2、技术人员到达现场时间：____分钟以内；
- 3、核心业务恢复时限：____小时以内。

承诺期限：自合同签订之日起至免费质保期内有效。

违约责任：若我方违反上述承诺，我方愿承担以下责任：

- （1）向招标人支付合同总金额5%的违约金；
- （2）因处置不及时对招标人造成的经济损失、社会恶劣影响等，我方对此承担全部责任；
- （3）招标人有权从应付给我方的款项中直接扣除上述费用；
- （4）我方自愿接受列入不良行为记录名单的处理。

投标人：_____（盖单位章）

法定代表人或其委托代理人：_____（签字或盖章）

_____ 年 ____ 月 ____ 日

7、 其他内容格式自拟