陕西省康复医院网络信息系统安全等级保护测评项目

竞争性磋商文件

项目编号：ZX2025-11-37

采购人名称：陕西省康复医院

陕西正信招标有限公司

2025 年 11 月

目　录

第一部分　商务部分

第一章　磋商邀请

项目概况

网络信息系统安全等级保护测评项目采购项目的潜在供应商应在陕西省西安市莲湖区环城西路南段元晟合中心6层获取采购文件,并于2025年12月12日09时30分（北京时间）前提交响应文件。

一、项目基本情况

项目编号：ZX2025-11-37

项目名称：网络信息系统安全等级保护测评项目

采购方式：竞争性磋商

预算金额：220000.00元

采购需求：

合同包1（网络信息系统安全等级保护测评项目）：

合同包预算金额：220000.00元

合同包最高限价：220000.00元

品目号	品目名称	采购标的	数量（单位）	技术规格、参数及要求	品目预算（元）
1-1	软件运维服务	网络信息系统安全等级保护测评	1(项)	详见采购文件	220000.00

本合同包不接受联合体磋商

合同履行期限：根据合同约定

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;

2.落实政府采购政策需满足的资格要求：

合同包1(网络信息系统安全等级保护测评项目)落实政府采购政策需满足的资格要求如下:

本项目为非专门面向中小企业采购。

3.本项目的特定资格要求：

合同包1(网络信息系统安全等级保护测评项目)特定资格要求如下:

（1）法定代表人授权委托书：法定代表人参加磋商的，须出示身份证；法定代表人授权本单位他人参加磋商的，须提供法定代表人授权委托书；

（2）控股管理关系：提供直接控股和直接管理关系清单。若与其他供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则磋商无效；

（3）本项目不接受联合体磋商，不允许分包。供应商应提供《非联合体不分包投标声明》；

（4）供应商具有有效的《网络安全等级测评与检测评估机构服务认证证书》或《网络安全服务认证证书等级保护测评服务认证》。

三、 获取采购文件

时间:2025年11月28日至2025年12月05日,每天上午09:00:00至12:00:00，下午13:30:00至17:00:00（北京时间,法定节假日除外）

途径：西安市莲湖区环城西路南段元晟合中心6层

方式：现场获取

售价：500元

四、 响应文件提交

截止时间： 2025年12月12日09时30分00秒（北京时间）

地点：西安市莲湖区环城西路南段元晟合中心6层开标室一

五、开启

时间：2025年12月12日09时30分00秒（北京时间）

地点：西安市莲湖区环城西路南段元晟合中心6层开标室一

六、公告期限

自本公告发布之日起3个工作日。

七、其他补充事宜

1.购买采购文件时需携带经办人单位介绍信或授权委托书、身份证原

件及复印件加盖公章，售后不退。

2.收款单位：陕西正信招标有限公司

开户银行：中国银行股份有限公司西安四府街支行

银行账号：102460065607。

3.注意事项：报名供应商须按照《陕西省财政厅关于政府采购供应商注册登记有关事项的通知》的要求，通过陕西省政府采购网（http://www.ccgp-shaanxi.gov.cn/）注册登记加入陕西省政府采购供应商库。

4.落实的政府采购政策：

（1）《政府采购促进中小企业发展管理办法》的通知-财库[2020]46号

（2）财政部司法部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

（3）《国务院办公厅关于建立政府强制采购节能产品制度的通知》-国办发〔2007〕51号

（4）《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》-（财库[2019]9号）

（5)《关于印发环境标志产品政府采购品目清单的通知》-(财库〔2019〕18号）

（6）《关于印发节能产品政府采购品目清单的通知》-（财库〔2019〕19号）

（7）《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）

（8)《关于运用政府采购政策支持乡村产业振兴的通知》-(财库〔2021〕19号）

（9）《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）

（10）陕西省财政厅关于印发《陕西省中小企业政府采购信用融资办法》-（陕财办采〔2018〕23号）

（11）《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》-（陕财办采〔2020〕15 号）

（12）《关于进一步加强政府绿色采购有关问题的通知》-（陕财办采〔2021〕29 号）

（13）《陕西省财政厅、中国人民银行西安分行关于深入推进政府采购信用融资业务的通知》-（陕财办采〔2023〕5 号）

若享受以上政策优惠的企业，提供相应声明函或品目范围内产品有效认证证书。

八、凡对本次采购提出询问，请按以下方式联系。

1.采购人信息：

名称：陕西省康复医院

地址：西安市雁塔区电子二路 52 号

联系方式：艾老师 029-89288722

2.采购代理机构信息

名称：陕西正信招标有限公司

地址：西安市莲湖区环城西路南段元晟合中心 6 层

联系方式：029-88110800 转 8032

3.项目联系人

项目联系人：祁鑫　张浥清　蔡丹

电话：029-88110800 转 8032

陕西正信招标有限公司

2025 年 11 月 28 日

第二章　磋商须知

磋商须知前附表

序号	名称	具体内容和要求
1	采购项目	网络信息系统安全等级保护测评项目
	采购预算	220000.00 元
	项目性质	自有资金
	本项目设定的最高限价	220000.00 元
	公告媒体	陕西省政府采购网
	项目属性	服务
	采购标的所属行业	单一属性项目：软件和信息技术服务业
2	采购人	1、名称：陕西省康复医院 2、地址：西安市雁塔区电子二路 52 号 3、电话：029-89288722 4、联系人：艾老师
3	采购代理机构	1、名称：陕西正信招标有限公司 2、地址：西安市莲湖区环城西路南段元晟合中心 6 层 3、电话：029-88110800 转 8032 4、联系人：祁鑫 张浥清 蔡丹
4	申请人资格条件	1、满足《中华人民共和国政府采购法》第二十二条规定： ①具有独立承担民事责任能力的法人、其他组织或自然人，提供合法有效的统一社会信用代码营业执照（事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书，自然人提供身份证）； ②财务状况报告：法人提供会计师事务所出具的有效的 2024 年度审计报告（成立时间至提交响应文件截止时间不足一年的可提供成立后任意时段的资产负债表），或提交自 2025 年 5 月 1 日以来银行出具的资信证明，或信用担保机构出具的投标担保函，（以上三种形式的资料提供任何一种即可）；其他组织和自然人提供

		银行出具的资信证明或财务报表； ③税收缴纳证明：法人提供自 2024 年 11 月 1 日以来至少一个月的纳税证明或完税证明，纳税证明或完税证明上应有代收机构或税务机关的公章或业务专用章；其他组织和自然人提供自 2024 年 11 月 1 日以来至少一个月缴纳税收的凭据；依法免税的或者依法不需缴税的供应商应提供相关文件证明； ④社会保障资金缴纳证明：提供自 2024 年 11 月 1 日以来至少一个月已缴纳的社会保障资金的证明（社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明等）；依法不需要缴纳社会保障资金的供应商应提供相关文件证明； ⑤提供具有履行本合同所必需的设备和专业技术能力的声明； ⑥参加本次采购活动前 3 年内在经营活动中没有重大违纪，以及未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的书面声明； **以上②-④项，提供“陕西省政府采购供应商信用承诺书”的，可不再提供其他证明文件。** 2、落实政府采购政策需满足的资格要求： 本项目为非专门面向中小企业采购。 3、本项目的特定资格要求： ①法定代表人授权委托书：法定代表人参加磋商的，须出示身份证；法定代表人授权本单位他人参加磋商的，须提供法定代表人授权委托书； ②控股管理关系：提供直接控股和直接管理关系清单。若与其他供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则磋商无效； ③本项目不接受联合体磋商，不允许分包。供应商应提供《非联合体不分包投标声明》； ④供应商具有有效的《网络安全等级测评与检测评估机构服务认证证书》或《网络安全服务认证证书等级保护测评服务认证》。 备注： 1、以上资格要求均为必备资格，缺项或未按要求响应的视为无效响应； 2、分支机构参与磋商时，须提供分支机构的资格要求证明文件；

		响应文件中应附法人（非负责人）出具的法定代表人授权委托书。法人只能授权一家分支机构参与磋商，且不能与分支机构同时参加本项目磋商； 3、事业单位法人参与磋商可不提供财务状况报告、社会保障资金缴纳证明及税收缴纳证明； 4、以上资格要求国家有最新规定的，以国家最新规定为准，旧证在有效期内的仍然认可。
5	现场踏勘	不组织
6	样品	不要求提供
7	联合体磋商	不接受
8	采购进口产品	本项目拒绝进口产品参加磋商
9	政府采购强制采购:节能产品	否
	政府采购优先采购:节能产品	
	政府采购优先采购:环境标志产品	
10	政府采购强制采购:信息安全认证	否
	政府采购优先采购:农副产品	本项目不适用
11	支持中小企业	非专门面向中小企业采购项目(价格扣除): 1、对小型和微型企业的价格给予 10%～20%的扣除，用扣除后的价格参与评审。本项目的扣除比例为：小型企业扣除 10%，微型企业扣除 10%。 2、如果一个货物项目或包含有多个采购标的，只有当供应商提供的每个标的均由小微企业制造，才能享受 10%-20%的价格扣除政策。如果小微供应商提供的货物既有中型企业制造货物，也有小微企业制造货物的，不享受价格扣除相关政策。 3、采购人应当根据政府采购有关规定和采购项目的实际情况，确

		定拟采购项目是货物、工程还是服务项目。享受中小企业扶持政策的供应商应当满足下列条件：在货物采购项目中，货物应当由中小企业制造，不对其中涉及的服务的承接商作出要求；在工程采购项目中，工程应当由中小企业承建，不对其中涉及的货物的制造商和服务的承接商作出要求；在服务采购项目中，服务的承接商应当为中小企业，不对其中涉及的货物的制造商作出要求。	
	支持监狱企业	1、非专门面向监狱采购项目(价格扣除)：监狱企业可视同小微企业在价格评审时给予10%～20%的扣除，用扣除后的价格参与评审。本项目的扣除比例为：扣除10%。 2、监狱企业属于小型、微型企业的，不重复享受政策。	
12	其他法律法规强制性规定或扶持政策	残疾人福利性单位可视同小微企业在价格评审时给予10%～20%的扣除，用扣除后的价格参与评审。 本项目的扣除比例为：扣除10%；但应满足下列条件： 1、残疾人福利性单位应符合《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）文件规定，并提供《残疾人福利性单位声明函》。 2、残疾人福利性单位属于小型、微型企业的，不重复享受政策。	
13	陕西省财政厅、中国人民银行西安分行关于深入推进政府采购信用融资业务的通知	业务流程	具体操作流程详见中征平台政府采购信用融资业务(即“政采贷”业务) http://www.ccgp-shaanxi.gov.cn/freecms/site/shanxi/1128/info/2023/2206952.html
		办理平台	中国人民银行征信中心应收账款融资服务平台： https://www.crcrfsp.com/
14	供应商须提供的其他资料	供应商根据实际情况填写(如业绩证明材料、人员投入情况、供货承诺等)	
15	澄清或者修改时间	1、对已发出的磋商文件进行必要澄清或者修改的，在原刊登磋商公告的媒体上发布更正公告，并以书面形式通知所有磋商文件收受人。 2、澄清或修改的内容可能影响响应文件编制的，采购人或者采购代理机构应当在提交首次响应文件截止之日5日前，以书面形式通知所有接受磋商文件的供应商，如果澄清或者修改时间距本章磋商须知前附表规定的磋商截止时间不足5日，将相应顺延提交	

		响应文件的截止时间。 3、澄清或者修改内容为磋商文件的组成部分，对所有领取磋商文件的供应商均具有约束力。
16	响应文件递交截止时间和地点	1、时间：2025-12-12 09:30:00(北京时间) 2、地点：西安市莲湖区环城西路南段元晟合中心 6 层开标室一
17	磋商时间和地点	1、时间：响应文件递交截止时间 2、地点：西安市莲湖区环城西路南段元晟合中心 6 层开标室一
18	磋商保证金	**磋商保证金收取：** 1、要求提供，金额不得超过采购项目预算金额的 2%，本项目的磋商保证金为：人民币肆仟壹佰壹拾叁元柒角（¥4113.7 元），须提交到以下指定账户。 2、磋商保证金收款账户： **户名：陕西正信招标有限公司** **账号：102119413784** **开户行：中国银行西安北大街支行营业部** 以转账方式交纳磋商保证金须注明项目编号及用途(磋商保证金)，查询电话：029-88110800 转 8008 3、交纳方式：磋商保证金应当以转账、支票、汇票、本票、保函等非现金形式提交。 4、交纳截止时间：响应文件递交截止时间。 备注： （1）磋商保证金须从供应商户名支付，如从个人户名或非供应商户名支付，将被拒绝，视为自动放弃磋商权利（该个人是供应商的情形除外）；以保函形式交纳投标保证金的，投标人应在投标截止时间前将保函扫描成清晰的 PDF 文件，发送至邮箱 2559647209@qq.com（邮件命名：项目编号），并将保函原件单独递交至代理机构财务；投标人应在投标文件中附保函复印件。保函必须由具有开具投标保函资格的单位开具；若供应商违约，开具保函单位承担连带责任； （2）磋商保证金的提交金额、时间不满足磋商文件要求的，投标无效； （3）磋商保证金以采购代理机构到账凭证为准，供应商无需更换

		交纳凭证，由采购代理机构统一提供。 （4）未按指定账户提交的，我公司将退回，供应商须在文件递交截止时间前按照指定账户再次提交。
		磋商保证金退还： 未成交供应商的保证金，在成交通知书发出后5个工作日内全额退还；成交供应商的保证金，在服务费足额到账3个工作日内或收到合同3个工作日内退还中标单位保证金，但因供应商自身原因导致无法及时退还的除外。
19	磋商响应有效期	自磋商响应文件截止时间起90日（日历日）
20	响应文件份数	正本壹份，副本贰份，U盘壹份(封装在正本中)
	U盘须包含的内容	内含响应文件正本的Word版本及盖章扫描后的PDF版本
21	响应文件封套上应载明的信息	(网络信息系统安全等级保护测评项目)磋商响应文件（正本、副本、U盘） 项目编号：ZX2025-11-37 在2025-**-** **:**:**之前不得启封 供应商名称：
22	信用查询	1、查询渠道：“信用中国”（www.creditchina.gov.cn）和“中国政府采购”（ccgp.gov.cn）为供应商信用信息查询渠道。 2、查询截止时点 ：响应文件递交截止时间。 3、查询记录和留存方式：供应商在磋商截止时间前自行查询并提交《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声明函》，查询截图可附在声明函之后；采购人或者采购代理机构应当在评审现场进行复查，所有记录以复查结果为准，查询记录随其他采购文件一并保存。 备注： 1、供应商在参加政府采购活动前3年内因违法经营被禁止在一定期限内参加政府采购活动，期限届满的，可以参加政府采购活动，但应提供期限届满的证明材料。 2、《中华人民共和国政府采购法实施条例》第十九条 重大违法记录，是指供应商因违法经营受到刑事处罚或者责令停产停业、吊

<table>
<tr><td></td><td></td><td>销许可证后者执照、较大数额罚款等行政处罚。
3、财库[2022]3号文件，《中华人民共和国政府采购法实施条例》第十九条第一款规定的“较大数额罚款”认定为200万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于200万元的，从其规定。</td></tr>
<tr><td>23</td><td>★提供服务的时间、地点等</td><td>1、服务期：一年
2、服务地点：陕西省康复医院指定地点</td></tr>
<tr><td>24</td><td>★采购资金的支付方式和时间</td><td>1、结算单位：采购人结算，在付款前必须开具等额发票给采购人。
2、付款方式：合同签订后支付合同总金额的30%，采购人收到检测报告及供应商开具的正式发票后，支付合同总金额的40%。采购人每季度收到供应商巡检报告，按季度支付合同总金额的7.5%，直至服务结束支付完成。</td></tr>
<tr><td>25</td><td>履约保证金</td><td>不要求提供</td></tr>
<tr><td>26</td><td>代理服务费</td><td>1、代理服务费：参照附件下浮15%收取，按照差额定率累进法计算，由中标人支付。
2、支付方式：成交供应商应在领取通知书的同时，支付本项目代理服务费。
代理服务费收款账户：
单位名称：陕西正信招标有限公司
开户银行：中国银行股份有限公司西安四府街支行
银行账号：102460065607
3、附件：
<table>
<tr><td>服务类型/费率/中标金额（万元）</td><td>货物招标</td><td>服务招标</td><td>工程招标</td></tr>
<tr><td>100以下</td><td>1.5%</td><td>1.5%</td><td>1.0%</td></tr>
<tr><td>100-500</td><td>1.1%</td><td>0.8%</td><td>0.7%</td></tr>
<tr><td>500-1000</td><td>0.8%</td><td>0.45%</td><td>0.55%</td></tr>
<tr><td>1000-5000</td><td>0.5%</td><td>0.25%</td><td>0.35%</td></tr>
<tr><td>5000-10000</td><td>0.25%</td><td>0.1%</td><td>0.2%</td></tr>
<tr><td>10000-100000</td><td>0.05%</td><td>0.05%</td><td>0.05%</td></tr>
<tr><td>1000000以上</td><td>0.01%</td><td>0.01%</td><td>0.01%</td></tr>
</table>
例如：某服务采购成交金额为678.2万元，代理服务费计算如下：</td></tr>
</table>

		100 万元*1.5%=1.50 万元 (500-100)*0.8%=3.20 万元 (678.2-500)*0.45%=0.8019 万元 服务费=1（1.50+3.20+0.8019）*0.85=4.676615 万元。 **4、转账时请备注：251137 项目服务费。**
27	报价组成	磋商报价是指完成本项目的所有费用，以磋商文件的内容和要求作为响应依据。
28	其他	1、磋商文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行； 2、正文与前附表表述不一致时，以磋商须知前附表为准。

磋商须知正文

一、总则

1.定义

1.1“采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。本次政府采购的采购人名称、地址、电话、联系人见磋商须知前附表。

1.2“采购代理机构”是指接受采购人委托，代理采购项目的集中采购机构和其他采购代理机构。本次政府采购的采购代理机构名称、地址、电话、联系人见磋商须知前附表。

1.3“供应商”是指响应磋商文件要求、参加竞争性磋商采购的法人、其他组织或者自然人。本次政府采购项目邀请的供应商通过磋商须知前附表所述方式产生。

1.3.1 供应商应当经过正常渠道购买磋商文件，供应商名称与购买磋商文件时登记的供应商名称应当相符。

1.3.2 分支机构参与投标的，必须出具总公司授权书，以自己的名义从事民事活动，产生的民事责任由法人承担；也可以先以该分支机构管理的财产承担，不足以承担的，由法人承担。

1.4“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。

1.5 “磋商小组”由采购人代表和评审专家共3人以上单数组成，其中评审专家人数不得少于磋商小组成员总数的2/3。

1.6“货物”是指各种形态和种类的物品，包括原材料、燃料、设备、产品等。

1.7“服务”是指除货物和工程以外的其他政府采购对象。

1.8“进口产品”是指通过中国海关报关验放进入中国境内且产自关境外的产品。

2.采购项目预算及最高限价

2.1本项目采购资金已列入政府采购预算，预算金额见磋商须知前附表。

2.2本项目最高限价要求见供应商须知前附表。

3.供应商的资格要求

3.1供应商应当符合磋商须知前附表中规定的资格条件要求。

3.2供应商存在下列情形之一的不得参加竞争性磋商：

3.2.1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，不得参加同一合同项下的政府采购活动。为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

3.2.2因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，或者存在财政部门认定的其他重大违法记录，以及在财政部门禁止参加政府采购活动期限以内的。

4.参与磋商的费用

4.1无论磋商的结果如何，供应商应自行承担所有与竞争性磋商采购活动有关的全部费用。

5.授权委托

5.1供应商代表为供应商法定代表人的，应持有法定代表人身份证明。供应商代表不是供应商法定代表人的，应持有法定代表人授权书，并附授权代表的身份证明及法定代表人身份证明，详见磋商须知前附表。

6.联合体形式

6.1 本项目是否接受联合体参与及相关要求见磋商须知前附表。

7.项目现场踏勘

7.1　本项目是否组织现场踏勘见磋商须知前附表。

8.采购进口产品

8.1 本项目是否采购进口产品及相关要求见磋商须知前附表。

9.政府采购政策支持与其他规定

9.1　供应商享受支持中小企业发展政策优惠的，可用扣除后的最后报价参与价格比较。本项目价格扣除比例及相关要求见供应商须知前附表。参加政府采购活动的供应商应提供《中小企业声明函》。

9.2　监狱企业视同小型、微型企业，享受促进中小企业发展政策优惠，可用扣除后的最后报价参与价格比较。本项目价格扣除比例及相关要求见供应商须知前附表。监狱企业参加政府采购活动时，应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的证明文件。

9.3 残疾人福利性单位视同小型、微型企业，享受促进中小企业发展政策优惠，可用扣除后的最后报价参与价格比较。本项目价格扣除比例及相关要求见磋商须知前附表。符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》。

9.4 其他法律法规强制性规定。本项目的详细要求见磋商须知前附表。

二、磋商文件

10.磋商文件的组成

10.1 磋商文件由下列文件组成：

第一部分　商务部分

第一章　磋商邀请

第二章　磋商须知

第三章　评审方法及标准

第四章　合同草案条款

第五章　响应文件组成

第二部分　技术部分

第六章　项目采购需求

10.2 磋商须知前附表规定的提交首次响应文件截止时间前，对磋商文件进行澄清或者修改的内容，为磋商文件的组成部分。

10.3　磋商小组根据与供应商磋商情况可能实质性变动的内容，包括采购需求中的技术、服务要求以及合同草案条款，对磋商文件作出的实质性变动是磋商文件的有效组成部分。

10.4　供应商应仔细阅读磋商文件的全部内容，按照磋商文件要求的内容编制响应文件。任何对磋商文件的忽略或误解不能作为响应文件存在缺陷或瑕疵的理由，其风险由供应商承担。

11.磋商文件的澄清或者修改

11.1 在磋商须知前附表规定的提交首次响应文件截止之日前，采购代理机构可以对已发出的磋商文件进行必要的澄清或者修改。

11.2 澄清或者修改的内容可能影响响应文件编制的，应当在磋商须知前附表规定的提交首次响应文件截止之日 5 日，以书面形式通知所有接收磋商文件的供应商，不足 5 日的，顺延供应商提交首次响应文件截止时间。

11.3 澄清或者修改内容为磋商文件的组成部分，对所有接收了磋商文件的供应商均具有约束力。

12.偏离

12.1 本条所称偏离为响应文件对磋商文件第一部分的偏离，即不满足或不响应磋商文件的要求。

三、响应文件

13.一般要求

13.1 供应商应仔细阅读磋商文件的所有内容，必须按磋商文件的要求编制响应文件，并保证所提供的全部资料的真实性，以使其响应文件对磋商文件做出实质性的响应。

13.2 供应商提交的响应文件及供应商与采购人或采购代理机构、磋商小组就有关磋商的所有来往函电必须使用中文。供应商可以提交其他语言的资料，但应附中文注释，在有差异时以中文为准。

13.3 除技术要求另有规定外，本文件所要求使用的计量单位均采用国家法定的度、量、衡标准单位计量。未列明时亦默认为我国法定计量单位。

13.4 供应商应当按磋商文件中提供的响应文件内容进行填写。

13.5 磋商响应文件应采用书面形式，磋商文件中要求提供电子版的，必须按要求提供。

14.响应文件的组成

14.1 响应文件应包括但不限于下列内容：

14.1.1 商务部分

(1)磋商响应声明

(2)报价一览表及分项价格表

(3)商务部分偏离表

(4)供应商符合资格条件的证明文件

(5)符合政府采购政策的证明材料

(6)其他资料

14.1.2 技术部分

(1)服务响应偏离表

(2)服务方案

(3)组织机构

(4)服务承诺

(5) 供应商认为需要提供的其他资料

14.2 本项目是否要求提供样品的见磋商须知前附表。

14.3 在磋商过程中，供应商提交的最后报价(或者重新提交的响应文件和最后报价)是响应文件的有效组成部分。

14.4 磋商文件规定可能发生实质性变动的，供应商应当在《服务/商务

响应偏离表》中的对应内容处注明。

14.5 供应商无论成交与否，其响应文件不予退还。

15.报价

15.1 供应商应当按磋商文件规定的服务要求、责任范围和合同条件，以人民币进行报价。

15.2 供应商必须按报价一览表和分项价格表要求的内容填写各项货物及服务的分项价格和总价。供应商在磋商须知前附表规定的提交首次响应文件截止之日前修改报价一览表中的报价的，应同时修改其分项价格表中的报价。

16.磋商保证金

16.1 本项目是否交纳磋商保证金详见磋商须知前附表。

16.2 未成交供应商的保证金，在成交通知书发出后 5 个工作日内全额退还；成交供应商的保证金，在服务费足额到账 3 个工作日内或收到合同 3 个工作日内退还中标单位保证金，但因供应商自身原因导致无法及时退还的除外。

16.3 有下列情形之一的，保证金不予退还：

(1)供应商在磋商须知前附表规定的提交首次响应文件截止时间后撤回响应文件的；

(2)供应商在响应文件中提供虚假材料的；

(3)除因不可抗力或磋商文件认可的情形以外，成交供应商不与采购人签订合同的，在签订合同时向采购人提出附加条件的；

(4)供应商与采购人、其他供应商或者采购代理机构恶意串通的；

17.磋商响应有效期

17.1 磋商响应有效期见磋商须知前附表，在此期间响应文件对供应商具有法律约束力。响应文件有效期从磋商须知前附表规定的提交首次响应文件截止时间之日起计算。磋商响应有效期不足的将被视为无效响应。

18.响应文件的签署及规定

18.1 供应商应根据磋商须知前附表规定提交响应文件。纸质文件的正

本和副本应分别装订成册。正本、副本的封面上应标记“正本”“副本”的字样，当正本和副本、电子版内容有差异时，以正本为准。

18.2 响应文件正本和副本应用不褪色的材料打印或书写，并按磋商文件要求在签字盖章处加盖公章和由法定代表人或其授权代表签字或盖章。响应文件中的任何加行、涂改、增删，应加盖单位公章或由法定代表人或其授权代表签字确认。否则，将导致响应文件无效。

18.3 在磋商过程中，供应商按磋商文件规定和磋商小组要求重新提交的响应文件和最后报价，应打印或用不褪色墨水书写，并由法定代表人或其授权代表签字或加盖单位公章。否则，将导致响应文件无效。

18.4 副本可以是正本的复印件。

19.响应文件的密封和标记

19.1 响应文件应当密封并加贴封条。

19.2 响应文件封套或外包装上应写明的内容见磋商须知前附表。

19.3 响应文件未密封和标记，采购人或采购代理机构应当拒绝接收。

20.响应文件的递交

20.1 响应文件应在磋商须知前附表规定的提交时间和指定地点提交。

20.2 在截止时间后送达的响应文件为无效文件，采购代理机构应当拒收。

20.3 响应文件应当由法定代表人或授权代表递交并参与现场磋商。

21.响应文件的补充、修改或者撤回

21.1 供应商在磋商须知前附表规定的提交首次响应文件截止时间前，可以对所提交的首次响应文件进行补充、修改或者撤回，并书面通知采购代理机构，该通知应有供应商法定代表人或其授权代表签字。

21.2 修改、补充的内容为响应文件的组成部分。修改、补充的响应文件应按本章第 18、19、20 项规定编制、签署、密封、标记和递交，并标明“修改、补充”字样。

21.3 补充、修改的内容与响应文件不一致时，以补充、修改的内容为准。

四、磋商与评审

22.磋商小组

22.1 磋商与评审由依法组建的磋商小组负责，磋商小组由采购人代表和评审专家组成。

采购人委派代表参加评审委员会的，要向采购代理机构出具授权函。

23. 初步审查

23.1 资格性审查：由采购人或出具授权委托招标代理机构对供应商的资格进行审查。

合格供应商不足 3 家的，不得继续进行磋商，26.5 情形除外。

供应商不具备磋商文件规定的供应商资格条件的，应在资格审查时按照无效响应处理。

23.2 磋商小组应当对供应商提交的首次响应文件进行初步审查，包括响应文件的有效性、完整性、符合性。除可变动的技术、服务要求以及合同草案条款外，首次提交的响应文件有下列情况之一，其响应文件无效，磋商小组应当告知有关供应商。

(1) 响应文件未按照磋商文件规定份数提交的；

(2)未按照磋商文件规定要求签署、盖章的；

(3)响应有效期不足的或无有效期的；

(4)报价超过磋商文件中规定的预算金额或最高限价的；

(5)不满足本磋商文件中标注“★”的实质性条款要求的；

(6)法律、规章、规范性文件和磋商文件规定的其他无效情形。

24.澄清

磋商小组在对响应文件(包括首次响应文件、重新提交的响应文件)的有效性、完整性和对磋商文件的响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。该要求应当以书面形式作出。供应商的澄清、说明或者更正应当采用书面形式，由其法定代表人或其授权代表签字，供应商的澄清、说明或者更正不得超出磋商文件的范围或者改变响应文件的实质性内容。

25.磋商

25.1 初审结束后，磋商小组所有成员集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。供应商应派其法定代表人或授权代表参加磋商。

25.2 在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

25.3 对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。

25.4 供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

25.5 磋商文件不能详细列明采购标的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案。

25.6 磋商小组应当根据实际情况与供应商进行磋商。

25.7 已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。采购代理机构应当退还退出磋商的供应商的磋商保证金。

25.8 磋商结束后，供应商按照磋商小组要求重新提交的响应文件，不满足磋商文件及变动后的技术、服务要求以及合同草案条款的实质性要求的，将视为无效响应文件。

26.最后报价

26.1 磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价。

26.2 二轮报价为最后报价。

26.3 磋商文件不能详细列明采购标的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案，并

要求其在规定时间内提交最后报价。

26.4 最后报价是供应商响应文件的有效组成部分。如磋商小组没有对磋商文件作实质性变动或增加新的需求，最后报价不得高于首轮报价。

26.5 采用竞争性磋商采购方式组织实施的市场竞争不充分的科研项目、需要扶持的科技成果转化项目，以及政府购买服务项目(含政府和社会资本合作项目)，符合要求的供应商(社会资本)只有 2 家的，竞争性磋商采购活动可以继续进行。

27.报价评审

27.1 报价计算错误修正的原则

(1)报价的大写金额和小写金额不一致的，以大写金额为准。

(2)总价金额与按分项报价汇总金额不一致的，以分项报价金额计算结果为准。

(3)分项报价金额小数点有明显错位的，应以总价为准，并修改分项报价。

(4)如果供应商不接受对其错误的更正，其报价将被视为无效报价或确定为无效响应。

27.2 价格得分：以供应商的最后报价作为价格评分依据。

价格评分统一采用低价优先法计算，即满足磋商文件要求且价格最低的评审价为评审基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：

价格评分＝(评审基准价/评审价)×价格分

28.综合评审

28.1 经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。

28.2 评审办法及标准见第三章。

28.3 评审时，磋商小组成员应当独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

29.提出成交供应商

29.1 磋商小组应当按照综合评分由高到低的顺序提出 3 名以上成交候选供应商，并编写评审报告。符合上述 26.5 情形的，可以推荐 2 家成交候选供应商。

29.2 评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照服务方案得分由高到低顺序推荐。评审得分且最后报价且服务方案得分均相同的，由采购人代表确定排序（采购人代表缺席时，由磋商小组确定排序）。响应文件满足磋商文件全部实质性要求，且按照评审因素的量化指标评审得分最高的供应商为排名第一的成交候选人。

30.确定成交供应商

30.1 采购代理机构应当在评审结束之日起 2 个工作日内将评审报告送采购人确认。

30.2 采购人应当在收到评审报告之日起 5 个工作日内，从评审报告提出的成交候选供应商中，按照排序由高到低的原则确定成交供应商。

31.磋商终止

31.1 出现下列情形之一的，应当终止竞争性磋商采购活动，在财政部指定的媒体上发布项目终止公告并说明原因，重新开展采购活动：

(1)因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

(2)出现影响采购公正的违法、违规行为的；

(3)除市场竞争不充分的科研项目、需要扶持的科技成果转化项目，以及政府购买服务项目外，在采购过程中符合竞争要求的供应商或者报价未超过采购预算的供应商不足 3 家的，或者提交最后报价的供应商少于 3 家的；

(4)因重大变故，采购任务取消的。

32.重新评审

32.1　除资格性检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观分评分不一致、经磋商小组一致认定评分畸高、畸低的情形外，采购人或者采购代理机构不得以任何理由组织重新评审。

33.保密

33.1 磋商小组成员以及与评审工作有关的人员不得泄露评审情况以及

评审过程中获悉的国家秘密、商业秘密。

34.禁止行为

34.1 供应商不得与采购人、采购代理机构、其他供应商恶意串通；不得向采购人、采购代理机构或者磋商小组成员行贿或者提供其他不正当利益；不得提供虚假材料谋取成交；不得以任何方式干扰、影响采购工作。

五、成交结果信息公布与签订合同

35.成交信息的公布

35.1 成交供应商确定之日起 2 个工作日内，采购代理机构应在磋商须知前附表中规定的公告媒体上公布成交结果信息。

35.2 磋商文件随成交结果同时公告。但成交结果公告前磋商文件已公告的，不再重复公告。

35.3 采用书面推荐供应商参加采购活动的，在公告结果同时公告采购人和评审专家的推荐意见。

35.4 成交供应商享受本办法规定的中小企业扶持政策的，采购人、采购代理机构应当随成交结果公开成交供应商的《中小企业声明函》。

36.成交通知

36.1 成交供应商确定后，采购代理机构在发布成交公告的同时以书面形式向成交供应商发出成交通知书。成交通知书对采购人和成交供应商具有同等法律效力。

37.履约保证金

37.1 本项目是否缴纳履约保证金详见磋商须知前附表。

38.签订合同

38.1 磋商文件、成交供应商的响应文件及补充文件等均为签订政府采购合同的依据。

38.2 成交供应商应当在成交通知书发出之日起25日内与采购人签订政府采购合同。

38.3 采购人不得向成交供应商提出超出磋商文件以外的任何要求作为签订合同的条件，不得与成交供应商订立背离磋商文件确定的合同文本以

及背离采购标的、规格型号、采购金额、采购数量、技术和服务要求等实质性内容的协议。

38.4 自政府采购合同签订之日起2个工作日内，本项目政府采购合同在磋商须知前附表规定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

38.5 政府采购合同履行中，采购人需追加与合同标的相同的货物、工程或者服务的，在不改变合同其他条款的前提下，可以与成交供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十；

38.6 成交供应商因不可抗力或者自身原因不能履行政府采购合同的，采购人可以与排位在成交供应商之后第一位的成交候选人签订政府采购合同，以此类推，也可以重新开展磋商活动。因自身原因拒绝签订政府采购合同的成交供应商不得参加对该项目重新开展的磋商活动。

38.7 成交后，成交供应商应按照合同约定履行义务，完成磋商项目的供货，经采购人同意，成交供应商可以依法采取分包方式履行合同。分包部分为成交项目的部分非主体、非关键性工作。接受分包的供应商应当具备相应的资格条件，并不得再次分包。分包履行的，成交供应商就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

38.8 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。

六、其他规定

39.代理服务费

39.1 成交供应商是否交纳代理服务费及相关要求见磋商须知前附表。

40.询问、质疑、投诉

40.1 供应商对政府采购活动事项有疑问的，可以向采购人提出询问，采购人应当及时作出答复，但答复的内容不得涉及商业秘密。

40.2 供应商认为磋商文件、磋商过程和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

形式向采购代理机构一次性提出针对同一采购程序环节的质疑，两次或多次对同一采购程序环节提出的质疑函可以拒收。

40.3 不在法定质疑期内提出的质疑函可以拒收；不符合要求的质疑函在法定质疑期内及时补充完整，否则作质疑不成立处理。

40.4 供应商提出质疑的，应当以书面形式向采购代理机构提交质疑函和必要的证明材料。质疑函应当包括的内容详见中国政府采购网《政府采购供应商质疑函范本》。

40.5 质疑书应当由供应商法定代表人或其授权的磋商代表签字并加盖供应商公章，质疑书由授权的磋商代表签字的应附供应商法定代表人委托授权书。

40.6 供应商对采购代理机构的答复不满意，或采购代理机构未在规定的期限作出答复的，可在答复期满后 15 个工作日内，按政府采购法律法规规定及程序，向采购人同级财政部门提出投诉。

40.7 接收质疑函的方式：书面形式

联系部门：项目中心

联系人：张浥清　祁鑫

联系电话：029-88110800 转 8032

电子邮箱：438904813@qq.com

通讯地址：西安市莲湖区环城西路南段元晟合中心 6 层

41.成交供应商有下列情形之一的,将被列入不良行为记录名单,在 1～3 年内禁止参加政府采购活动，并予以通报：

(1)成交后无正当理由不与采购人签订合同的；

(2)未按照采购文件确定的事项签订政府采购合同，或者与采购人另行订立背离合同实质性内容的协议的；

(3)拒绝履行合同义务的；

(4)《政府采购法》第七十七条和《政府采购法实施条例》第七十二条规定的其他情形；

(5)其他违反法律法规相关规定的情形。

42.其他规定

42.1 磋商文件的其他规定见磋商须知前附表。

43.未尽事宜

43.1 其他未尽事宜按政府采购法律法规的规定执行。

44.文件解释权

44.1 本磋商文件的解释权归采购代理机构所有。

第三章　评审方法及标准

采用综合评分法，评审因素见下表（满分 100 分）：

序号	评分因素	分值	评分标准
1	磋商报价（15 分）	15	价格分统一采用低价优先法计算，即满足磋商文件要求且磋商价格最低的磋商报价为评标基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算： 价格分=(评标基准价／磋商报价)×报价分值 注：1、计算分数时四舍五入取小数点后两位； 2、落实采购政策：参见供应商须知前附表。
2	服务方案（70 分）	10	**整体实施方案** 供应商对项目需求进行深入分析，从等级保护测评、渗透测试、安全等方面围绕测评准备、方案编制、现场测评、分析与报告阐述项目工作流程和整体实施方案。 满足磋商文件要求，无瑕疵：10 分； 每存在一处瑕疵扣 1 分； 存在 10 处及以上瑕疵或未提供，不计分。
		10	**等级保护测评服务方案** 针对等级保护测评有完整的服务方案，包含但不限于安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评，以及安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等，并严格遵循相关流程要求。 满足磋商文件要求，无瑕疵：10 分； 每存在一处瑕疵扣 1 分； 存在 10 处及以上瑕疵或未提供，不计分。
		10	**差异化测评服务及风险分析** 分析平台安全情况与等级保护基本要求的差距，提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，针对整改项进行再次测评，配合采购人安全整改工作。 满足磋商文件要求，无瑕疵：10 分；

			每存在一处瑕疵扣 1 分； 存在 10 处及以上瑕疵或未提供，不计分。
		8	**项目质量管理** 有严格的项目质量管理，过程控制及监控手段，能保证技术人员按照相应的操作指导规范实施测评；明确每项工作的时间安排、操作时间和操作人员。 满足磋商文件要求，无瑕疵：8 分； 每存在一处瑕疵扣 1 分； 存在 8 处及以上瑕疵或未提供，不计分。
		6	**风险防范措施** 提供整个测评项目实施过程中的风险防范措施。保证项目运行平稳高效、安全可靠。 满足磋商文件要求，无瑕疵：6 分； 每存在一处瑕疵扣 1 分； 存在 6 处及以上瑕疵或未提供，不计分。
		2	**保密承诺** 供应商提供保密承诺，承诺如若中标，供应商的所有涉密人员均与采购人单位签订专门的保密协议。提供此承诺计 2 分，未提供不计分。
		6	**安全巡检服务** 在项目服务期内，提供至少每季度 1 次的安全巡检服务，并提供详细的安全巡检服务方案。对发现的安全风险，提出风险防范对策并协助采购人整改，提供每月一次风险预警报告。 满足磋商文件要求，无瑕疵：6 分； 每存在一处瑕疵扣 1 分； 存在 6 处及以上瑕疵或未提供，不计分。
		6	**安全培训服务** 提供每季度 1 次的信息安全相关专业知识培训服务，并提供详细的安全培训方案。明确培训方法、培训内容及计划安排。 满足磋商文件要求，无瑕疵：6 分； 每存在一处瑕疵扣 1 分； 存在 6 处及以上瑕疵或未提供，不计分。
		6	**制度体系建设服务**

			供应商提供针对本项目的制度体系建设服务方案，协助采购人建立网络安全管理制度、解决技术问题、构建基础的网络安全管理体系等。 满足磋商文件要求，无瑕疵：6 分； 每存在一处瑕疵扣 1 分； 存在 6 处及以上瑕疵或未提供，不计分。
		6	**应急响应服务** 供应商在项目服务期提供应急响应服务，包括重大事件应急响应及应急处理服务、重要时期保障服务、配合检查服务等。提供详细合理的应急响应服务方案，明确响应时效。 满足磋商文件要求，无瑕疵：6 分； 每存在一处瑕疵扣 1 分； 存在 6 处及以上瑕疵或未提供，不计分。
3	履约能力（12 分）	8	**项目服务团队** 有明确的项目服务团队介绍，并针对本项目成立本地化等级保护测评小组。确保人员稳定，如需更换测评人员，须由采购人同意。 ①团队成员具备高级测评师、中级测评师，提供相应证件，每提供一名高级测评师计 2 分，中级测评师计 1 分，最高得 4 分。 ②供应商提供人员管理及配备方案，明确项目经理和质量负责人，提供团队成员相关履历材料（包括不限于人员履历简介、承担过项目介绍、相关证书等）。 满足磋商文件要求，无瑕疵：4 分； 每存在一处瑕疵扣 1 分； 存在 4 处及以上瑕疵或未提供，不计分。
		4	**业绩**：提供供应商 2022 年 1 月 1 日至今同类项目合同扫描件（以合同签订日期为准），扫描件必须清晰体现签约主体和日期、项目名称及内容、合同金额等核心要素，否则不计为有效业绩。每提供 1 个有效业绩得 1 分，最高得 4 分。 备注：响应文件中提供合同扫描件加盖供应商公章。
4	成果交付（3 分）	3	供应商应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。 确保出具项目成果交付物完

			整、真实并积极配合采购人验收。 满足磋商文件要求，无瑕疵：3 分； 每存在一处瑕疵扣 1 分； 存在 3 处及以上瑕疵或未提供，不计分。
备注： 1、在评审期间，磋商小组只对需要询问的供应商进行询问； 2、本文所称“瑕疵”是指内容缺项、不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；对同一问题前后表述矛盾；存在逻辑漏洞、科学原理或常识错误；不利于本项目目标的实现、现有技术条件下不可能出现的情形等任意一种情形。			

第四章　合同草案条款（仅供参考）

售后服务是软件得以正常使用的保证。为保障采购人的使用效果，特制定本协议。在用甲方认可本协议的情况下，乙方对甲方负有本协议中所列出的责任。

一、服务项目合同模板（可依照项目特性扩展）

需方(甲方)：陕西省康复医院

地　　址：西安市雁塔区电子二路 52 号

电　　话：029-89288722

邮　　编：710065

供方(乙方)：

地　　址：

电　　话：

邮　　编：

联 系 人：

签约地点：西安市雁塔区

根据《中华人民共和国民法典》的规定和甲方需求，本着平等互利、协商一致的原则，经甲乙双方友好协商，特订立本合同，共同遵守。

1．标的物清单

（一）项目名称：网络信息系统安全等级保护测评项目

(二)项目实施地点:陕西省康复医院指定地点;

（三）项目范围：

本项目负责完成陕西省康复医院 2025 年度网络安全等级保护测评服务和其它网络安全保障服务，等级保护测评服务包括定级、备案和测评等服务，从“安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理”等方面开展等级保护测评工作，测评对象为 7 个三级信息系统“医院综合信息系统、电子病历系统、医学影像信息系统（PACS）、陕西省康复医院患者服务平台、心电网络系统、DRG 管理及医保智能审核系

统、传染病智能监测预警前置软件”，1 个二级信息系统“OA 办公系统”；其它网络安全保障服务包括：应急响应及应急处理服务、重要时期保障服务、安全巡检服务、安全培训服务。

(四)项目内容:自本协议签定之日起，乙方提供以下服务。

① 网络安全等级保护测评服务

依据《基本要求》（GB/T 22239-2019）、测评要求》（GB/T 28448-2019）和《测评过程指南》（GB/T 28449-2018）等国家关于网络安全等级保护 2.0 的相关标准和规范要求，为我院提供以上 7 个信息系统等级保护测评实施工作，测评工作包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评，以及安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理 10 个层面测评。在开展网络安全等级保护测评工作过程中要求严格遵循如下流程：

a、定级备案：按照等级保护相关制度要求，本着自主定级的原则，协助我院完成未备案信息系统的定级报告编制、备案表填写，组织相关专家对定级结果进行评审，完善相关资料，递交至公安部门完成定级备案工作。

b、系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状，出具《资产调查表》。

c、现场测评：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果，出具《现场检查表单》。

d、分析整改：分析信息系统安全情况与等级保护基本要求的差距,提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合我院安全整改工作，出具《整改建议书》。

e、等级测评：根据差异化测评以及国家等级测评相关标准及编制的相关等级保护测评指导书进行符合性测评，并进行记录。

f、结论报告（报告编制）：分析当前信息系统安全保护能力是否符合二级的安全要求，针对整改项进行再次测评，提供安全等级符合性测评服务，出具相关信息系统测评报告。

g、配合验收：整理项目过程中所有相关的过程文档，提交我院。按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

② 重大事件应急响应及应急处理服务

在项目服务期内，提供 7×24 小时的信息安全应急处理保障服务。一旦信息系统出现紧急重大安全事件，收到陕西省康复医院的服务请求，测评单位自接到通知 10 分钟内响应，在 2 小时内到达现场，成立应急小组对信息网络应用系统突发的信息安全事件

进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。完成技术服务后需提供相应的《应急响应及应急处理报告》。

③ 重要时期保障服务

在项目服务期内，根据我院实际需要，为我院提供在国家重大政治活动和节假日期间的技术防护保障服务，针对近期可能发生的网络安全威胁，提供技术防护服务，确保活动期间的网络安全可靠运行。

④ 安全巡检服务

在项目服务期内，为我院提供至少每季度 1 次的安全巡检服务，对所有软硬件设备、信息系统进行深度安全巡检，包括但不限于对信息系统中指定的服务器、网络设备、安全设备及安全日志等的安全状态核查。摸清被测系统基础网络环境，从网络安全结构、网络访问控制、网络安全设计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备保护等方面进行安全检查，并开展工具测试包括漏洞扫描，分析存在的网络安全风险，提出风险防范对策并协助我院进行风险问题整改。每月提供一次风险预警报告，如因巡查不及时，未检查出风险项目而被上级和网监部门通报，扣除本季度巡检服务费的 10%。

⑤ 安全培训服务

在项目服务期内，为我院提供每季度 1 次的信息安全相关专业知识培训服务，包含网络安全意识培训及网络安全技术培训，网络安全意识培训内容主要包括：网络安全法知识普及、典型信息安全事件知识案例讲解、安全保密意识建立以及前沿信息安全技术知识培训。安全技术能力培训针对主机安全、应用安全、网络安全、数据库安全相关的检查方法进行培训。 结合我院实际情况，每季度制定一份为全院职工关于网络安全方面的培训内容。

⑥ 制度体系建设服务

在项目服务期内，协助我院建立网络安全管理制度，完善网络安全管理机构部门岗位职能，落实安全责任；协助解决信息系统安全方面存在的技术问题，提高信息系统安全保障水平，保证信息系统安全稳定运行；构建基础的网络安全管理体系，并分类整理相关制度资料、形成胶装文件、电子档案以及管理制度展板制作。

（五）合同总价款：人民币（小写）大写）￥

说明：

1、本合同为一次性包死，不受市场价格变化因素的影响。

2.服务标准

对应《信息安全技术网络安全等级保护基本要求》各安全要求项的测评称为单项测

评。整体测评是在单项测评的基础上，通过进一步分析定级对象安全保护功能的整体相关性，对定级对象实施的综合安全测评。具体测评项如下表：

三级系统测评指标

安全层面	安全子类	测评指标描述
安全物理环境	物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；
		b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；
		b）应将通信线缆铺设在隐蔽安全处；
		c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
	防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地；
		b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
	防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
		b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
		c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
	防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
		c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
	防静电	a）应采用防静电地板或地面并采用必要的接地防静电措施；
		b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；
		b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
		c）应设置冗余或并行的电力电缆线路为计算机系统供电。
	电磁防护	a）电源线和通信线缆应隔离铺设，避免互相干扰；
		b）应对关键设备实施电磁屏蔽。
安全通信网络	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；
		b）应保证网络各个部分的带宽满足业务高峰期需要；
		c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络

安全层面	安全子类	测评指标描述
		区域分配地址； d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
	通信传输	a）应采用校验技术或经国家密码局认证核准的密码技术保证通信过程中数据的完整性； b）应采用国家密码局认证核准的密码技术保证通信过程中数据的保密性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； b）应能够对非授权设备私自联到内部网络的行为进行检查或限制； c）应能够对内部用户非授权联到外部网络的行为进行检查或限制； d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
	访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
	入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻

安全层面	安全子类	测评指标描述
		击时间，在发生严重入侵事件时应提供报警。
	恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
		b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
	安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，具体要求包括： 1)系统应为不同用户提供不同的用户身份标识； 2)系统的用户名和口令不得相同，用户口令应为数字、字母、特殊字符混合组合； 3)用户口令长度应不低于 8 位； 4)系统应具有用户口令定期更新提示和更新确认； 5)禁止明文存储口令。
		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，具体要求包括： 1)宜限制操作系统同一用户连续登录失败次数为 6-10 次，具体次数应在相关安全策略中明确； 2)登录失败超过规定次数，用户账户应被锁定 10 分钟，或申请由系统管理员进行密码重置。
		c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，具体要求包括： 应采用 SSH、Https、VPN 等安全的远程管理方式。
		d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用国家密码

安全层面	安全子类	测评指标描述
		局认证核准的密码技术来实现，具体要求包括： 其中一种鉴别技术宜采用动态口令、数字证书、生物特征或设备指纹。
	访问控制	a）应对登录的用户分配账户和权限；
		b）应重命名或删除默认账户，修改默认账户的默认口令，具体要求包括： 操作系统应禁用无法重命名或无法删除的默认账户，或阻止默认账户直接远程登录。
		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d）应授予管理用户所需的最小权限，实现管理用户的权限分离；
		e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
		f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
		g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d）应对审计进程进行保护，防止未经授权的中断。
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b）应关闭不需要的系统服务、默认共享和高危端口；
		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态

安全层面	安全子类	测评指标描述
		可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	a）应采用校验技术或经国家密码局认证核准的密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
		b）应采用校验技术或经国家密码局认证核准的密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
	数据保密性	a）应采用国家密码局认证核准的密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
		b）应采用国家密码局认证核准的密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；
		b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
		c）应提供重要数据处理系统的热冗余，保证系统的高可用性。
	剩余信息保护	a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
		b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；
		b）应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a）应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
		b）应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数

安全层面	安全子类	测评指标描述
		的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
		e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
		f）应能对网络中发生的各类安全事件进行识别、报警和分析。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
	管理制度	a）应对安全管理活动中的各类管理内容建立安全管理制度；
		b）应对管理人员或操作人员执行的日常管理操作建立操作规程；
		c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
	制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；
		b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理机构	岗位设置	a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
		b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
		c）应设立系统管理员、安全审计员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	a）应配备一定数量的系统管理员、安全审计员和安全管理员等；
		b）应配备专职安全管理员，不可兼任。
	授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
		c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门

安全层面	安全子类	测评指标描述
		和审批人等信息。
	沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
		b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
		c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
		b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
		c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
安全管理人员	人员录用	a）应指定或授权专门的部门或人员负责人员录用；
		b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
		c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
	人员离岗	a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
		b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
	安全意识教育和培训	a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
		b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
		c）应定期对不同岗位的人员进行技能考核。
	外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
		b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
		c）外部人员离场后应及时清除其所有的访问权限；
		d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
安全建设管理	定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
		b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确

安全层面	安全子类	测评指标描述
		性进行论证和审定； c）应保证定级结果经过相关部门的批准； d）应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含国家密码局认证核准的密码技术的相关内容，并形成配套文件； c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定，具体要求包括： 应根据党政机关电子公文系统安全可靠应用推进工作领导小组办公室发布的安全可靠应用相关产品目录采购产品。 b）应确保密码产品与服务的采购和使用符合国家密码管理局的要求； c）应预先对产品进行选型测试，确定产品的候选范围，并及时审定和更新候选产品名单，具体要求包括： 应按照党政机关电子公文系统安全可靠应用推进工作领导小组办公室相关工作要求进行产品选型测试。 d）应通过专有的应用供应渠道下载软件。
	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； c）应制定代码编写安全规范，要求开发人员参照规范编写代码； d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制； e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码； b）应保证开发单位提供软件设计文档和使用指南； c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门

安全层面	安全子类	测评指标描述
		和隐蔽信道。
	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；
		b）应制定安全工程实施方案控制工程实施过程；
		c）应通过第三方工程监理控制项目的实施过程。
	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
		b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
	系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
		b）应对负责运行维护的技术人员进行相应的技能培训；
		c）应提供建设过程文档和运行维护文档。
	等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
		b）应在发生重大变更或级别发生变化时进行等级测评；
		c）应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；具体包括： 应按照党政机关电子公文应用推进工作领导小组办公室的要求和服务商推荐名录选择服务供应商，如集成服务、软件开发等单位；
		b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
		c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
安全运维管理	环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
		b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；
		c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
		b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
		c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
	介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实

安全层面	安全子类	测评指标描述
		行存储环境专人管理，并根据存档介质的目录清单定期盘点；
		b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
		b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
		c）信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；
		d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
	漏洞和风险管理	a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
		b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
	网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
		c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
		e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
		f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
		g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
		h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
		i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口

安全层面	安全子类	测评指标描述
		或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
		j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
	恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
		b）应定期验证防范恶意代码攻击的技术措施的有效性。
	配置管理	a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
		b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
	密码管理	a）应遵循密码相关国家标准和行业标准；
		b）应使用国家密码管理主管部门认证核准的密码技术和产品。
	变更管理	a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
		b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
		c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
	备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；
		b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；
		c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
	安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；
		b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
		c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
		d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
	应急预案管理	a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
		b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

安全层面	安全子类	测评指标描述
		c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
		d）应定期对原有的应急预案重新评估，修订完善。
	外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；
		b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
		c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
		d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

4.付款方式和条件

(一)等保测评服务费

1)、服务费￥(大写:) 元/年，服务期一年。

2)、合同有效期为 年_月_ 日至 年 月 日

3）、服务期限：自签订合同起，服务期一年。

4）服务人员数量及组成：

1. 测评人员要求：本项目的测评人员需具有 1 年以上测评工作经验，项目经理和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方案，确保人员稳定，如需更换测评人员，须由我院同意。

2. 人员配备：投标方参与此项目不少于 6 人，现场测评人员不得少于 4 人，其中至少包含 1 名高级测评师，2 名中级测评师。投标人必须为本项目成立本地化等级保护测评小组，由测评小组组长统一负责，测评小组组长具有一定的技术及管理知识和经验，能容易地与客户沟通，能很好的执

行与完成测评工作，并根据适当情况增加测评人员。

3. 投标人应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

(二)验收与付款方式

1）、验收方式

项目交付物：①《信息系统安全等级保护测评方案》；②《信息系统安全等级测评报告》；③《信息系统整改建议书》；④《信息系统渗透测试报告》；⑤《信息系统安全等级保护定级备案证明》

验收方式：甲方以会议形式，根据合同、招标文件、验收资料等文件，组织项目验收。

2）、付款方式

合同签订后支付合同总金额的30%,采购人收到检测报告及供应商开具的正式发票后,支付合同总金额的40%。采购人每季度收到供应商巡检报告，按季度支付合同总金额的7.5%，直至服务结束支付完成。

(三)支付方式

通过银行转帐方式将款项转入乙方银行帐户。

乙方银行帐户信息如下:

帐户名称:

帐号:

开户行:

甲方仅认可上述指定账户并向该账户付款。如乙方账户信息变更，乙方应出具由法定代表人签署的书面变更文件并加盖乙方公司公章,否则甲

方有权拒绝向指定账户之外的任何账户付款，并且由此导致的付款延迟责任由乙方承担。

(四)结算要求:

乙方要如实开具发票，不得变更开票内容，乙方开具发票出现税务争议时乙方需承担税款、滞纳金、罚款等赔偿责任以及其他相关责任。乙方迟延开具发票、无法开具发票或开具的发票金额低于约定金额的，甲方有权相应地迟延付款、暂不付款或按低于约定金额的发票金额来付款，并对此不承担任何责任。

5．其他

1）为期一年的售后服务工作中，服务方将向医院提供包括应急响应及应急处理服务、配合检查服务、电话支持服务、安全咨询服务等服务在内的安全维保服务。具体服务内容如下：

1.应急响应及应急处理服务

针对本次项目，服务方提供7×24的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

2. 配合检查服务

服务方根据院方需要，无条件协助医院响应配合公安部、网信办等信息安全监管部门的安全检查工作，按照安全检查的各项要求，并配合开展安全自查。

3.电话支持服务

服务方提供每周 7 天/每天 24 小时不间断的电话支持服务，解答医院在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过 10 分钟，到达现场时间不超过 2 小时，解决问题不超过 24 小时。

4.安全咨询服务

服务方为医院无条件提供一年技术咨询服务，提供每周 7 天*24 小时不间断的电话支持服务，解答客户遇到的网络安全问题，及时提出解决问题的建议和操作方法，帮助客户解决信息安全相关技术问题。

5. 安全巡检服务

服务方为医院无条件提供一年安全巡检服务，并每季度提供巡检报告，摸清被测系统基础网络环境，从网络安全结构、网络访问控制、网络安全设计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备保护等方面进行开展自查，并开展工具测试包括漏洞扫描，分析存在的网络安全风险，提出风险防范对策。

6. 安全培训服务

为建立人才培养机制，通过网络安全教育，提升全员网络安全防范意识和法律意识，提升技术支撑服务队伍和网络安全员网络安全处置能力，提高应对突发网络与信息安全事件的综合能力。服务方为医院信息化技术人员提供信息安全相关专业技术知识培训。要求每季度无条件为客户提供一次培训，并提供最新网络风险预警报告。

2）保密声明

双方确定因履行本合同应遵守的保密义务和责任声明如下:

2.1）甲方的义务和责任:

2.1.1）保密内容(包括技术信息和经营信息):乙方的工作方式、原理，以及竞争性技术、工作成果。

2.1.2）涉密人员范围:甲方的所有项目人员

2.1.3）保密期限:不论本合同是否变更、解除、终止，长期有效。

2.1.4)泄密责任:赔偿乙方因泄密造成的经济损失,直至追究法律责任。

2.2）乙方的保密义务和责任:

2.2.1)保密内容(包括技术信息和经济信息):甲方网络设备、信息系统、信息数据等相关信息、本合同服务范围内的工作成果。

2.2.2）涉密人员范围:乙方的所有项目人员

2.2.3）保密期限:不论本合同是否变更、解除、终止，长期有效。

2.2.4)泄密责任:赔偿甲方因泄密造成的经济损失,直至追究法律责任。

根据以上声明，乙方的所有涉密人员需与甲方单位签订专门的保密协议。

6．合同生效

本合同一式肆份，甲方执叁份、乙方执壹份，自甲乙双方签字、盖章之日起生效，各份合同均具有同等法律效力。

7.违约责任

1）服务缺陷的补救措施和索赔

(1)如果乙方提供的服务不符合本合同约定以及磋商文件、响应文件关于服务的要求和承诺，乙方应按照甲方同意的下列一种或几种方式结合起来解决索赔事宜：

①乙方同意将服务款项退还给甲方，由此发生的一切费用和损失由乙方承担。如甲方以适当的条件和方法购买与未履约标的相类似的服务，乙方应负担新购买类似服务所超出的费用。

②根据服务的质量状况以及甲方所遭受的损失，经过甲乙双方商定降低服务的价格。

(2)如果在甲方发出索赔通知后10日内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后10日内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付服务款中扣除索赔金额或者没收履约保证金，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

2）未履行合同义务的违约责任

(1)守约方有权终止全部或部分合同。

(3)由违约一方支付合同总金额5%的违约金

(3)违约金不足以弥补守约方实际损失、可预见或者应当预见的损失，由违约方全额予以赔偿。

（4）依据《中华人民共和国民法典》、《中华人民共和国政府采购法》的相关条款和本合同约定，乙方未全面履行合同义务或者发生违约，甲方会同采购代理机构有权终止合同，依法向乙方要求经济索赔，并报请政府

采购监督管理机关进行相应的行政处罚。

（5）采购人违约的，应当赔偿给乙方造成的经济损失。

（6）延迟交付:如因乙方自身原因导致未能如期交付工作成果，则每延期 1 日，应向甲方支付应付款项的 0.1%作为违约金，最高不超过合同总额的 5%。

泄密:乙方或其员工违反本合同的保密义务，给甲方造成损失，乙方应赔偿甲方遭受的实际直接损失。

8.争议处理

本合同在履行过程中发生的任何争议，应由甲、乙双方友好协商解决，协商不成的，甲乙双方任意一方有权向甲方所在地人民法院提起诉讼。因违约方违反约定事宜产生纠纷，守约方由此产生的费用（包括但不限于诉讼费、律师费、保全费、保全保险费)均由违约方承担。

9、甲乙双方的权利义务

（1）甲方的权利义务：1）甲方有权对合同约定范围内乙方的服务行为进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员数量。对甲方认为不合理的部分有权下达整改通知书，并要求乙方限期整改。2)负责检查监督乙方管理工作的实施及制度的执行情况。3)根据本合同约定，按时向乙方支付应付服务费用。4)国家法律、法规所规定由甲方承担的其它责任。

（2）乙方的权利和义务：1）按本合同约定的服务内容向甲方提供全面服务，并对甲方提出的合理要求进行响应。2）根据本合同的约定向甲方收取相关服务费用，并有权在本项目管理范围内管理及合理使用。3）及时向

甲方通告本项目服务范围内有关服务的重大事项，及时配合处理投诉。4)接受项目行业管理部门及政府有关部门的指导，接受甲方的监督。5)国家法律、法规所规定由乙方承担的其它责任。

（3）甲方责任：

3.1 按合同规定提供予以项目便利的配合，包括及时提供准确完整的相关资料、办公环境和网络环境。

3.2 负责协调乙方工作过程中与本项目有关科室的配合问题。

（4）乙方责任：

4.1 乙方应根据合同的规定，在双方约定的时间内完成服务项目内容。

4.2 乙方应根据工作需要，派出相关专业的工作人员进行项目配合及监督执行。

4.3乙方应按国家规定和本合同及采购文件约定的服务规范和要求进行服务，并对服务质量负责。

10.不可抗力

1）、如果合同双方因不可抗力而导致合同实施延误或合同无法实施，不应该承担误期赔偿或不能履行合同义务的责任。

2）、本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的客观情况，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

3）、在不可抗力事件发生后，当事方应及时将不可抗力情况通知合同对方，在不可抗力事件结束后 3 日内以书面形式将不可抗力的情况和原因通知合同对方，并提供相应的证明文件。合同各方应尽可能继续履行合同

义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行的协议。

11、履约说明

乙方在合同服务期内，须完全履行磋商文件、响应文件及合同中的服务要求、承诺内容和售后服务，未完全履行的，则视为虚假应答，将乙方纳入失信名单。

12.其他约定

本协议中未涉及的事项，双方本着公平公正原则,友好协商解决，补充协议与本协议具有同等法律效力。如双方当事人协商不成，任一方可向甲方住所地人民法院起诉。因违约方违反约定事宜产生纠纷，守约方由此产生的费用（包括但不限于诉讼费、律师费、保全费、保全保险费)均由违约方承担。

第五章　响应文件组成

说明：

1、响应文件统一采用A4格式，**建议双面打印**。其中资格、证明、授权（如有）、图纸等资料为A4幅面纸张，图纸不受纸张幅面大小限制但必须折叠成A4幅面。资格、证明、授权、图纸等资料不受双面打印或复印要求，可以采用插页，可以不编写页码。

2、响应文件须编制目录和从数字“1”开始的连续页码。

3、响应文件请参考以下条目与格式制作，具体响应文件内容以磋商文件要求为准。

4、纸质响应文件装订要求：纸质响应文件统一采用A4格式打印，建议采用纸质封面（不建议使用硬壳封面、亮片、精装、封面压膜、塑料胶面）。由于装订原因造成响应文件的散落、丢失等责任自负。

5、响应文件建议在书脊标明项目编号、项目名称、供应商名称（机打或手写均可）。

6、响应文件的签署或盖章要求：按照磋商文件格式中要求进行签字和（或）盖章。除供应商对错误处须修改外，全套响应文件应无涂改或行间插字和增删。如有修改，修改处由供应商加盖供应商公章并由磋商授权代表签字或盖章。

7、响应文件密封要求：每个封包的封口处用封条妥善密封，密封须完整。

8、商务部分和技术部分可装订成一本也可分开装订。

第一部分　商务部分

一、磋商响应声明

附件 1—1　法定代表人身份证明复印件

二、报价一览表、分项价格表

附件 2—1　报价一览表

附件 2—2　分项价格表

三、商务部分偏离表(格式附后)

四、供应商的资格证明材料

五、提供符合政府采购政策的证明材料

附件 5—1　中小企业声明函(格式附后)

附件 5—2　残疾人福利性单位声明函（格式附后）

附件 5—3　投标担保函

六、其他资料

第二部分　技术部分

一、服务响应偏离表

二、服务方案

三、履约能力

四、服务保证及建议

五、供应商认为需要提供的其他资料

政府采购响应文件

（商务部分）

项目名称：_____

项目编号：_____

供应商名称：_____（公司全称）_____

_____年____月____日

第一部分　商务部分

一、磋商响应声明

我单位收到_____（项目编号）磋商文件，经详细研究，决定参加本次磋商活动。为此，我方郑重承诺以下诸点，并保证诚实守信。

1.愿意按照磋商文件中的全部要求，提供合格的产品及服务，全面履行合同规定的责任和义务。

2.我方提交的磋商响应文件包括正本_____份、副本_____份、U盘(内含磋商响应文件正本的Word版本及PDF版本)壹份。

3.我方已详细阅读和核实全部磋商文件内容，完全理解并同意放弃提出含糊不清和误解问题的权力。

4.我方在磋商后到承诺的磋商有效期内撤回磋商响应文件，我方的磋商保证金将被没收。

5.本磋商响应文件的有效期为磋商之日起90天，如成交，有效期将延长至合同终止日为止。

6.我方承诺，按照本项目招标文件规定的收费标准支付代理服务费。如因代理服务费发生争议，任何一方可以向招标代理机构住所地人民法院提起诉讼。

7.我方与采购人和招标代理机构无任何的隶属关系或者其他利害关系。

8.保证我方所提供的磋商响应文件、证明资料等真实、可信，否则自愿承担一切后果。

9.所有关于本项目的函电，请按下列地址联系：

地　　址：_____

电　　话：_____

传　　真：_____

邮　　编：_____

供应商全称（公章）：_____

法定代表人或被授权人（签字或盖章）：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

附件 1—1　法定代表人身份证明复印件

法定代表人身份证明复印件 （正反面复印/完整复印）

二、报价一览表及分项价格表

附件 2—1

报价一览表

序号	项目名称	
	项目编号	
1	磋商总报价	大写：人民币_____ 小写：￥_____元

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

附件 2—2

分项价格表

项目名称：_____

项目编号：_____

货币：人民币　　单位：元

序号	服务内容	报价	备注 (收费依据、收费标准等)
1			
2			
3			
…			
N			
总计		大写：人民币_____元 小写：¥_____	

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力

三、商务部分偏离表

实质性商务部分偏离表

项目名称：　　项目编号：

序号	磋商文件的 商务部分	响应文件的 商务部分	偏离	说明
1				
2				
3				
…				
N				

说明：

1、填写磋商文件须知前附表中标注★号的内容。

2、在偏离项，必须注明“正偏离”、“负偏离”或“完全响应”，并予以说明。

3、响应文件实际存在偏离，但供应商未在偏离表中注明的，视为负偏离，应当按照磋商文件的规定执行。成交供应商在签订合同时，不得以任何理由进行抗辩。

4、未按★号的内容填写，视为“完全响应”。

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

四、供应商的资格证明材料

各供应商对照“磋商须知前附表”第4条“供应商资格条件”要求的内容进行响应

陕西省政府采购供应商信用承诺书

供应商主体名称：

证件类型：统一社会信用代码

证件号码：

登记机关：

承诺内容：

为维护公开、公平、公正的政府采购市场秩序，树立诚实守信的政府采购供应商形象，本单位自愿做出以下承诺：

一、承诺本单位严格遵守国家法律、法规和规章，全面履行应尽的责任和义务，全面做到履约守信，具备《政府采购法》第二十二条规定的条件；

二、承诺本单位提供给注册登记部门、行业管理部门、司法部门、行业组织以及在政府采购活动中提交的所有资料均合法、真实、有效，无任何伪造、修改、虚假成份，并对所提供资料的真实性负责；

三、承诺本单位严格依法开展生产经营活动，主动接受行业监管，自愿接受依法开展的日常检查；违法失信经营后将自愿接受约束和惩戒，并依法承担相应责任；

四、承诺本单位自觉接受行政管理部门、行业组织、社会公众、新闻舆论的监督；

五、承诺本单位将按照《陕西省社会信用条例》要求，向社会公示信用信息；

六、承诺本单位自我约束、自我管理，重合同、守信用，不制假售假、商标侵权、虚假宣传、违约毁约、恶意逃债、偷税漏税、价格欺诈、垄断和不正当竞争，维护经营者、消费者的合法权益；

七、承诺本单位在信用中国、中国政府采购网等网站中无违法违规、较重或严重失信记录；

八、承诺本单位提出政府采购质疑和投诉坚持依法依规、诚实信用原则，在全国范围 12 个月内没有三次以上查无实据的政府采购投诉；

九、根据政府采购相关法律法规的规定需要作出的其他承诺：_____。

十、承诺本单位若违背承诺约定，经查实，愿意接受行业主管部门和信用管理部门相应的规定处罚，承担违约责任，并依法承担相应的法律责任。自愿按照《陕西省社会信用条例》规定，违背承诺约定行为作为失信信息，记录到省社会信用信息服务平台，并予公开；

十一、承诺本单位同意将以上承诺事项上网公示。

承诺单位（盖章）：

法定代表人（负责人）：

承诺日期：

注：法定代表人或负责人、主体名称发生变更的应当重新做出承诺。

具有履行本合同所必需的设备和专业技术能力的声明

(示例略)

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

参加本次政府采购活动前三年内，在经营活动中

没有重大违法记录声明函

本单位郑重声明：

我单位在参加采购活动前三年内在经营活动中没有《政府采购法》第二十二条第一款第(五)项所称重大违法记录，包括：

我单位未因经营活动中的违法行为受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

1、我方_____（填“未被列入”或“被列入”）失信被执行人名单。

2、我方_____（填“未被列入”或“被列入”）重大税收违法案件当事人名单。

3、我方_____（填“未被列入”或“被列入”）政府采购严重违法失信行为记录名单。

我单位已就上述不良信用行为按照磋商文件中供应商须知前附表规定进行了查询。我单位承诺：合同签订前，若我单位具有不良信用记录情形，贵方可取消我单位成交资格或者不授予合同，所有责任由我单位自行承担。同时，我单位愿意无条件接受监管部门的调查处理。

特此声明！

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

备注：

1、供应商在参加政府采购活动前3年内因违法经营被禁止在一定期限内参加政府采购活动，期限届满的，可以参加政府采购活动，但应提供期限届满的证明材料。

2、《中华人民共和国政府采购法实施条例》第十九条 重大违法记录，是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

3、财库[2022]3号文件，《中华人民共和国政府采购法实施条例》第十九条第一款规定的“较大数额罚款”认定为200万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于200万元的，从其规定。

法定代表人授权委托书(授权代表参加磋商)

致：_____(采购代理机构)

_____(供应商名称)的法定代表人(姓名、职务)授权_____(磋商代表姓名)为本项目的磋商代表，就_____(项目名称)磋商及相关事务代表本公司处理与之有关的一切事务。代理人无转委托权。

本授权书自响应文件递交截止时间起有效期90天。

特此声明。

法定代表人身份证明复印件 （正反面复印/完整复印）

授权代表身份证明复印件 （正反面复印/完整复印）

供应商名称(公章)：_____

法定代表人(签字或盖章)：_____手机号码:_____

身份证号码：_____

授权代表(签字或盖章)：_____手机号码:_____

身份证号码：_____

_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

授权委托书(格式二)(适用于自然人磋商)

致：_____(采购代理机构)

我_____(姓名)系自然人，现授权委托_____(姓名)以本人名义参加_____(项目名称)的磋商活动，并代表本人全权办理针对上述项目的磋商、签约等具体事务和签署相关文件。

本人对被授权人的签字事项负全部责任，代理人无转委托权。

授权委托代理期限:本授权书自响应文件递交截止时间起有效期90天。

特此委托。

我已在下面签字，以资证明。

自然人签字并在签名处加盖食指指印：

年　　月　　日

直接控股和管理关系清单

我方与以下单位存在直接控股、管理关系：

存在直接控股、管理关系的相关单位			
序号	直接控股股东名称及出资比例	直接管理关系单位名称	备注
1			
2			
3			
...			

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

备注：1.直接控股股东：是指其出资额占有限责任公司资本总额百分之五十以上或者其持有的股份占股份有限公司股份总额百分之五十以上的股东；出资额或者持有股份的比例虽然不足百分之五，但依其出资额或者持有的股份所享有的表决权已足以对股东会、股东大会的决议产生重大影响的股东。

2.直接管理关系：是指不具有出资持股关系的其他单位之间存在的管

理与被管理关系，如一些上下级关系的事业单位和团体组织。

3.本表所指的控股、管理关系仅限于直接控股、直接管理关系，不包括间接的控股或管理关系。公司实际控制人与公司之间的关系不属于本表所指的直接控股关系。

4.投标人如不存在直接控股股东的，则在“直接控股股东名称及出资比例”处填写“无”或“/”。投标人不存在直接管理关系的，则在“直接管理关系单位名称”中填“无”或“/”。

本项目不接受联合体投标，不允许分包

本单位郑重声明，参加___项目名称____（项目编号：_____）采购活动，为非联合体投标，本项目实施过程由本单位独立承担。

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。

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

五、提供符合采购政策的证明材料

附件 5—1

中小企业声明函（服务）

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，服务全部由符合政策要求的中小企业承接。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：

（标的名称），属于（采购文件中明确的所属行业）；承建（承接）企业为（企业名称），从业人员_____人，营业收入为____万元，资产总额为_____万元，属于（中型企业、小型企业、微型企业）；

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

备注：1.填写前请认真阅读《工业和信息化部　国家统计局　国家发展和改革委员会　财政部关于印发中小企业划型标准规定的通知》(工信部联企业〔2011〕300 号)和《财政部、工业和信息化部关于印发〈政府采购促进中小企业发展管理办法〉的通知》（财库〔2020〕46 号）相关规定。

2.授权用投标专用章的，与公章具有相同法律效力。

3.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相关数据，参照国务院批准的中小企业划分标准，根据企业自身情况如实判断。

特别提醒：

1、供应商应当对其出具的《中小企业声明函》真实性负责，供应商出具的《中小企业声明函》内容不实的，属于提供虚假材料谋取中标。如供应商对相关制造商信息了解不充分，或者不能确定相关信息真实、准确的，不建议出具《中小企业声明函》。

2、成交供应商享受本项目价格优惠扶持政策的，《中小企业声明函》随成交结果同时公开。

附件 5—2

残疾人福利性单位声明函（若有）

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。

供应商名称(公章)：_____

日期：_____年____月____日

备注：1.填写前请认真阅读《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采的通知》(财库〔2017〕141 号)相关规定。

2.授权用投标专用章的，与公章具有相同法律效力。

附件 5—3：投标担保函（仅供参考）

（适用于磋商保证金保函）

保函编号:

致陕西正信招标有限公司(下称受益人):

鉴于___(下称被保证人)将于__年 月 日参加贵方招标编号为（采购项目编号）的（项目名称）__的投标,我方接受被保证人的委托,在此向受益人提供不可撤销的投标保证:

一、本保证担保的担保金额为人民币(币种)____元(小写)___元整(大写）。

二、本保证担保的保证期间为该项目的投标有效期(或延长的投标有效期)后 30 日(含 30 日),延长投标有效期无须通知我方。

三、在本保证担保的保证期间内,如果被保证人出现下列情形之一,受益人可以向我方提起索赔:

1.被保证人在招标文件规定的投标有效期内撤回其投标;

2.被保证人在投标有效期内收到受益人发出的中标通知书后,不能或拒绝按招标文件的要求签署合同;

3.被保证人在投标有效期内收到受益人发出的中标通知书后,不能或拒绝按招标文件的规定提交履约担保;

4.被保证人中标后未按照招标文件规定交纳代理服务费。

四、在本保证担保的保证期间内,我方收到受益人经法定代表人或其授权委托代理人签字并加盖公章的书面索赔通知后,将不争辩、不挑剔、不可撤销地立即向受益人支付本保证担保的担保金额。

五、受益人的索赔通知应当说明索赔理由,并必须在本保证担保的保证期间内送达我方。

六、本保证担保项下的权利不得转让。

七、本保证担保的保证期间届满,或我方已向受益人支付本保证担保的担保金额,我方的保证责任免除。

八、本保证担保适用中华人民共和国法律。

九、本保证担保以中文文本为准,涂改无效。

保证人(盖章):_____

法定代表人或其授权委托代理人(签字）：_____

单位地址:_____

电话:_____

日期:___年___月___日

六、其他资料

陕西省政府采购供应商拒绝政府采购领域商业贿赂承诺书

为响应党中央、国务院关于治理政府采购领域商业贿赂行为的号召，我公司在此庄严承诺：

1、自觉遵守各项法律、法规、规章、制度以及社会公德，诚信经营，维护廉洁环境，与同场竞争的供应商平等参加政府采购活动。

2、不向政府采购人、采购代理机构和政府采购评审专家进行任何形式的商业贿赂以谋取交易机会。

3、不向政府采购代理机构和采购人提供虚假资质文件或采用虚假应标方式参与政府采购市场竞争并谋取成交。

4、不采取“围标、陪标”等商业欺诈手段获得政府采购订单。

5、不采取不正当手段诋毁、排挤其他供应商。

6、不在提供商品和服务时“偷梁换柱、以次充好”损害采购人的合法权益。

7、不与采购人、采购代理机构、评审专家或其它供应商恶意串通，进行质疑和投诉，维护政府采购市场秩序。

8、尊重和接受政府采购监督管理部门的监督和政府采购代理机构招标采购要求，承担因违约行为给采购人造成的损失。

9、不发生其他有悖于政府采购公开、公平、公正和诚信原则的行为。

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

政府采购响应文件

（技术部分）

项目名称：_____

项目编号：_____

供应商名称：_____（公司全称）_____

___年____月____日

第二部分　技术部分

一、服务响应偏离表

服务响应偏离表

项目名称：　　项目编号：

序号	磋商要求	响应情况	偏离情况	说明
1				
2				
3				
4				
…				
N				

1、“磋商要求”一栏应**填写磋商文件第六章**“项目采购需求”的内容；

2、“响应情况”一栏必须详细填写服务内容，并应对照磋商文件技术要求一一对应响应；

3、“偏离情况”一栏应如实填写“正偏离”、“负偏离”或“无偏离”；

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

二、服务方案

三、履约能力（示例略）

四、服务保证及建议(示例略)

供应商名称(公章)：_____

日期：_____年____月____日

说明：授权用投标专用章的，与公章具有相同法律效力。

五、供应商认为需要提供的其他资料

（示例略）

公章授权书(如有)

公章授权书

_____(供应商名称)_____，中华人民共和国合法企业，法定地址：_____。在参与_____(项目名称)(项目编号)__竞争性磋商活动中，我公司授权投标专用章/业务专用章在此次活动中代为公章使用。

投标专用章/业务专用章所签署的磋商文件、澄清等，我公司承认并同意具备与我公司公章签署等同的法律的效力。

投标专用章/业务专用章签署的所有文件、协议不因授权的撤销而失效。

投标专用章/业务专用章：_____(盖章)

供应商公章：_____(盖章)

供应商法定代表人：_____(签字或盖章)

日期：　　年　　月　　日

第二部分　技术部分

第六章　项目采购需求

一、服务项目（项目属性为服务的填写）

1、服务范围

本项目负责完成陕西省康复医院2025年度网络安全等级保护测评服务和其它网络安全保障服务，等级保护测评服务包括定级、备案和测评等服务，从“安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理”等方面开展等级保护测评工作，测评对象为7个三级信息系统“医院综合信息系统、电子病历系统、医学影像信息系统(PACS)、陕西省康复医院患者服务平台、心电网络系统、DRG管理及医保智能审核系统、传染病智能监测预警前置软件”，1个二级信息系统“OA办公系统”；其它网络安全保障服务包括：应急响应及应急处理服务、重要时期保障服务、安全巡检服务、安全培训服务。

2、服务要求

（1）服务内容：

①网络安全等级保护测评服务

依据《基本要求》（GB/T 22239-2019）、测评要求》（GB/T 28448-2019）和《测评过程指南》（GB/T 28449-2018）等国家关于网络安全等级保护2.0的相关标准和规范要求，为我院提供以上7个信息系统等级保护测评实施工作，测评工作包括安全物理环境、安全通信网络、安全区域边界、安全

计算环境、安全管理中心测评，以及安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理10个层面测评。在开展网络安全等级保护测评工作过程中要求严格遵循如下流程：

a、定级备案：按照等级保护相关制度要求，本着自主定级的原则，协助我院完成未备案信息系统的定级报告编制、备案表填写，组织相关专家对定级结果进行评审，完善相关资料，递交至公安部门完成定级备案工作。

b、系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状，出具《资产调查表》。

c、现场测评：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果，出具《现场检查表单》。

d、分析整改：分析信息系统安全情况与等级保护基本要求的差距,提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合我院安全整改工作，出具《整改建议书》。

e、等级测评：根据差异化测评以及国家等级测评相关标准及编制的相关等级保护测评指导书进行符合性测评，并进行记录。

f、结论报告（报告编制）：分析当前信息系统安全保护能力是否符合二级的安全要求，针对整改项进行再次测评，提供安全等级符合性测评服务，出具相关信息系统测评报告。

g、配合验收：整理项目过程中所有相关的过程文档，提交我院。按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

② 重大事件应急响应及应急处理服务

在项目服务期内，提供7×24小时的信息安全应急处理保障服务。一旦信息系统出现紧急重大安全事件，收到陕西省康复医院的服务请求，测评单位自接到通知10分钟内响应，在2小时内到达现场，成立应急小组对信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。完成技术服务后需提供相应的《应急响应及应急处理报告》。

③重要时期保障服务

在项目服务期内，根据我院实际需要，为我院提供在国家重大政治活动和节假日期间的技术防护保障服务，针对近期可能发生的网络安全威胁，提供技术防护服务，确保活动期间的网络安全可靠运行。

④安全巡检服务

在项目服务期内，为我院提供至少每季度1次的安全巡检服务，对所有软硬件设备、信息系统进行深度安全巡检，包括但不限于对信息系统中指定的服务器、网络设备、安全设备及安全日志等的安全状态核查。摸清被测系统基础网络环境，从网络安全结构、网络访问控制、网络安全设计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备保护等方面进行安全检查，并开展工具测试包括漏洞扫描，分析存在的网络安全风险，提出风险防范对策并协助我院进行风险问题整改。

⑤安全培训服务

在项目服务期内，为我院提供每半年1次的信息安全相关专业知识培训服务，包含网络安全意识培训及网络安全技术培训，网络安全意识培训

内容主要包括：网络安全法知识普及、典型信息安全事件知识案例讲解、安全保密意识建立以及前沿信息安全技术知识培训。安全技术能力培训针对主机安全、应用安全、网络安全、数据库安全相关的检查方法进行培训。

⑥制度体系建设服务

在项目服务期内，协助我院建立网络安全管理制度，完善网络安全管理机构部门岗位职能，落实安全责任；协助解决信息系统安全方面存在的技术问题，提高信息系统安全保障水平，保证信息系统安全稳定运行；构建基础的网络安全管理体系，并分类整理相关制度资料、形成胶装文件、电子档案以及管理制度展板制作。

（2）服务标准：

对应《信息安全技术网络安全等级保护基本要求》各安全要求项的测评称为单项测评。整体测评是在单项测评的基础上，通过进一步分析定级对象安全保护功能的整体相关性，对定级对象实施的综合安全测评。具体测评项如下表：

三级系统测评指标

安全层面	安全子类	测评指标描述
安全物理环境	物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；
		b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；
		b）应将通信线缆铺设在隐蔽安全处；
		c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
	防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地；
		b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
	防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，

安全层面	安全子类	测评指标描述
		并自动灭火；
		b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
		c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
	防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
		c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
	防静电	a）应采用防静电地板或地面并采用必要的接地防静电措施；
		b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；
		b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
		c）应设置冗余或并行的电力电缆线路为计算机系统供电。
	电磁防护	a）电源线和通信线缆应隔离铺设，避免互相干扰；
		b）应对关键设备实施电磁屏蔽。
安全通信网络	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；
		b）应保证网络各个部分的带宽满足业务高峰期需要；
		c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
		d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
		e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
	通信传输	a）应采用校验技术或经国家密码局认证核准的密码技术保证通信过程中数据的完整性；
		b）应采用国家密码局认证核准的密码技术保证通信过程中数据的保密性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；

安全层面	安全子类	测评指标描述
		b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；
		c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；
		d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
	访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
		b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
		c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
		d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
		e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
	入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
		b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
		c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
		d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
	恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
		b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
	安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节

安全层面	安全子类	测评指标描述
		进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，具体要求包括： 1)系统应为不同用户提供不同的用户身份标识； 2)系统的用户名和口令不得相同，用户口令应为数字、字母、特殊字符混合组合； 3)用户口令长度应不低于 8 位； 4)系统应具有用户口令定期更新提示和更新确认； 5)禁止明文存储口令。
		b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施，具体要求包括： 1)宜限制操作系统同一用户连续登录失败次数为 6-10 次，具体次数应在相关安全策略中明确； 2)登录失败超过规定次数，用户账户应被锁定 10 分钟，或申请由系统管理员进行密码重置。
		c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，具体要求包括： 应采用 SSH、Https、VPN 等安全的远程管理方式。
		d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用国家密码局认证核准的密码技术来实现，具体要求包括： 其中一种鉴别技术宜采用动态口令、数字证书、生物特征或设备指纹。
	访问控制	a) 应对登录的用户分配账户和权限；
		b) 应重命名或删除默认账户，修改默认账户的默认口令，具体要求包括： 操作系统应禁用无法重命名或无法删除的默认账户，或阻止默认账户直接远程登录。
		c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；
		e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
		f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
		g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

安全层面	安全子类	测评指标描述
	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d）应对审计进程进行保护，防止未经授权的中断。
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b）应关闭不需要的系统服务、默认共享和高危端口；
		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
	数据完整性	a）应采用校验技术或经国家密码局认证核准的密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
		b）应采用校验技术或经国家密码局认证核准的密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
	数据保密性	a）应采用国家密码局认证核准的密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
		b）应采用国家密码局认证核准的密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；

安全层面	安全子类	测评指标描述
		b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
		c）应提供重要数据处理系统的热冗余，保证系统的高可用性。
	剩余信息保护	a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
		b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；
		b）应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a）应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
		b）应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
		e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
		f）应能对网络中发生的各类安全事件进行识别、报警和分析。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

安全层面	安全子类	测评指标描述
	管理制度	a）应对安全管理活动中的各类管理内容建立安全管理制度；
		b）应对管理人员或操作人员执行的日常管理操作建立操作规程；
		c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
	制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；
		b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理机构	岗位设置	a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
		b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
		c）应设立系统管理员、安全审计员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	a）应配备一定数量的系统管理员、安全审计员和安全管理员等；
		b）应配备专职安全管理员，不可兼任。
	授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
		c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
	沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
		b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
		c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
		b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
		c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
安全管理人员	人员录用	a）应指定或授权专门的部门或人员负责人员录用；
		b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，

安全层面	安全子类	测评指标描述
		对其所具有的技术技能进行考核；
		c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
	人员离岗	a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
		b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
	安全意识教育和培训	a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
		b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
		c）应定期对不同岗位的人员进行技能考核。
	外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
		b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
		c）外部人员离场后应及时清除其所有的访问权限；
		d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
安全建设管理	定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
		b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
		c）应保证定级结果经过相关部门的批准；
		d）应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
		b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含国家密码局认证核准的密码技术的相关内容，并形成配套文件；
		c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定，具体要求包括： 应根据党政机关电子公文系统安全可靠应用推进工作领导小组办公室发布的安全可靠应用相关产品目录采购产品。
		b）应确保密码产品与服务的采购和使用符合国家密码管理局的要

安全层面	安全子类	测评指标描述
		求；
		c）应预先对产品进行选型测试，确定产品的候选范围，并及时审定和更新候选产品名单，具体要求包括： 应按照党政机关电子公文系统安全可靠应用推进工作领导小组办公室相关工作要求进行产品选型测试。
		d）应通过专有的应用供应渠道下载软件。
	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
		b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
		c）应制定代码编写安全规范，要求开发人员参照规范编写代码；
		d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制；
		e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
		f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
		g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
		b）应保证开发单位提供软件设计文档和使用指南；
		c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；
		b）应制定安全工程实施方案控制工程实施过程；
		c）应通过第三方工程监理控制项目的实施过程。
	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
		b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
	系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
		b）应对负责运行维护的技术人员进行相应的技能培训；
		c）应提供建设过程文档和运行维护文档。
	等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
		b）应在发生重大变更或级别发生变化时进行等级测评；

安全层面	安全子类	测评指标描述
		c）应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；具体包括： 应按照党政机关电子公文应用推进工作领导小组办公室的要求和服务商推荐名录选择服务供应商，如集成服务、软件开发等单位；
		b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
		c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
安全运维管理	环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
		b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；
		c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
		b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
		c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
	介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
		b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
		b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
		c）信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；
		d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
	漏洞和风险管理	a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
		b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的

安全层面	安全子类	测评指标描述
		安全问题。
	网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
		c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
		e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
		f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
		g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
		h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
		i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
		j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
	恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
		b）应定期验证防范恶意代码攻击的技术措施的有效性。
	配置管理	a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
		b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
	密码管理	a）应遵循密码相关国家标准和行业标准；
		b）应使用国家密码管理主管部门认证核准的密码技术和产品。
	变更管理	a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案

安全层面	安全子类	测评指标描述
		经过评审、审批后方可实施；
		b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
		c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
	备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；
		b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；
		c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
	安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；
		b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
		c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
		d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
	应急预案管理	a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
		b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
		c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
		d）应定期对原有的应急预案重新评估，修订完善。
	外包运维管理	a）应确保外包运维服务商的选择符合国家的有关规定；
		b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
		c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
		d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

（3）服务人员数量及组成：

1. 测评人员要求：本项目的测评人员需具有 1 年以上测评工作经验，项目经理和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方

案，确保人员稳定，如需更换测评人员，须由我院同意。

2.人员配备：供应商参与此项目不少于6人，现场测评人员不得少于4人，其中至少包含1名高级测评师，2名中级测评师。供应商必须为本项目成立本地化等级保护测评小组，由测评小组组长统一负责，测评小组组长具有一定的技术及管理知识和经验，能容易地与客户沟通，能很好的执行与完成测评工作，并根据适当情况增加测评人员。

3.供应商应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

（4）其他要求：

1）为期一年的售后服务工作中，服务方将向医院提供包括应急响应及应急处理服务、配合检查服务、电话支持服务、安全咨询服务等服务在内的安全维保服务。具体服务内容如下：

1.应急响应及应急处理服务

针对本次项目，服务方提供7×24的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

2. 配合检查服务

服务方根据院方需要，无条件协助医院响应配合公安部、网信办等信息安全监管部门的安全检查工作，按照安全检查的各项要求，并配合开展安全自查。

3.电话支持服务

服务方提供每周7天/每天24小时不间断的电话支持服务，解答医院在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过10分钟，到达现场时间不超过2小时，解决问题不超过24小时。

4.安全咨询服务

服务方为医院无条件提供一年技术咨询服务，提供每周7天*24小时不间断的电话支持服务，解答客户遇到的网络安全问题，及时提出解决问题的建议和操作方法，帮助客户解决信息安全相关技术问题。

7. 安全巡检服务

服务方为医院无条件提供一年安全巡检服务，并每季度提供巡检报告，摸清被测系

统基础网络环境，从网络安全结构、网络访问控制、网络安全设计、边界完整性检查、网络入侵防范、恶意代码防范、网络设备保护等方面进行开展自查，并开展工具测试包括漏洞扫描，分析存在的网络安全风险，提出风险防范对策。

8. 安全培训服务

为建立人才培养机制，通过网络安全教育，提升全员网络安全防范意识和法律意识，提升技术支撑服务队伍和网络安全员网络安全处置能力，提高应对突发网络与信息安全事件的综合能力。服务方为医院信息化技术人员提供信息安全相关专业技术知识培训。要求每季度无条件为客户提供一次培训，并提供最新网络风险预警报告。

2）保密声明

双方确定因履行本合同应遵守的保密义务和责任声明如下:

2.1）甲方的义务和责任:

2.1.1）保密内容(包括技术信息和经营信息):乙方的工作方式、原理，以及竞争性技术、工作成果。

2.1.2）涉密人员范围:甲方的所有项目人员

2.1.3）保密期限:不论本合同是否变更、解除、终止，长期有效。

2.1.4）泄密责任:赔偿乙方因泄密造成的经济损失，直至追究法律责任。

2.2）乙方的保密义务和责任:

2.2.1）保密内容(包括技术信息和经济信息):甲方网络设备、信息系统、信息数据等相关信息、本合同服务范围内的工作成果。

2.2.2）涉密人员范围:乙方的所有项目人员

2.2.3）保密期限:不论本合同是否变更、解除、终止，长期有效。

2.2.4）泄密责任:赔偿甲方因泄密造成的经济损失，直至追究法律责任。

根据以上声明，乙方的所有涉密人员需与甲方单位签订专门的保密协议。

3、服务事项的验收（考核）标准（如内容较多，可单独作为附件）

项目交付物：（1）《信息系统安全等级保护测评方案》；（2）《信息系统安全等级测评报告》；（3）《信息系统整改建议书》；（4）《信息系统渗透测试报告》；（5）《信息系统安全等级保护定级备案证明》

验收方式：甲方以会议形式，根据合同、招标文件、验收资料等文件，组织项目验收。

陕西正信招标有限公司

地　　址：西安市莲湖区环城西路南段元晟合中心6层

电　　话：029-88110800

邮　　编：710082