

# 竞争性磋商文件

(服务类)

采购项目名称：信息系统等保测评服务

采购项目编号：DLZB-2026-0410

西北妇女儿童医院

典亮工程项目管理有限公司共同编制

2026年5月12日

## 目 录

第一章 竞争性磋商邀请 .....	1
第二章 供应商须知 .....	4
第三章 采购项目技术、服务、商务及其他要求 .....	15
第四章 资格审查 .....	31
第五章 磋商过程中可实质性变动的内容 .....	32
第六章 磋商办法 .....	33
第七章 响应文件格式 .....	41
第八章 拟签订合同文本 .....	61

# 第一章 竞争性磋商邀请

## 项目概况

信息系统等保测评服务的潜在供应商应在西安市莲湖区南二环西段9号泊达国际酒店27楼东户招标部，带授权委托书、身份证复印件加盖公章获取竞争性磋商文件，并于2026年5月27日14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：DLZB-2026-0410

项目名称：信息系统等保测评服务

采购方式：竞争性磋商

预算金额：450000.00元

采购需求：

合同包1(信息系统等保测评服务)：

合同包预算金额：450000.00元

合同包最高限价：450000.00元

品目号	品目名称	采购标的	数量(单位)	采购需求	品目预算(元)
1-1	安全运维服务	信息系统等保测评服务	1(项)	详见采购文件	450000.00

本合同包不接受联合体投标

合同履行期限：详见采购文件

## 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(信息系统等保测评服务)落实政府采购政策需满足的资格要求如下：

本项目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(信息系统等保测评服务)特定资格要求如下：

1) 供应商为具有独立承担民事责任能力的法人、其他组织或自然人。企业法人应提供合法有效的标识有统一社会信用代码的营业执照；事业法人应提供事业单位法人证书；其他组织应提供合法登记证明文件；自然人应提供身份证；

2) 财务状况：提供注册会计师行业统一监管平台(网址<http://acc.mof.gov.cn>)赋码可查询的2024年度或2025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); 或开标前 12 个月内其开户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) 具有依法缴纳税收的良好记录: 提供缴费所属日期为投标截止时间前 12 个月内任一月份(投标截止时间当月不计入)的增值税(或所得税)缴费凭据或税务机关出具的完税证明/在法规范围内不需提供的应出具书面说明和证明文件; 或具有依法缴纳税收的诚信声明; 以上两种形式的资料提供任何一种即可;

4) 具有依法缴纳社会保障资金的良好记录: 提供缴费所属日期为投标截止时间前 12 个月内任一月份(投标截止时间当月不计入)的缴费凭据或社保机关出具的缴费证明/在法规范围内不需提供的应出具书面说明和证明文件; 或具有依法缴纳社会保障资金的缴纳记录的诚信声明; 以上两种形式的资料提供任何一种即可;

5) 授权委托书: 法定代表人参加投标须提供《法定代表人身份证明》及身份证复印件; 法定代表人授权他人参加投标, 须提供《法定代表人授权委托书》及委托代理人身份证复印件;

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

7) 具有履行合同所必需的设备和专业技术能力: 具有履行合同所必需的设备和专业技术能力, 提供声明文件;

8) 供应商须提供公安部第三研究所颁发的《网络安全服务认证证书(等级保护测评服务认证)》;

9) 本项目不接受联合体投标。

### 三、获取采购文件

时间: 2026 年 5 月 12 日至 2026 年 5 月 19 日, 每天上午 09:00:00 至 12:00:00, 下午 14:00:00 至 18:00:00 (北京时间, 法定节假日除外)

途径: 西安市莲湖区南二环西段 9 号泊达国际酒店 27 楼东户招标部, 带授权委托书、身份证复印件加盖公章

方式: 现场获取

售价: 0 元

### 四、响应文件提交

截止时间: 2026 年 5 月 27 日 14 时 30 分(北京时间)

地点: 西安市莲湖区南二环西段 9 号泊达国际酒店 27 楼东户会议室

### 五、开启

截止时间: 2026 年 5 月 27 日 14 时 30 分(北京时间)

地点: 西安市莲湖区南二环西段 9 号泊达国际酒店 27 楼东户会议室

## 六、公告期限

自本公告发布之日起5个工作日。

## 七、其他补充事宜

1. 供应商信用融资：根据《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）和《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）文件要求，为助力解决政府采购成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录陕西省政府采购网—陕西省政府采购金融服务平台

（<http://www.ccgp-shaanxi.gov.cn/zcdservice/zcd/shanxi/>），选择符合自身情况的“政采贷”银行及其产品，凭项目中标（成交）结果、中标（成交）通知书等信息在线向银行提出贷款意向申请、查看贷款审批情况等。

2. 请供应商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中的要求，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。

## 八、对本次招标提出询问，请按以下方式联系。

### 1. 采购人信息

名称：西北妇女儿童医院

地址：西安市雁翔路1616号

联系方式：寇老师 029-89550667

### 2. 采购代理机构信息

名称：典亮工程项目管理有限公司

地址：西安市莲湖区南二环西段9号泊达国际酒店27楼东户会议室

联系方式：029-87613089

### 3. 项目联系方式

项目联系人：李博、余翠、王晶、何勇、许彩茹

电话：029-87613089

## 第二章 供应商须知

### 2.1 供应商须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	本项目各包采购预算金额如下： 采购包 1：450000.00 元供应商的采购包响应报价高于采购包采购预算的，其响应文件将按无效处理。
2	最高限价（实质性要求）	招标最高限价：450000.00 元，供应商的采购包响应报价高于最高限价的，其响应文件将按无效处理。
3	评审方法	采购包 1：综合评分法（详见第六章）
4	是否接受联合体	采购包 1：不接受 如以联合体响应的，联合体各方均应当具备本磋商文件要求的资格条件和能力。 （1）联合体各方均应具有承担本磋商项目必备的条件，如相应的人力、物力、资金等。 （2）磋商文件对供应商资格条件有特殊要求的，联合体各个成员都应当具备规定的相应资格条件。 （3）同一专业的单位组成的联合体，应当按照资质等级较低的单位确定联合体的资质等级。如：某联合体由三个单位组成，其中两个单位资质等级为甲级，另一单位资质等级为乙级，则该联合体资质等级为乙级。
5	落实节能、环保产品政策	1. 根据《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）相关要求，政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门确定实施政府优先采购和强制采购的产品类别，以品目清单的形式发布并适时调整。 2. 本项目采购无产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效投标处理。 3. 本项目采购无产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购的___/___产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分/响应报价相同的，按供应商提供的优先采购产品认证证书数量由多到少顺序排列。
6	小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）	（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）第九条和《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）的规定。 关于本项目采购包中执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除情况、具体扣除比例和规则详见第六章。 （其他情形）不适用。
7	不正当竞争预防措施	启动异常低价投标（响应）审查。具体内容详见 2.4.7 响应

	(实质性要求)	报价(实质性要求)
8	答疑	已领取本竞争性磋商文件的供应商若对本竞争性磋商文件有疑问,需要采购人或采购代理机构回复的,应在响应文件递交截止时间 5 天前向采购代理机构指定邮箱提交疑问问题 word 版电子文件以及加盖公章的 PDF 扫描件,如缺少上述要求的书面材料或逾期提交的,采购人或采购代理机构将依法不予进行回复。 指定邮箱为: 1430023389@qq.com
9	磋商保证金	采购包 1 保证金金额: 8000.00 元 缴交渠道: 包括但不限于现金、转账、支票、汇票、保函等形式 开户名称: 典亮工程项目管理有限公司 开户银行: 陕西秦农农村商业银行股份有限公司劳动南路支行 银行账号: 2701050701201000053069
10	标书费信息	免费获取
11	履约保证金(实质性要求)	采购包 1: 不缴纳
12	质量保证金	采购包 1: 不缴纳
13	磋商有效期(实质性要求)	提交响应文件的截止之日起不少于 90 天。
14	磋商程序	本次磋商项目采用二次报价。 (1) 对供应商的响应文件的密封性进行审查; (2) 由工作人员拆封供应商的响应文件; (3) 核验供应商的资格证明材料,资格审查不合格的不进入下一步评审环节; (4) 对供应商的响应文件进行符合性审查,对通过符合性审查的供应商进行下一步评审; (5) 对有效供应商分别进行磋商; (6) 对有效供应商要求提交第二次商务报价,在磋商小组未对竞争性磋商文件进行实质性修改的情况下,第二次报价不得超过一次报价; (7) 磋商小组评审。 注:在本项目磋商过程中,磋商小组可根据本竞争性磋商文件要求和磋商情况实质性变动服务要求中的技术、服务要求以及合同草案条款。根据相关规定,所有报价在公示前均不公开宣布。
15	磋商小组的组建	磋商小组构成: 3 人。 磋商小组确定方式: 评审前 24 小时内政府采购平台的专家库系统中随机抽取技术、经济方面的专家。
16	定标方式	是否授权磋商小组确定成交供应商: <input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否 采购人依据磋商小组推荐的成交候选人确定成交供应商,磋商小组推荐成交候选人的人数: 3 ;
17	招标代理服务费(实质性要求)	本项目收取代理服务费 代理服务费用收取对象: 中标/成交供应商 代理服务费收费标准: 成交供应商在领取成交通知书时,向

		典亮工程项目管理有限公司交纳招标代理服务费。服务费收费标准参照国家计委颁发的《招标代理服务收费管理暂行办法》（计价格〔2002〕1980号）的有关规定按标准计取。 招标代理服务费账户： ①公司名称：典亮工程项目管理有限公司 ②账号：2701050701201000053069 ③开户行：陕西秦农农村商业银行股份有限公司劳动南路支行
18	采购结果公告	采购结果将在陕西省政府采购网予以公告。
19	成交通知书	采购结果公告发布的同时，代理机构向中标供应商发出成交通知书。
20	政府采购合同公告、备案	政府采购合同签订之日起2个工作日内，采购人将政府采购合同在“陕西省政府采购网”予以公告；政府采购合同签订之日起7个工作日内，采购人将本项目采购合同通过政府采购平台进行备案。
21	进口产品	不允许
22	响应文件份数及格式	响应文件的数量及签署规定： 响应文件正本壹份、副本贰份、U盘贰份（单独密封装袋标明公司名称，U盘内应包含：响应文件正本的Word版本及盖章扫描后的PDF版本）（响应文件不退还），每份文件须清楚地标明“正本”或“副本”。若正本和副本不符，以正本为准。
23	装订要求	响应文件牢固装订成册，鼓励双面打印。
24	现场踏勘	是否组织踏勘： <input type="checkbox"/> 组织/ <input checked="" type="checkbox"/> 不组织  各供应商可自行前往项目所在地进行踏勘。过程中所产生的任何费用及安全问题由供应商自行承担。不论供应商是否踏勘，与本项目实施的所有因素、细节由供应商自行考虑并承担相关不利风险，任何因忽视或误解工地情况而导致的索赔或工期延长申请将不获批准。
25	采购标的对应的中小企业划分标准所属行业	所属行业为：软件和信息技术服务业

## 2.2 总则

### 2.2.1 适用范围

一、本竞争性磋商文件仅适用于本次公开招标采购项目。

二、本竞争性磋商文件的最终解释权由西北妇女儿童医院和典亮工程项目管理有限公司享有。对竞争性磋商文件中供应商参加本次政府采购活动应当具备的条件，采购项目技术、服务、商务及其他要求，评标细则及标准由西北妇女儿童医院负责解释。除上述竞争性磋商文件内容，其他内容由典亮工程项目管理有限公司负责解释。

### 2.2.2 有关定义

一、“采购人”是指依法进行政府采购的各级国家机关、事业单位、团体组织。本次招标的采购人是西北妇女儿童医院。

二、“供应商”是指按照采购公告规定获取了竞争性磋商文件，拟参加投标和向采购人提供货物、工程或服务的法人、其他组织或者自然人。

三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是典亮工程项目管理有限公司。

## 2.3 竞争性磋商文件

### 2.3.1 竞争性磋商文件的构成

一、竞争性磋商文件是供应商准备响应文件和参加投标的依据，同时也是资格审查、评标的重要依据。竞争性磋商文件用以阐明采购项目所需的资质、技术、服务及报价等要求、招标投标程序、有关规定和注意事项以及合同主要条款等。本竞争性磋商文件包括以下内容：

- (一) 竞争性磋商邀请；
- (二) 供应商须知；
- (三) 采购项目技术、服务、商务及其他要求；
- (四) 资格审查；
- (五) 磋商过程中可实质性变动的内容；
- (六) 磋商办法；
- (七) 响应文件格式；
- (八) 拟签订合同文本。

二、供应商应认真阅读和充分理解竞争性磋商文件中所有的事项、格式条款和规范要求。供应商没有对竞争性磋商文件全面做出实质性响应所产生的风险由供应商承担。

### 2.3.2 竞争性磋商文件的澄清和修改

一、在响应文件提交截止时间前，采购人或者代理机构可以对已发出的竞争性磋商文件进行必要的澄清或者修改。

二、澄清或者修改的内容为竞争性磋商文件的组成部分，采购人或者代理机构将在陕西省政府采购网发布更正公告，供应商应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响响应文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的竞争性磋商文件，供应商应依据更正后的竞争性磋商文件编制响应文件。若供应商未按前述要求进行投标响应的，自行承担不利后果。

## 2.4 响应文件

### 2.4.1 响应文件的语言

一、供应商提交的响应文件以及供应商与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。响应文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，磋商小组将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对供应商的不利后果，由供应商承担。

### 2.4.2 计量单位

除竞争性磋商文件中另有规定外，本项目均采用国家法定的计量单位。

### 2.4.3 响应货币

本次项目均以人民币报价。

### 2.4.4 知识产权

一、供应商应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

二、供应商将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，供应商需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

三、如采用供应商所不拥有的知识产权，则在响应报价中必须包括合法使用该知识产权的相关费用。

#### 2.4.5 响应文件的组成

供应商应当按照竞争性磋商文件的要求编制响应文件。响应文件应当对竞争性磋商文件提出的要求和条件作出明确响应。

响应文件具体内容详见第六章。

#### 2.4.6 响应文件格式

一、供应商应按照竞争性磋商文件第六章中提供的“响应文件格式”填写相关内容。

二、对于没有格式要求的响应文件由供应商自行编写。

#### 2.4.7 响应报价（实质性要求）

一、供应商的报价是其响应本项目要求的全部工作内容的价格体现，包括税费等供应商完成本项目所需的一切费用。

二、供应商提供的服务内容只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

三、响应文件报价出现前后不一致的，按照磋商文件第六章磋商办法规定予以修正，修正后的报价经供应商签字确认，供应商未在规定时间内确认的，其投标无效。

四、政府采购评审中出现下列情形之一的，磋商小组应当启动异常低价投标（响应）审查程序：

（一）投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值 50% 的，即投标（响应）报价 $<$ 全部通过符合性审查供应商投标（响应）报价平均值 $\times$ 50%；

（二）投标（响应）报价低于通过符合性审查的次低报价供应商投标（响应）报价 50% 的，即投标（响应）报价 $<$ 通过符合性审查的次低报价供应商投标（响应）报价 $\times$ 50%；

（三）投标（响应）报价低于采购项目最高限价 45% 的，即投标（响应）报价 $<$ 采购项目最高限价 $\times$ 45%；

（四）磋商小组基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形。

采购人可以结合具体项目实际情况，提高上述第（一）项至第（三）项中启动异常低价投标（响应）审查的数值标准，但是最高不得超过 65%。

相关法律法规对供应商报价有规定的，从其规定。

#### 五、启动异常低价投标（响应）审查

（一）磋商小组启动异常低价投标（响应）审查后，属于前述第（一）项至第（四）项情形的，应当要求相关供应商在评审现场合理的时间对投标（响应）价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等，给予相关供应商的合理时间一般不少于 30 分钟。其中，属于第（三）项情形，供应商已随投标（响应）文件一并提交相关书面说明及必要的证明材料的，在评审现场可不再重复提交。

（二）磋商小组依据专业经验，参考同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。投标（响应）供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，磋商小组应当将其作为无效投标（响应）处理。

（三）采购人、采购代理机构应当为磋商小组在评审现场及时获取同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业

平均成本等相关信息资料提供便利。磋商小组借助互联网等渠道查询相关信息的，应当严格遵守评审工作纪律，不得实施影响评审公正的行为。

(四) 异常低价投标(响应)审查的启动原因、审查意见和审查结果应当在评审报告中记录，并随供应商提供的相关书面说明及证明材料，以及磋商小组有关互联网浏览、查询历史一并归档。

#### 2.4.8 磋商有效期(实质性要求)

磋商有效期详见第二章“供应商须知前附表”，响应文件未明确磋商有效期或者磋商有效期小于“供应商须知前附表”中磋商有效期要求的，其响应文件按无效处理。

#### 2.4.9 响应文件的制作、签章(实质性要求)

##### 1. 响应文件编制的原则

1.1 供应商应在认真阅读竞争性磋商文件所有内容的基础上，按照竞争性磋商文件的要求编制完整的响应文件。竞争性磋商文件中对响应文件格式有要求的，应按格式逐项填写内容，不准有空项；无相应内容可填的项应填写“无”、“没有相应指标”等明确的回答文字。响应文件中留有空项的，将被视为不完整响应的响应文件，其将有可能被拒绝。

1.2 供应商必须保证响应文件所提供的全部资料真实可靠，并接受对其中任何资料进一步审查的要求。

1.3 响应文件须对竞争性磋商文件中的内容做出实质性和完整的响应，否则其将被拒绝。

##### 2. 投标语言

由供应商编写的响应文件和往来信件应以中文书写。

##### 3. 计量单位

除在竞争性磋商文件的技术规格中另有规定外，计量单位应使用中华人民共和国法定计量单位。

##### 4. 响应文件的组成

4.1 所有服务方案只允许供应商有一个响应方案，不接受任何有选择的方案和报价(包括有条件的折扣)。供应商未按要求，提供了选择方案和报价的，其投标将被拒绝。

4.2 供应商编写的响应文件应包括下列部分：

1) 投标函、响应报价表以及所有附件内容。

2) 按照供应商须知出具的供应商资格证明文件。

3) 按照供应商须知出具的报价符合竞争性磋商文件规定的证明文件及供应商认为需加以说明的其他内容。

4) 竞争性磋商文件要求供应商提供的其他内容。

##### 5. 响应文件格式

供应商应按竞争性磋商文件中提供的响应文件格式填写。

##### 6. 响应报价

6.1 本项目响应报价为供应商响应文件中提供的所有内容金额的总和。

6.2 凡本竞争性磋商文件要求(或允许)及供应商认为需要进行报价的各项费用项目(不论是否要求进入报价)，若报价时未报或未在竞争性磋商文件中予以说明，采购人将认为这些费用供应商已计取，并包含在报价中。

6.3 供应商应按照竞争性磋商文件附件提供的格式填写。如果“响应报价表”中的报价与响应文件中的报价不符，以“响应报价表”中的价格为准。文字大写表示的数据与同一数字表示的有差别，则以文字大写表示的数据为准。如果单价与总价不符，以单价为准；除非磋商小组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。

6.4 供应商所报的响应报价在合同执行过程中是固定不变的，不得以任何理由予以变更。根据供应商须知的规定，以可调整的价格提交的响应文件为非响应性投标而予以拒绝。

##### 7. 响应货币

采购人只接受人民币作为唯一响应货币。

## 8. 证明供应商资格的证明文件

供应商必须按要求提交证明文件，以证明其有资格参加投标和成交后有履行合同的能力，并作为其响应文件的一部分。

### 9. 证明的合格性和符合竞争性磋商文件规定的文件

9.1 供应商应对竞争性磋商文件中的各项条款做出清晰准确的答复。

9.2 证明服务与竞争性磋商文件的要求相一致的文件，它可以是文字资料、图表、数据、证书、业主证明，包括：

1) 提供响应方案。根据竞争性磋商文件提供的需求提供对应的响应方案。响应方案必须满足采购人项目需求，并逐条说明所提供服务的已对采购人的技术要求做出了实质性的响应，或申明与技术要求条文的偏差和例外；

2) 提供项目实施方案，说明供应商将在成交后，如何利用人力及其他资源来承担其合同项下整体的管理和协调责任。该方案应包括详细的以进度表表示的合同执行计划，标明完成合同所有关键活动的预计时间、顺序和内在联系。项目实施方案还应说明在合同执行期间，需要采购人和其它有关方所做的工作，以及建议采购人如何对有关各方活动进行协调。

### 10. 磋商保证金

详见须知前附表。

### 11. 磋商有效期

11.1 响应文件从磋商之日起，磋商有效期为 90 天。响应文件的有效期比本须知规定的有效期短的，将被视为非响应报价，采购人有权拒绝。

11.2 特殊情况下，采购人可于磋商有效期满之前要求供应商同意延长有效期，要求与答复均应为书面形式。供应商可以拒绝上述要求，其磋商保证金不被没收。对于同意该要求的供应商，既不要求也不允许其修改响应文件，但将要求其相应延长磋商保证金的有效期，有关退还和没收磋商保证金的规定在磋商有效期的延长期内继续有效。

### 12. 响应文件的签署及格式

12.1 响应文件正本应打印或用不褪色的墨水书写，并由供应商的法定代表人或其委托代理人签字加盖单位公章。委托代理人签字的，响应文件应附法定代表人签署的授权委托书。响应文件应尽量避免涂改、行间插字或删除。如果出现上述情况，改动之处应加盖单位公章或由供应商的法定代表人或其授权的代理人签字确认。字迹潦草、表达不清、未按要求填写而导致非唯一理解，造成非实质性响应竞争性磋商文件的响应文件将会被认定为无效投标。副本可以是正本的复印件，正本与副本不一致时以正本为准。

响应文件统一采用 A4 纸编制（如部分附表需要用其他规格的复印纸编写，则应按 A4 复印纸折叠），采用电脑打印或复印，文本格式采用常规的文本格式。一旦正本和副本有差异，以正本为准。

12.2 除供应商对错处作必要修改外，响应文件中不许有加行、涂抹或改写。若有修改须由签署响应文件的授权代表在旁边签字才有效。

12.3 以电话、传真、电子邮件形式的投标将被拒绝。

## 2.4.10 响应文件的提交

### 1. 响应文件的数量、包装和标记

1.1 供应商制作响应文件，壹份正本“响应文件”、贰份副本“响应文件”、电子版贰份（标注单位名称、项目编号），密封于“正本”纸质文件中。每套“响应文件”封面应注明“正本”或“副本”。一旦正本与副本不符，以正本为主。

1.2 响应文件必须密封递交。对封装材料及样式不作特别规定，但供应商应当保证其封装的可靠性，不因搬运、堆放等原因散开。

1.3 响应文件的密封材料和样式不作统一规定，各供应商应使用不易破损的包装材料进行包装。

### 2. 磋商截止时间

2.1 所有响应文件都必须按“招标公告”中规定的响应文件递交截止时间前送达竞争性磋商文件规定的递交地址。

2.2 出现因竞争性磋商文件的修改推迟投标截止日期时，则按采购人修改通知规定的时间递交。

2.3 在响应文件递交截止时间之后的任何响应文件将拒绝接收。

#### **2.4.11 响应文件的补充、修改、撤回（实质性要求）**

1. 供应商在递交响应文件后，在规定的截止时间之前，可以以书面形式补充修改或撤回已提交的响应文件，并以书面形式通知招标代理机构。补充或修改的内容作为响应文件的组成部分。

2. 供应商对响应文件的补充修改，应按照竞争性磋商文件的规定密封、标记和提交。其送达时间不得迟于磋商截止时间。

3. 在响应文件截止时间之后，供应商不得对其响应文件做任何修改，不得退回文件。

### **2.5 开启、资格审查、磋商和确定成交供应商**

#### **2.5.1 开标及开标程序**

一、本项目为线下开标。开标的开始时间为响应文件提交截止时间。成功提交响应文件的供应商不足3家的，不予开标，采购人或代理机构将作废标处理。

二、开标

2.1 采购代理机构按招标公告中规定的时间和地点接收供应商递交的响应文件，主持开标会议，邀请供应商参加。

2.2 开标时，由供应商代表检查响应文件的密封情况；经确认无误后，由采购代理机构工作人员当众拆封，宣布供应商名称、响应文件份数等内容。

#### **2.5.2 查询及使用信用记录**

开标结束后，采购人或代理机构根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的要求，通过“信用中国”网站（[www.creditchina.gov.cn](http://www.creditchina.gov.cn)）、“中国政府采购网”网站（[www.ccgp.gov.cn](http://www.ccgp.gov.cn)）等渠道，查询供应商在响应文件提交截止时间前的信用记录，拒绝列入失信被执行人名单、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中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

#### **2.5.3 资格审查**

详见竞争性磋商文件第四章。

#### **2.5.4 评审**

详见竞争性磋商文件第六章。

#### **2.5.5 成交通知书**

一、采购人或者磋商小组确认中标供应商后，代理机构在陕西省政府采购网发布成交结果公告、发出成交通知书。

二、成交通知书是采购人和中标供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的中标无效情形的，将以公告形式宣布发出的成交通知书无效，成交通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、成交通知书对采购人和中标供应商均具有法律效力。

### **2.6 签订及履行合同和验收**

### 2.6.1 签订合同

一、采购人应在成交通知书发出之日起三十内与成交供应商签订采购合同。

二、采购人和成交供应商签订的采购合同不得对竞争性磋商文件确定的事项以及成交供应商的响应文件作实质性修改。

### 2.6.2 合同公告

采购人应当自政府采购合同签订（双方当事人均已完成盖章）之日起2个工作日内，在陕西省政府采购网公告本项目采购合同，但合同中涉及国家秘密、商业秘密的内容除外。

### 2.6.3 合同备案

采购人自政府采购合同签订（双方当事人均已完成盖章）之日起7个工作日内，将本项目采购合同通过报同级财政部门备案。

### 2.6.4 采购人增加合同标的的权利

采购合同履行过程中，采购人需要追加与合同标的相同的货物或者服务的，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。

### 2.6.5 履行合同

一、合同一经签订，双方应严格履行合同规定的义务。

二、在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》规定及合同条款约定进行处理。

### 2.6.6 履约验收方案

按国家现行项目实施规范和合同规定的验收评定标准等要求进行验收，具体内容详见合同。

### 2.6.8 资金支付

采购人按财政部门的相关规定及采购合同的约定进行支付。

## 2.7 纪律要求

### 2.7.1 磋商活动纪律要求

采购人、代理机构应保证磋商活动在严格保密的情况下进行，采购人、代理机构、供应商和磋商小组成员应当严格遵守政府采购法律法规规章制度和本项目磋商文件以及代理机构现场管理规定，接受采购人委派的监督人员的监督，任何单位和个人不得非法干预和影响磋商过程和结果。

对各供应商的商业秘密，磋商小组成员应予以保密，不得泄露给其他供应商。

### 2.7.2 供应商不得具有的情形（实质性要求）

一、有下列情形之一的，视为供应商串通投标：

- （一）不同供应商的响应文件由同一单位或者个人编制；
- （二）不同供应商委托同一单位或者个人办理磋商事宜；
- （三）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；
- （四）不同供应商的响应文件异常一致或者响应报价呈规律性差异；
- （五）不同供应商的响应文件相互混装。
- （六）不同供应商的磋商保证金从同一单位或者个人的账户转出。

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他供应商；

四、与采购人或代理机构、其他供应商恶意串通；

五、向采购人或代理机构、磋商小组成员行贿或者提供其他不正当利益；

- 六、在招标过程中与采购人或代理机构进行协商磋商；
- 七、中标后无正当理由拒不与采购人签订政府采购合同；
- 八、未按照采购文件确定的事项签订政府采购合同；
- 九、将政府采购合同转包或者违规分包；
- 十、提供假冒伪劣产品；
- 十一、擅自变更、中止或者终止政府采购合同；
- 十二、拒绝有关部门的监督检查或者向监督检查部门提供虚假情况；
- 十三、法律法规规定的其他禁止情形。

供应商有上述情形的，按照规定追究法律责任，具备一至十一条情形之一的，其响应文件无效，或取消被确认为中标供应商的资格或认定中标无效。

### 2.7.3 采购人员及相关人员回避要求

政府采购活动中，采购人员及相关人员与供应商有下列利害关系之一的，应当回避：

- (一) 参加采购活动前3年内与供应商存在劳动关系；
- (二) 参加采购活动前3年内担任供应商的董事、监事；
- (三) 参加采购活动前3年内是供应商的控股股东或者实际控制人；
- (四) 与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；
- (五) 与供应商有其他可能影响政府采购活动公平、公正进行的关系。

供应商认为采购人员及相关人员与其他供应商有利害关系的，可以向代理机构书面提出回避申请，并说明理由。代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员应当回避。

## 2.8 询问、质疑和投诉

一、询问、质疑、投诉的接收和处理严格按照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购质疑和投诉办法》等规定办理。

二、供应商询问、质疑的答复主体：

根据委托代理协议约定，供应商对竞争性磋商文件中采购需求的询问、质疑由典亮工程项目管理有限公司负责答复；供应商对除采购需求外的采购文件的询问、质疑由典亮工程项目管理有限公司负责答复；供应商对采购过程、采购结果的询问、质疑由典亮工程项目管理有限公司负责答复。

三、供应商提出的询问，应当明确询问事项，如以书面形式提出的，应由供应商签字并加盖公章。

为提高采购效率，降低社会成本，鼓励询问主体对于不损害国家及社会利益或自身合法权益的问题或情形采用询问方式处理解决（包含但不限于文字错误、标点符号、不影响响应文件的编制的情形）。

四、供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：

- (一) 对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日
- (二) 对采购过程提出质疑的，为各采购程序环节结束之日；
- (三) 对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

五、本项目不接受在线提交质疑，供应商通过书面形式线下向采购人或代理机构提交质疑资料。

六、供应商提出质疑时应当准备的资料

- (一) 质疑书正本 1 份；（政府采购供应商质疑函范本）
- (二) 法定代表人或主要负责人授权委托书 1 份（委托代理人办理质疑事宜的需提供）；
- (三) 法定代表人或主要负责人身份证复印件 1 份；
- (四) 委托代理人身份证复印件 1 份（委托代理人办理质疑事宜的需提供）；
- (五) 针对质疑事项必要的证明材料。

答复主体：代理机构

联系人：李博

联系电话：17765836697

地址：西安市莲湖区南二环西段 9 号泊达国际酒店 27 楼东户

邮编：710000

注：根据《中华人民共和国政府采购法》的规定，供应商质疑不得超出采购文件、采购过程、采购结果的范围。

七、供应商对采购人或代理机构的质疑答复不满意，或者采购人或代理机构未在规定时间内作出答复的，供应商可以在答复期满后 15 个工作日内向同级财政部门提起投诉。

投诉受理单位：本采购项目同级财政部门。（政府采购供应商投诉书范本）

## 第三章 采购项目技术、服务、商务及其他要求

### 一、内容及要求

根据国家《信息安全等级保护管理办法》（公通字〔2007〕43号）、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303号）、《陕西省信息安全等级保护安全建设整改工作指导意见》（陕等保办〔2011〕2号）等相关文件要求，对采购人的信息管理系统（含HIS、LIS、PACS）、电子病历、医院综合运营管理系统、互联网医院、集成平台、云上妇幼远程医疗、智算基础平台（含AI语音诊疗应用系统、病历内涵质控系统）、OA、官网共9个核心系统（其中OA和官网为二级系统，其余为三级系统），实施网络安全等级保护测评工作。

#### （一）项目服务内容

1. 系统调研：在采购人系统相关负责人的协助下，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。

2. 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。

3. 分析整改：根据前述工作内容，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，配合采购人安全整改工作。

4. 结论报告：根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评，提供安全等级符合性测评服务，出具相关系统测评报告。

5. 配合验收：整理项目过程中所有相关的过程文档，提交采购人系统相关负责人。

#### （二）其他要求

1. 测评人员要求：本项目的测评人员需具有2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，并确保人员稳定。如需更换测评人员，须经采购人同意。

2. 人员配备：投标人参与此项目不少于6人，现场测评人员不得少于5人，其中至少包含2名高级测评师，3名中级测评师。投标人实施项目时需要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，能很好地执行和完成测评工作，并根据实际情况适当增加测评人员。

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、项目技术标准及要求

### （一）总体要求

根据国家《信息安全等级保护管理办法》（公通字〔2007〕43号）与《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019要求，等级测评工作须覆盖安全物理环境、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的内容，并根据现场实际情况完成风险分析工作，最终为完善等级保护安全防护体系提供指导依据。

### （二）第一阶段：等级保护

信息安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、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、安全运维管理十个安全类别进行安全测评。

#### 1. 定级要求

该项工作开展的主要依据是《网络安全等级保护定级指南》（GB/T 22240-2020）确定系统等级。

#### 2. 备案

信息系统的安全保护等级确定后，二级以上（含二级）信息系统的运营使用单位或主管部门应到属地公安机关办理备案手续。按照国家政策要求，跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应向当地设区的市级以上公安机关备案。该项目系统应向归属地网络安全监察支队申请重要信息系统备案。

完成备案的信息系统，将获得公安机关颁发的《信息系统安全等级保护备案证明》。

#### 3. 等级保护测评要求

投标人在测评过程中应按照等级保护2.0标准等相关规范开展等级测评工作。《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058-2010）、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018），对系统的安全物理环境、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、安全运维管理共10个层面进行安全等级保护测评。  
测评指标如下：

## 等级保护技术要求（二级）

安全层面	安全控制点	测评指标
安全物理环境	物理位置选择	a) 机房和办公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高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应有专人值守，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记； b) 应将通信线缆铺设在隐蔽安全处；
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a) 机房应设置火灾自动消防系统，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；
	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。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	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，至少满足主要设备在断电情况下的正常运行要求。
	电磁防护	电源线线和通信线缆应隔离铺设，避免互相干扰。
	安全通信网络	网络架构
通信传输		应采用校验技术保证通信过程中数据的完整性。
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	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。
	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，受控接口应拒绝所有通信； 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对进出数据流提供明确的允许/拒绝访问的能力；
	入侵防范	应在关键网络节点处监视网络攻击行为。
	恶意代码防范	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。
	安全审计	a) 应在网络边界、重要网络节点处进行安全审计，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。

安全层面	安全控制点	测评指标
	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；
		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；
		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。
	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；
		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。
	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。
	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；		
恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。	
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	应采用校验技术保证重要数据在传输过程中的完整性。	
数据和备份恢复	a) 应提供重要数据的本地数据备份与恢复功能；	
	b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。	
剩余信息保护	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。	
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。
安全管理中心	审计管理	a) 应对审计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审计操作，并对这些操作进行审计；
		b) 应通过审计管理员对审计记录进行分析，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；

安全层面	安全控制点	测评指标
		b) 应对要求管理人员或操作人员执行的日常管理操作建立操作规程。
	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； b) 应设立系统管理员、审计管理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	应配备一定数量的系统管理员、审计管理员和安全管理员等。
	授权和审批	a) 应根据各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执行审批过程。
	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	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。
	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。
	人员离岗	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。
安全管理人员	安全意识教育和培训	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。
	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。
	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。
安全建设管理	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进行安全方案设计； c) 应组织相关部门和有关安全专家对安全方案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； 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主管部门的要求。
	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。

安全层面	安全控制点	测评指标
	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。
	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。
	测试验收	a) 应制定测试验收方案, 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。
	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; 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。
	安全运维管理	环境管理
资产管理		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。
安全运维管理	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) 应对配套设施、软硬件维护管理做出规定, 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。
	漏洞和风险管理	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。
	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。
	恶意代码防范管理	a) 应增强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) 应对恶意代码防范要求做出规定, 包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等;

安全层面	安全控制点	测评指标
安全运维管理	恶意代码防范管理	c) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
	配置管理	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。
	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	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。
	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。		
应急预案管理	a) 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；	
	b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案演练。	
外包运维管理	a) 应确保外包运维投标人的选择符合国家的有关规定；	
	b) 应与选定的外包运维投标人签订相关的协议，明确约定外包运维的范围、工作内容。	

### 等级保护技术要求（三级）

安全类	安全控制点	测评项数	测评指标（2.0）
安全物理环境	物理位置选择	2	a) 机房和办公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高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	1	a) 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	3	a) 应将设备或主要部件进行固定，并设置明显的不易去除的标识；
			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	2	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	3	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。			
防水防潮	3	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	2	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	1	a) 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	

安全类	安全控制点	测评项数	测评指标 (2.0)
			的范围之内。
	电力供应	3	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	2	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	5	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	2	a) 应采用校验技术或密码技术保证通信过程中数据的完整性； b) 应采用密码技术保证通信过程中数据的保密性。	
可信验证	1	a) 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，在监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	4	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测或限制；
			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	5	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	4	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、攻击目的、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	2	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	4	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、用户、事件类型、事件是否成功及其他	

安全类	安全控制点	测评项数	测评指标 (2.0)
安全计算环境			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；
	可信验证	1	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。
			a) 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。
	身份鉴别	4	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；
			b) 应启用登陆失败处理功能，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时自动退出等相关措施；
			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；
			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密码技术实现。
	访问控制	7	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；
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；			
安全审计	4	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。	
		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、时间、事件类型、事件是否成功及其他与审计相关的工作；	
		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；	
入侵防范	6	d) 应对审计进程进行保护，防止未经授权的中断。	
		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；	
恶意代码防范	1	f) 应能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。	
		a) 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	1	a) 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	

安全类	安全控制点	测评项数	测评指标 (2.0)
			形成审计记录送至安全管理中心。
	数据完整性	2	a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性, 包括但不限于数据鉴别、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, 包括但不限于数据鉴别、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	2	a) 应采用密码技术保证重要数据在传输过程中的保密性, 包括但不限于数据鉴别、重要业务数据和重要个人信息等; b) 应采用密码技术保证重要数据在存储过程中的保密性, 包括但不限于数据鉴别、重要业务数据和重要个人信息等。
	数据备份和恢复	3	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用场地; c) 应提供重要数据处理系统的冗余, 保证系统的高可用性。
	剩余信息保护	2	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	2	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	2	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	2	a) 应对审计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审计操作, 并对这些操作进行审计; b) 应通过审计管理员对审计记录进行分析, 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。
	安全管理	2	a) 应对安全管理员进行身份鉴别, 只允许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识, 对主体进行授权, 配置安全可信验证策略等。
	集中管控	6	a) 应划分特定的管理区域, 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、安全代码、补丁升级等安全事项进行集中管理; 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	1	a) 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	3	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) 应对要求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, 记录表单等构成安全管

安全类	安全控制点	测评项数	测评指标 (2.0)
			理制度体系。
	制定和发布	2	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	1	a) 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	3	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、审计管理员、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	2	a) 应配备一定数量的系统管理员、审计管理员、安全管理员等；
			b) 应配备专职的安全管理员，不可兼任。
	授权和审批	3	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，及时更新授权和审批的项目、审批部门和审批人等信息。			
沟通和合作	3	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	3	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、安全配置和安全策略的一致性，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	3	a) 应指定或授权专门的部门或人员负责人员录用；
			b) 应对被录用人的身份、安全背景、专业资格或资质等进行审查，对其所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	2	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方可离开。			
安全意识教育和培训	3	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	4	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；	

安全类	安全控制点	测评项数	测评指标 (2.0)
			d) 获得系统访问授权的外部人员签署保密协议, 不得进行非授权操作, 不得复制和泄露敏感信息。
安全建设管理	定级和备案	4	a) 应以书面的形式说明保护对象的安全保护等级及确定安全保护等级的方法和理由;
			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	3	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, 设计内容应包含密码技术相关内容、并形成配套文件;
			c) 应组织相关部门和有关安全技术专家对整体安全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	3	a) 应确保网络安全产品采购和使用符合国家的有关规定;
			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主管部门的要求;
			c) 应预先对产品进行选型测试, 确定产品的候选范围, 并定期审定和更新产品候选名单。
	自行软件开发	7	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	3	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面和隐蔽信道。	
工程实施	3	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	2	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安全测试内容。	
系统交付	3	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) 应对负责系统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	3	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;	

安全类	安全控制点	测评项数	测评指标 (2.0)
			b) 在发生重大变化或级别发生时进行等级测评;
			c) 应确保测评机构的选择符合国家相关规定。
			a) 应确保服务供应商的选择符合国家的有关规定;
	服务供应商管理	3	b) 应与选定的投标人签订相关协议, 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, 并对其变更服务进行控制。
			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;
	环境管理	3	b) 应建立机房安全管理制度, 对有关物理访问, 物品带进带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, 不随意放置包含敏感信息的纸质文件和移动介质。
			a) 应编制并保存与信息系统相关的资产清单, 包括资产责任部门、重要程度和所处位置等内容;
	资产管理	3	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做出规定, 并对信息的使用, 传输和存储等进行规范化管理。
			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;
	介质管理	2	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, 并对介质归档和查询等进行登记记录。
			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;
安全运维管理	设备维护管理	4	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) 信息处理设备应经过审批才能带离机房或办公地点, 含有储存介质的设备带出工作环境时其重要数据应加密;
			d) 含有存储介质的设备在报废或重用前, 应进行完全清除或完全覆盖, 保证该设备上的敏感数据和授权软件无法被恢复重用。
			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;
	漏洞和风险管理	2	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。
			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;
	网络和系统安全管理	10	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、参数的设置和修改的内容;
			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;

安全类	安全控制点	测评项数	测评指标 (2.0)
			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, 操作结束后应同步配置更新配置信息库;
			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行为。
	恶意代码防范管理	2	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	2	a) 应记录和保存基本配置信息, 包括网络拓扑结构、各类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	2	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	3	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) 应建立终止变更并从失败的变更中恢复的程序, 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	3	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、存储介质和保存期等;
			c) 应根据数据的重要性的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	4	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露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	4	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	4	a) 应确保外包运维投标人的选择符合国家有关规定;
			b) 应与选定的外包运维投标人签订相关的协议, 明确约定外包运维的范围、工作内容;

安全类	安全控制点	测评项数	测评指标 (2.0)
			c) 应保证选择的外包运维投标人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，并将能力在签订的协议中明确； d) 应在与外包运维投标人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、储存要求，对IT基础设施中断服务的应急保障要求等。

注：本次系统测评项目需按照等级保护2.0测评标准执行。

### (三) 第二阶段：渗透检测

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机信息系统是否安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，通常该分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

另：针对本次信息系统等级保护测评服务项目，投标人可自行选择提供包含但不限于风险评估、基线测评等在内的其他非必要响应服务。

### (四) 第三阶段：建设整改咨询及安全加固（不涉及硬件）

建设整改咨询工作以等级测评和渗透检测发现的安全问题为工作重点，编写《信息系统安全建设整改建议》；将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。

在医院依据相关《信息系统安全建设整改建议》开展建设整改工作时，投标人将提供建设整改过程中的与建设整改相关的咨询服务。

对信息系统安全整改建议进行确认，并依照建议，协助采购人进行漏洞修复、补丁升级等非硬件层面的安全加固，制定可执行的安全整改方案和计划，并协助采购人分步实施安全整改工作。

### (五) 第四阶段：售后服务

为期一年的售后服务工作中，向采购人提供包括应急响应、安全监测、配合检查、电话支持、安全咨询、重要活动安全保障等服务在内的安全维保服务。具体服务内容如下：

#### 1. 应急响应服务

针对本次项目，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

协助采购人响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助采购人准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

### 3. 电话支持服务

每周7天/每天24小时不间断的电话支持服务，解答采购人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。电话响应时间不大于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

为采购人提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到采购人的服务请求，技术服务工程师将立即开始提供服务，帮助采购人解决信息安全相关技术问题，全面配合采购人做好业务系统安全保障工作。

## 三、保密责任与赔偿承诺

1. 严格遵守采购人有关保密规定，不得泄露系统的一切敏感信息。

2. 对项目进行深入细致调研，并结合实际对测评方案进行完善。在测评过程中，投标人需保证工具测试过程中不影响系统正常运行，并保证网络拓扑、IP地址等敏感信息不被泄露。

3. 在技术服务期间，对接触到的有关采购人商业活动、技术情报和技术资料等文件进行保密。

## 四、商务要求

1. 服务地点：采购人指定地点。

2. 实施工期：实施工期≤30天。

3. 验收标准：成交供应商提交满足技术参数要求的验收文档；服务项目验收应在所有系统技术服务完毕，且在服务期内无重大缺陷、问题、冲突等。

4. 付款方式：银行转账。项目验收合格后30个日历日一次性付清。付款前成交供应商须提供符合税法规定的全额正式发票。

5. 维保期：本次系统测评项目需按照等级保护2.0测评标准执行，维保期一年。

## 五、交付内容

1. 《信息系统安全等级测评报告》

2. 《信息系统整改建议书》

3. 《信息系统渗透测试报告》

## 第四章 资格审查

资格审查由代理机构依据法律法规和磋商文件的规定，对响应文件中的资格证明等进行审查，以确定供应商是否具备响应资格。

资格审查标准及要求如下：

1. 供应商为具有独立承担民事责任能力的法人、其他组织或自然人。企业法人应提供合法有效的标识有统一社会信用代码的营业执照；事业法人应提供事业单位法人证书；其他组织应提供合法登记证明文件；自然人应提供身份证；

2. 财务状况：提供注册会计师行业统一监管平台(网址 <http://acc.mof.gov.cn>)赋码可查询的 2024 年度或 2025 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）；或开标前 12 个月内其开户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. 具有依法缴纳税收的良好记录：提供缴费所属日期为投标截止时间前 12 个月内任一月份（投标截止时间当月不计入）的增值税（或所得税）缴费凭据或税务机关出具的完税证明/在法规范围内不需提供的应出具书面说明和证明文件；或具有依法缴纳税收的诚信声明；以上两种形式的资料提供任何一种即可；

4. 具有依法缴纳社会保障资金的良好记录：提供缴费所属日期为投标截止时间前 12 个月内任一月份（投标截止时间当月不计入）的缴费凭据或社保机关出具的缴费证明/在法规范围内不需提供的应出具书面说明和证明文件；或具有依法缴纳社会保障资金的缴纳记录的诚信声明；以上两种形式的资料提供任何一种即可；

5. 授权委托书：法定代表人参加投标须提供《法定代表人身份证明》及身份证复印件；法定代表人授权他人参加投标，须提供《法定代表人授权委托书》及委托代理人身份证复印件；

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

7. 具有履行合同所必需的设备和专业技术能力：具有履行合同所必需的设备和专业技术能力，提供声明文件；

8. 供应商须提供公安部第三研究所颁发的《网络安全服务认证证书（等级保护测评服务认证）》；

9. 非联合体声明：本项目不接受联合体投标（须提供声明函）。

10. 磋商保证金：须提供。

11. 中小企业声明函：本项目为专门面向中小企业项目，须符合《政府采购促进中小企业发展管理办法》（财库【2020】46 号）规定的中小企业参加，提供《中小企业声明函》。

## 第五章 磋商过程中可实质性变动的内容

磋商小组可以根据磋商文件和磋商情况实质性变动第三章“采购项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，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。

在磋商过程中，磋商小组根据项目实际需要制定磋商内容，在获得采购人代表确认的前提下，可以根据磋商情况实质性变动相关内容。磋商小组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，磋商小组应及时通知所有参加磋商的供应商。

## 第六章 磋商办法

### 6.1 总则

一、根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购竞争性磋商采购方式管理暂行办法》《陕西省政府采购评审专家管理实施办法》等法律法规，结合本采购项目特点制定本竞争性磋商评审方法。

二、评审工作由代理机构组织，具体评审事务由依法组建的磋商小组负责。

三、评审工作应遵循客观、公正、审慎的原则，并以相同的磋商程序 and 标准对待所有的供应商。

四、本项目采取线下评审。磋商小组成员、采购人、代理机构和供应商应当按照本磋商文件规定开展或者参加评审活动。

五、评审过程应当独立、保密，任何单位和个人不得非法干预评审活动。供应商非法干预评审活动的，其响应文件将作无效处理；代理机构、采购人及其工作人员、采购人监督人员非法干预评审活动的，将依法追究其责任。

### 6.2 磋商小组

一、评审专家是采取随机方式在政府采购平台的专家库系统（以下简称专家库系统）抽取/由采购人根据《陕西省政府采购评审专家管理实施办法》（陕财办采〔2018〕20号）的规定，报主管部门同意后自行选定。

二、磋商小组成员应当满足采购评审的工作需要，签到、推荐磋商小组组长。

三、磋商小组成员根据响应文件，开展评审活动。出现应当回避的情形时，磋商小组成员应当主动回避；代理机构按规定申请补充抽取评审专家；无法及时补充抽取的，采购人或者代理机构应当封存供应商响应文件，按规定重新组建磋商小组，解封响应文件后，开展评审活动。

四、磋商小组按照磋商文件规定的磋商程序、评分方法和标准进行评审，并独立履行下列职责：

- （一）熟悉和理解磋商文件；
- （二）审查供应商响应文件等是否满足磋商文件要求，并作出评价；
- （三）根据需要要求采购组织单位对磋商文件作出解释；根据需要要求供应商对响应文件有关事项作出澄清、说明或者更正；
- （四）推荐成交候选供应商，或者受采购人委托确定成交供应商；
- （五）起草资格审查报告、评审报告并进行签署；
- （六）向采购组织单位、财政部门或者其他监督部门报告非法干预评审工作的行为；
- （七）法律、法规和规章规定的其他职责。

### 6.3 评审程序

#### 6.3.1. 熟悉和理解磋商文件和停止评审

一、磋商小组正式评审前，应当对磋商文件进行熟悉和理解，内容主要包括磋商文件中供应商资格条件要求、采购项目技术、服务和商务要求、磋商办法和标准、政府采购政策要求以及政府采购合同主要条款等。

二、本磋商文件有下列情形之一的，磋商小组应当停止评审：

- （一）磋商文件的规定存在歧义、重大缺陷的；
- （二）磋商文件明显以不合理条件对供应商实行差别待遇或者歧视待遇的；
- （三）采购项目属于国家规定的优先、强制采购范围，但是磋商文件未依法体现优先、强制采购相关规定的；

(四) 采购项目属于政府采购促进小微企业发展的范围，但是磋商文件未依法体现促进小微企业发展相关规定的；

(五) 磋商文件将供应商的资格条件列为评分因素的；

(六) 磋商文件载明的成交原则不合法的；

(七) 磋商文件有违反国家其他有关强制性规定的情形。

出现上述应当停止评审情形的，磋商小组应当向采购组织单位提交相关说明材料，说明停止评审的情形和具体理由。除上述情形外，磋商小组不得以任何方式和理由停止评审。

出现上述应当停止评审情形的，采购组织单位应当在陕西省政府采购网公告。采购组织单位认为磋商小组不应当停止评审的，可以书面报告采购项目同级财政部门依法处理，并提供相关证明材料。

### 6.3.2 符合性审查

一、磋商小组依据本磋商文件的实质性要求，对符合资格的响应文件进行审查，以确定其是否满足本磋商文件的实质性要求。本项目的符合性审查事项必须以本磋商文件的明确规定的实质性要求为依据。

二、在符合性审查过程中，如果出现磋商小组成员意见不一致的情况，按照少数服从多数的原则确定，但不得违背政府采购基本原则和磋商文件规定。

三、磋商小组对所有响应文件进行审查后，确定参加磋商的供应商名单。

符合性审查标准见下表：

采购包 1：

序号	符合审查要求概况	评审点具体描述
1	不正当竞争预防措施（实质性要求）	启动异常低价投标（响应）审查。 <b>具体内容详见 2.4.7 响应报价（实质性要求）</b>
2	有效性审查	响应文件的签署、加盖公章是否有效；提供的各种证明文件、数据、资料是否有效。
3	完整性审查	响应文件是否按照磋商文件要求的格式编写；响应文件内容是否有重大缺漏项。
4	响应性审查	1. 响应报价是否超过采购预算（限价）； 2. 响应报价有效期是否符合磋商文件的要求； 3. 响应文件内容是否符合国家法律法规，没有重大偏离； 4. 对磋商文件中规定的要求是否做出了实质性响应。
5	不存在政府采购规定的串通投标的情形。	1. 不同供应商的响应文件由同一单位或者个人编制； 2. 不同供应商委托同一单位或者个人办理响应事宜； 3. 不同供应商的响应文件载明的项目管理成员或者联系人员为同一人； 4. 不同供应商的响应文件异常一致或者磋商报价呈规律性差异； 5. 不同供应商的响应文件相互混装； 6. 不同供应商的投标保证金从同一单位或者个人的账户转出。

### 6.3.3 磋商

一、磋商小组按照磋商文件的规定与邀请参加磋商的供应商分别进行磋商，磋商顺序由磋商小组确定。

二、磋商小组所有成员集中与单一供应商对技术、服务、合同条款等内容分别进行一轮或多轮的磋商。在磋商中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

三、磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，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。

四、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，磋商小组应将变动情况同时通知所有参加磋商的供应商。磋商过程中，磋商小组可以根据磋商情况调整磋商轮次。

五、磋商过程中，磋商文件变动的，供应商应当按照磋商文件的变动情况和磋商小组的要求就磋商文件变动部分，以“供应商响应表”形式在线提交磋商小组。“供应商响应表”作为响应文件的组成部分，响应文件应加盖供应商（法定名称）印章，否则无效。

六、经最终磋商后，响应文件仍有下列情况之一的，应按照无效响应处理：

（一）响应文件仍不能实质响应磋商文件可实质性变动的实质性要求的；

（二）响应文件中仍有磋商文件规定的其他无效响应情形的。

七、磋商小组对供应商在磋商、评审过程中的书面交换材料，未按要求加盖印章或签字的，视同未提交书面交换材料。

八、磋商小组在最终磋商后，对所有响应文件的有效性、完整性和响应程度进行审查后，确定最后报价的供应商名单。

九、磋商过程中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

十、磋商过程中，磋商小组发现或者知晓供应商存在违法行为的，应当磋商报告中予以记录，并向本级财政部门报告，依法应将该供应商响应文件作无效处理的，应当作无效处理。

#### **6.3.4 最后报价（现场磋商环节报价）**

##### **一、方案评审**

采购包1：磋商/谈判/协商文件能够详细列明采购标的的技术、服务要求，磋商/谈判/协商结束后，磋商/谈判/协商小组可以根据磋商/谈判/协商情况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，提交最后报价的供应商不得少于3家。

二、供应商在未提高响应文件中承诺的标准情况下，其最后报价不得高于对该项目之前的报价，否则，磋商小组将对其响应文件作无效处理，并告知供应商，说明理由。

三、供应商最后报价属于明显低价不正当竞争的，磋商小组应按照“供应商须知前附表”第8项规定处理。

四、供应商未在响应文件提交截止时间内提交报价或未按要求进行报价的，视为无效响应，由供应商自行承担不利后果。

五、供应商未按磋商小组要求在规定时间内提交最后报价的，视为其退出磋商。

六、最后报价一旦提交后，供应商不得以任何理由撤回。

七、最后报价为有效报价应符合下列条件：

（一）供应商所提供的最后报价是在规定的时间内提交。

（二）供应商的最后报价应加盖供应商（法定名称）印章或授权代表签字。

（三）供应商的最后报价应符合磋商文件的要求。

（四）最后报价唯一，且不高于最高限价。

八、最后报价出现下列情况的，不需要供应商澄清，按以下原则处理：

（一）报价中的大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；

（二）单价金额小数点或者百分比有明显错位的，应以总价为准，并修改单价；

（三）总价金额与按单价汇总金额不一致的，以单价汇总金额计算结果为准；

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的最后报价经加盖供应商（法定名称）印章后产生约束力，供应商不确认的，其最后报价无效。

#### **6.3.5 解释、澄清有关问题**

一、评审过程中，磋商小组认为磋商文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变磋商文件的原义或者影响公平、公正，解释事项如果涉及供应商权益的以有利于供应商的原则进行解释。

二、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，磋商小组应当要求供应商作出必要的澄清、说明或者更正，并给予供应商必要的反馈时间。供应商应当按磋商小组的要求进行澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。澄清不影响响应文件的效力，有效的澄清、说明或者更正材料是响应文件的组成部分。

三、供应商的澄清、说明或者更正需进行签章，应当不超出响应文件的范围、不实质性改变响应文件的内容、不影响供应商的公平竞争、不导致响应文件从不响应磋商文件变为响应磋商文件的条件。下列内容不得澄清：

（一）供应商响应文件中不响应磋商文件规定的技术参数指标和商务应答；

（二）供应商响应文件中未提供的证明其是否符合磋商文件资格、符合性规定要求的相关材料。

（三）供应商响应文件中的材料因印刷、影印等不清晰而难以辨认的。

四、响应文件报价出现前后不一致的情形，按照本章前述规定予以处理，不需要供应商澄清。

五、代理机构宣布评审结束之前，供应商应随时关注评审消息提示，及时响应磋商小组发出的澄清、说明或更正要求。供应商未能及时响应的，自行承担不利后果。

六、磋商小组应当积极履行澄清、说明或者更正的职责，不得滥用权力。

### **6.3.6 比较与评价**

磋商小组应当按照磋商文件规定的评标细则及标准，对符合性检查合格的响应文件进行商务和技术评估，综合比较和评价。

### **6.3.7 复核**

评审结束后，磋商小组应当进行复核，特别要对拟推荐为成交候选供应商的、报价最低的、响应文件被认定为无效的的进行重点复核。

评审结果汇总完成后，磋商小组拟出具磋商报告前，代理机构应当组织2名以上的工作人员，在采购现场监督人员的监督之下，依据有关的法律制度和磋商文件对评审结果进行复核，出具复核报告。代理机构复核过程中，磋商小组成员不得离开评审现场。

除资格检查认定错误、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，采购人或者代理机构不得以任何理由组织重新评审。采购人、代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，应当重新开展采购活动，并同时书面报告本级财政部门。

### **6.3.8 推荐成交候选供应商**

磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐如下成交候选供应商，并编写磋商报告。

采购包1：3家；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，按照技术指标优劣顺序推荐。评审得分且最后报价且技术指标得分均相同的，成交候选供应商并列。

### **6.3.9 编写磋商报告**

磋商小组推荐成交候选供应商后，应向代理机构出具磋商报告。磋商报告应当包括以下主要内容：

（一）邀请供应商参加采购活动的具体方式和相关情况；

（二）响应文件开启日期和地点；

（三）获取磋商文件的供应商名单和磋商小组成员名单；

（四）评审情况记录和说明，包括对供应商响应文件审查情况、磋商情况、报价情况等；

(五) 提出的成交候选供应商的排序名单及理由。

磋商报告应当由磋商小组全体人员签字或加盖电子签章认可。磋商小组成员对磋商报告有异议的，磋商小组按照少数服从多数的原则推荐成交候选供应商，采购程序继续进行。对磋商报告有异议的磋商小组成员，应当在报告上签署不同意见并说明理由，由磋商小组记录相关情况。磋商小组成员拒绝在磋商报告上签字，又不书面说明其不同意见和理由的，视为同意磋商报告。

#### 6.3.10 评审争议处理规则

在磋商过程中，对于符合性审查、对响应文件作无效响应处理的及其他需要共同认定的事项存在争议的，应当以少数服从多数的原则作出结论，但不得违背磋商文件规定。持不同意见的磋商小组成员应当在磋商报告中签署不同意见及理由，否则视为同意评审报告。持不同意见的磋商小组成员认为认定过程和结果不符合法律法规或者磋商文件规定的，应当及时向采购人或代理机构书面反映。采购人或代理机构收到书面反映后，应当书面报告采购项目同级财政部门依法处理。

### 6.4 评审办法及标准

一、磋商小组只对通过资格审查的响应文件，根据磋商文件的要求采用相同的评审程序、评分办法及标准进行评价和比较。

二、磋商小组成员应依据磋商文件规定的评分标准和方法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。

#### 6.4.1 评分办法

本次评审采用综合评分法，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。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

#### 6.4.2 评分标准

评审因素		评审标准	
分值构成		详细评审 75.0000 分 报价得分 25.0000 分	
评审因素分类	评审项	详细描述	分值
服务方案	工作流程和实施方案	<p>供应商结合采购人实际需求，提供完整的项目工作流程、实施方案，对等级测评各个工作阶段的工作内容、工作方法及工作成果具有详细说明。</p> <p>方案详实完整，针对性、可操作性强，完全满足采购需求得 10 分；以上方面中每缺少一方面内容扣 2 分；每有一处内容与实际需求不符或不满足要求扣 0.5 分，扣完为止。未提供不得分。</p>	10.0
	增值服务	<p>技术方案依据国家等级保护 2.0 测评标准体系要求，并结合采购人实际要求，提供包含但不限于风险评估、基线测评等在内的其它增值性响应服务。</p> <p>方案描述详细，测评指标选取合理，测评内容及方法明确，服务条理清晰，满足技术规范书要求，得 10 分；以上方面中每缺少一方面内容扣 5 分；每有一处内容与实际需求不符或不满足要求扣 0.5 分，扣完为止。</p>	10.0

	质量管控措施	<p>供应商针对本项目具有严格的项目质量管控措施、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。</p> <p>项目质量管控措施的完整，符合项目实际需求，得6分；以上方面中每缺少一方面内容扣2分；每有一处内容与实际需求不符或不满足要求扣0.5分，扣完为止。</p>	6.0
	工作分配及实施进度	<p>根据供应商对项目组成员工作分配及项目实施进度具有科学合理安排程度赋分。</p> <p>成员工作分配科学，进度安排科学、紧凑，得8分；以上方面中每缺少一方面内容扣4分；每有一处内容与实际需求不符或不满足要求扣0.5分，扣完为止。</p>	8.0
	风险防范措施和保密措施	<p>供应商针对本项目的服务提供明确的过程中的风险防范措施、保密措施、明确保密责任与赔偿承诺。</p> <p>风险防范措施、保密措施完整、保密责任与赔偿承诺明确，得6分；以上方面中每缺少一方面内容扣1.5分；每有一处内容与实际需求不符或不满足要求扣0.5分，扣完为止。</p>	6.0
项目团队	项目经理和质量负责人	<p>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：网络安全等级测评师高级证书、信息系统项目管理师(高级)、注册信息安全专业人员 CISP 证书；每提供1个证书计1分，满分6分。</p> <p>备注：提供项目经理和质量负责人的劳动合同或近三个月在本单位的社保缴纳证明，未提供不得分。</p> <p>并对测试说明、渗透测试工作方法、工作成果内容有详细说明，得3分；以上方面中每缺少一方面内容扣1分；每有一处内容与实际需求不符或不满足要求扣0.5分，扣完为止。</p>	9.0
	人员配备	<p>供应商参与此项目不少于6人，现场测评人员不得少于5人，其中至少包含2名高级测评师，每提供一人得1.5分，共6分；至少包含3名中级测评师，每提供一人得1分，共得5分；</p> <p>备注：提供具有《网络安全等级高级测评师》《网络安全等级中级测评师》证书人员的劳动合同或近三个月在本单位的社保缴纳证明，未提供不得分。</p>	11.0
企业实力	证书	<p>供应商具有信息安全风险评估资质证书，计2分；ISO27001信息安全管理体系认证证书，计1分；具有ISO9001质量管理体系认证证书，计1分；满分4分，未提供不计分。</p>	4.0
	业绩	<p>供应商提供2023年4月1日至今同类项目业绩，以合同签订日期为准，每提供1份计1分，满分5分；未提供不计分。（需提供合同关键页并加盖单位公章）。</p>	5.0
售后服务	服务能力	<p>供应商需要有本地化服务的能力，提供相关证明材料，计1分。</p>	1.0

	售后服务	为保障在测评项目结束后的信息安全，要求供应商提供完善的售后服务，包括应急响应、安全监测、配合检查、安全咨询、重要活动安全保障等服务。 服务内容完善并有详细说明，得5分；以上方面中每缺少一方面内容扣1分；每有一处内容与实际需求不符或不满足要求扣0.5分，扣完为止。未提供不得分。	5.0
价格分	价格	价格得分采用低价优先法计算，即满足磋商文件要求且最终报价最低的供应商的价格为磋商基准价，其价格得分为满分。其他供应商的价格得分统一按照下列公式计算：磋商报价得分=（磋商基准价/最终磋商报价）×价格权值（25%）×100	25.0

#### 价格扣除

序号	情形	适用对象	比例	说明	关联格式
无					

## 6.5 终止采购活动

出现下列情形之一的，采购人或者代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

- （一）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；
- （二）出现影响采购公正的违法、违规行为的；
- （三）除《政府采购竞争性磋商采购方式管理暂行办法》第二十一条第三款规定的情形外，在采购过程中符合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（财政部另有规定的除外）；
- （四）法律法规规定的其他情形。

## 6.6 确定成交供应商

一、评审结束后，代理机构在评审结束之日起2个工作日内将磋商报告及有关资料送交采购人。

二、采购人在收到磋商报告后5个工作日内，在磋商报告确定的成交候选供应商名单中按顺序确定成交供应商。成交候选供应商并列的，由采购人采取随机抽取的方式确定成交供应商。

三、采购人逾期未确定成交供应商且不提出异议的，视为确定磋商报告提出的排序第一的供应商为成交供应商。

四、根据采购人确定的成交供应商，代理机构在陕西省政府采购网上发布成交结果公告，同时向成交供应商发出成交通知书。

## 6.7 评审专家在政府采购活动中承担以下义务

- （一）遵守评审工作纪律；
- （二）按照客观、公正、审慎的原则，根据采购文件规定的评审程序、评审方法和评审标准进行独立评审；
- （三）不得泄露评审文件、评审情况和在评审过程中获悉的商业秘密；
- （四）及时向监督管理部门报告评审过程中的违法违规情况，包括采购组织单位向评审专家作出倾向性、误导性的解释或者说明情况，供应商行贿、提供虚假材料或者串通情况，其他非法干预评审情况等；

(五) 发现采购文件内容违反国家有关强制性规定或者存在歧义、重大缺陷导致评审工作无法进行时，停止评审并通过项目电子化交易系统向采购组织单位书面说明情况，说明停止评审的情形和具体理由；

(六) 配合答复处理供应商的询问、质疑和投诉等事项；

(七) 法律、法规和规章规定的其他义务。

## 6.8 评审专家在政府采购活动中应当遵守以下工作纪律

(一) 遵行《中华人民共和国政府采购法》第十二条和《中华人民共和国政府采购法实施条例》第九条及财政部关于回避的规定。

(二) 评审前，应当将通讯工具或者相关电子设备交由采购组织单位统一保管。

(三) 评审过程中，不得与外界联系，因发生不可预见情况，确实需要与外界联系的，应当在监督人员监督之下办理。

(四) 评审过程中，不得干预或者影响正常评审工作，不得发表倾向性、引导性意见，不得修改或细化磋商文件确定的评审程序、评审方法、评审因素和评审标准，不得接受供应商主动提出的澄清和解释，不得征询采购人代表的意见，不得协商评分，不得违反规定的评审格式评分和撰写评审意见，不得拒绝对自己的评审意见签字确认。

(五) 在评审过程中和评审结束后，不得记录、复制或带走任何评审资料，不得向外界透露评审内容。

(六) 服从评审现场采购组织单位的现场秩序管理，接受评审现场监督人员的合法监督。

(七) 遵守有关廉洁自律规定，不得私下接触供应商，不得收受供应商及有关业务单位和个人的财物或好处，不得接受采购组织单位的请托。

## 第七章 响应文件格式

【正本或副本】

### 响应文件封面

采购项目名称：\_\_\_\_\_

采购项目编号：\_\_\_\_\_

供应商名称：\_\_\_\_\_

法定代表人或被授权人（签字或盖章）：\_\_\_\_\_

日期：\_\_\_\_\_

# 一、响应函

致： {代理机构名称}

我单位作为 {项目名称}（项目编号： {项目编号}）的投标（响应）供应商，自愿参与本项目政府采购活动，充分理解采购文件的要求，在此郑重声明及承诺：

一、我单位具有独立承担民事责任的能力；

二、我单位具有良好的商业信誉和健全的财务会计制度；

三、我单位具有履行合同所必需的设备和专业技术能力；

四、我单位具有依法缴纳税收和社会保障资金的良好记录；

五、我单位参加政府采购活动前三年内，在经营活动中没有重大违法记录；

六、我单位满足采购文件规定的特定条件；

七、我单位不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为；

八、我单位不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商；

九、我单位不存在与其他供应商委托同一单位或者个人编制投标（响应）文件、办理投标（响应）事宜的情形；

十、如本项目采购过程中需要提供样品，我单位提供的样品即为中标（成交）后将要提供的产品，我单位对提供样品的性能和质量负责，因样品存在缺陷或者不符合采购文件要求导致未能中标（成交）的，我单位愿意承担相应不利后果；

十一、我单位一旦中标（成交），将严格按照采购文件规定交纳代理服务费，在约定期限内签订采购合同，并严格履行采购合同规定的责任和义务；

十二、我单位在本项目使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由我单位承担所有相关责任；

十三、我单位完全接受和理解本项目采购文件规定的实质性要求；

十四、我单位承诺，响应有效期为提交响应文件截止之日起 90 天；

十五、我方提交纸质响应文件正本 壹 份和副本 贰 份，U盘 贰 份（内含响应文件正本的Word版本及PDF版本）。并保证响应文件提供的数据和材料是真实、准确的。否则，愿承担《政府采购法》第七十七条规定的法律责任。

根据采购文件规定，以上承诺事项如需提供相关证明材料的，以投标（响应）文件中提供的证明材料为准。本函发出后，即对我单位产生约束力，我单位保证严格遵守本响应函的



## 二、磋商一览表

项目名称：

项目编号：

磋商一次报价（元）	服务地点	实施工期	维保期
大写： _____ 小写： _____	采购人指定地点		
备注：表内报价内容以元为单位，精确到小数点后两位。			

供应商（单位名称及公章）： \_\_\_\_\_

法定代表人或被授权人（签字或盖章）： \_\_\_\_\_

日 期： \_\_\_\_年\_\_月\_\_日

### 三、分项报价表

项目名称：

项目编号：

序号	服务内容	数量	单位	单价	总价	备注
1						
...						
N						
磋商总报价（人民币大写）：				（¥_____）		
备注：表内总报价保留小数点后两位。						

说明：

1. 所有磋商报价均含税，且用人民币表示，单位为元，精确到小数点后两位；
2. 该表中包含供应商认为完成本项目所需的所有费用，合计总价应与磋商一次报价表中响应总价金额一致。

供应商（单位名称及公章）：\_\_\_\_\_

法定代表人或被授权人（签字或盖章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_月\_\_日

## 四、技术、服务、合同条款及其他商务要求应答表

序号	磋商文件要求	磋商文件应答	备注
1			
2			
...	...	...	...

注：供应商人根据磋商文件第3章“服务内容及服务要求”逐条填写此表，并按磋商文件要求提供相应的证明材料。

供应商（单位名称及公章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_月\_\_日

## 五、 供应商资格证明资料

供应商需在此页附竞争性磋商文件中要求的资格证明文件，响应文件附资质复印件或扫描件加盖供应商公章。格式参考见下页。

### 附： 资质证明文件格式：

1、 供应商符合《政府采购法》第二十二条规定条件的承诺函

致典亮工程项目管理有限公司：

本公司\_\_\_\_\_（公司名称）参加\_\_\_\_\_的投标活动，现承诺：

我公司满足政府采购法第二十二条关于供应商的资格要求：

- （一）具有独立承担民事责任的能力；
- （二）具有良好的商业信誉和健全的财务会计制度；
- （三）具有履行合同所必需的设备和专业技术能力；
- （四）有依法缴纳税收的良好记录；
- （五）参加政府采购活动前三年内，在经营活动中没有重大违法记录；
- （六）法律、行政法规规定的其他条件。

同时也满足本项目法律法规规章规定关于供应商的其他资格性条件，未参与本采购项目前期咨询论证，不属于禁止参加投标的供应商。

如违反以上承诺，本公司愿承担一切法律责任。

供应商（单位名称及公章）：\_\_\_\_\_

法定代表人或被授权人（签字或盖章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_月\_\_日

## 2、供应商基本情况一览表

2-1 供应商基本情况一览表

供应商名称						
注册地址				邮政编码		
联系方式	联系人			电话		
组织结构						
法定代表人	姓名		技术职称		电话	
技术负责人	姓名		技术职称		电话	
成立时间			员工总人数：			
营业执照号			其中	高级职称人员		
注册资金				中级职称人员		
开户银行				初级职称人员		
账号				技 工		
经营范围						
备注						

2-2 供应商营业执照等资质证明材料。

### 3、法定代表人证明书及法定代表人授权书

#### 3-1 法定代表人证明书

致：典亮工程项目管理有限公司				
企 业 法 人	企业名称			
	法定地址			
	注册资金			
	工商登记机关			
	统一社会信用代码			
法 定 代 表 人	姓名		性别	
	职务		联系电话	
	传真			
法 定 代 表 人 身 份 证 复 印 件	(正反面)		法定代表人 (签字或盖章)	
			(供应商公章)	
		年 月 日		

### 3-2法定代表人授权书

#### 法定代表人授权书

典亮工程项目管理有限公司：

本授权委托书声明：我（法定代表人姓名）\_\_\_\_\_系注册于\_\_\_\_\_（供应商地址）\_\_\_\_\_的（供应商名称）\_\_\_\_\_的法定代表人，现代表公司授权（被授权人的姓名、职务）\_\_\_\_\_为我公司合法代理人，代表本公司参加（项目名称）\_\_\_\_\_采购项目编号为\_\_\_\_\_的采购活动。以我方名义全权处理该项目有关投标、签订合同以及执行合同等一切事宜。

本授权书有效期自响应文件递交截止之日起 90 日历日，特此声明。

供应商（单位名称及公章）：\_\_\_\_\_

法定代表人（签字或盖章）：\_\_\_\_\_

被授权人（签字或盖章）：\_\_\_\_\_性别：\_\_\_\_\_职务：\_\_\_\_\_

被授权人身份证号码：\_\_\_\_\_

联系地址：\_\_\_\_\_

联系电话：\_\_\_\_\_

法定代表人及被授权人身份证复印件

法定代表人身份证复印件（正/反面）	被授权人身份证复印件（正/反面）
-------------------	------------------

#### 4、无重大违法记录声明

我单位参与典亮工程项目管理有限公司组织的\_\_\_\_（项目名称）\_\_\_\_竞争性磋商，我单位郑重声明：我方参加本项目竞争性磋商工作前三年内在经营活动中无重大违法活动记录，未被信用中国网（www.creditchina.gov.cn）列入失信被执行人、重大税收违法案件当事人名单，未被中国政府采购（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单，符合《中华人民共和国政府采购法》规定的供应商资格条件，我方对此声明负全部法律责任。

特此声明。

供应商（单位名称及公章）：\_\_\_\_\_

法定代表人或被授权人（签字或盖章）：\_\_\_\_\_

日期：\_\_\_\_\_

说明：

1. 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。根据《财政部关于<中华人民共和国政府采购法实施条例>第十九条第一款“较大数额罚款”具体适用问题的意见》(财库(2022)3号)规定,“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。



- 6、财务状况
- 7、具有依法缴纳税收的良好记录
- 8、具有依法缴纳社会保障资金的良好记录
- 9、供应商须提供公安部第三研究所颁发的《网络安全服务认证证书（等级保护测评服务认证）》
- 10、非联合体声明（格式自拟）
- 11、磋商保证金凭证

## 六、响应方案

### 格式自拟

供应商应按照磋商文件要求响应，包括但不限于评审内容。

## 七、供应商业绩一览表

年份	用户名称	项目名称	完成时间	合同金额	完成项目质量	备注

注：以上业绩需提供合同复印件加盖公章。

供应商（单位名称及公章）：\_\_\_\_\_

法定代表人或被授权人（签字或盖章）：\_\_\_\_\_

日期：\_\_\_\_年\_\_月\_\_日

## 八、 供应商承诺书

### 陕西省政府采购供货商拒绝政府采购领域商业贿赂承诺书 I

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、在参与政府采购活动中遵纪守法、诚信经营、公平竞标。
- 2、不向采购人、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、排挤其它供货商。
- 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、代理机构政府采购评审专家或其它供货商恶意串通，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、不发生其它有悖于政府采购公开、公平、公正和诚信原则的行为。

供应商（单位名称及公章）： \_\_\_\_\_

法定代表人或被授权人（签字或盖章）： \_\_\_\_\_

日 期： \_\_\_\_年\_\_月\_\_日

## 九、供应商认为需要提供的其他资料

1. 依据竞争性磋商文件要求，供应商认为有必要说明的其他内容。
2. 其他可以证明供应商实力的文件。

## 十、中小企业声明函

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,本公司参加{采购单位名称}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:

1. {标的名称},属于{采购文件中明确的所属行业}行业;制造商为\_\_\_\_,从业人员\_\_\_\_人,营业收入为\_\_\_\_万元,资产总额为\_\_\_\_万元,属于\_\_\_\_;

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。

供应商名称(盖章): {供应商名称}

日期: {当前日期}

注:

1、供应商根据《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)规定,结合自身实际,确定对应的中小企业划型。

2、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从业人员、营业收入、资产总额均填0,根据提交投标(响应)文件时的实际情况填写企业类型。

3、供应商不属于中小企业的,无需提供此声明。

# 残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加 {采购单位名称} 单位的 {项目名称} 采购活动提供本单位制造的货物，或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

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(盖章): {供应商名称}

日期: {当前日期}

注：

1. 残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。残疾人福利性单位本身属于小型、微型企业或者监狱企业的，不重复享受政策。

2. 供应商不属于残疾人福利性单位的，不提供此声明。

## 监狱、戒毒企业的证明文件

本单位郑重声明，根据《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）的规定，本单位为符合条件的监狱、戒毒企业，且本单位参加 {采购单位名称} 单位的 {项目名称} 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），或者提供其他监狱、戒毒企业制造的货物（不包括使用非监狱、戒毒企业注册商标的货物）。

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(盖章): {供应商名称}

日期: {当前日期}

注：

1、根据《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，监狱企业参加政府采购活动时，应当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。

## 第八章 拟签订合同文本

# 西北妇女儿童医院 信息系统等保测评服务合同

甲 方：西北妇女儿童医院

乙 方：

# 西北妇女儿童医院信息系统等保测评服务合同

(合同草案条款仅供参考, 以实际签订合同为准)

西北妇女儿童医院(以下简称甲方)经政府采购, 选定\_\_\_\_\_公司(以下简称乙方)为信息系统等保测评服务成交单位。依据《中华人民共和国民法典》, 经甲、乙双方共同协商, 按下述条款和条件签署本合同。

## 一、合同内容

乙方负责按照合同和响应文件确定的信息系统等保测评服务内容及技术标准组织实施, 并按要求做好售后服务工作。

1. 系统调研: 在采购人系统相关负责人的协助下, 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。

2. 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。

3. 分析整改: 根据前述工作内容, 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, 配合采购人安全整改工作。

4. 结论报告: 根据前述工作内容, 分析当前信息系统安全保护能力是否符合相应等级的安全要求, 针对整改项进行再次测评, 提供安全等级符合性测评服务, 出具相关系统测评报告。

5. 配合验收: 整理项目过程中所有相关的过程文档, 提交采购人系统相关负责人。

## 二、商务约定

1. 服务地点: 采购人指定地点。

2. 实施工期: \_\_\_\_天。

3. 验收标准: 成交供应商提交满足技术参数要求的验收文档; 服务项目验收应在所有系统技术服务完毕, 且在服务期内无重大缺陷、问题、冲突等。

4. 合同金额: (小写) \_\_\_\_\_ (大写) \_\_\_\_\_。付款方式: 银行转账。项目验收合格后 30 个日历日一次性付清。付款前成交供应商须提供符合税法规定的全额正式发票。

5. 维保期: 本次系统测评项目需按照等级保护 2.0 测评标准执行, 维保期一年。

## 三、售后服务

为期一年的售后服务工作中，向西北妇女儿童医院提供包括应急响应、安全监测、配合检查、电话支持、安全咨询、重要活动安全保障等服务在内的安全维保服务。具体服务内容如下：

#### 1. 应急响应服务

针对本次项目，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

协助西北妇女儿童医院响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助西北妇女儿童医院准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

#### 3. 电话支持服务

每周7天/每天24小时不间断的电话支持服务，解答西北妇女儿童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。电话响应时间不大于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

为西北妇女儿童医院提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到采购人的服务请求，技术服务工程师将立即开始提供服务，帮助采购人解决信息安全相关技术问题，全面配合西北妇女儿童医院做好业务系统安全保障工作。

### 四、保密责任与赔偿承诺

1. 严格遵守采购人有关保密规定，不得泄露系统的一切敏感信息。

2. 对项目进行深入细致调研，并结合实际对测评方案进行完善。在测评过程中，投标人需保证工具测试过程中不影响系统正常运行，并保证网络拓扑、IP地址等敏感信息不被泄露。

3. 在技术服务期间，对接触到的有关采购人商业活动、技术情报和技术资料等文件进行保密

### 五、违约责任

1. 按《中华人民共和国民法典》中的相关条款执行。

2. 未按合同要求的提供产品或设备质量不能满足技术要求，甲方有权终止合同，甚至对乙方违约行为进行追究。

### 六、争议解决

本合同在履行过程中发生争议时，甲乙双方应及时协商解决，协商或调解不成时，任何一方均有权向甲方所在地人民法院起诉。

## 七、其他事项

1. 本合同一式肆份，甲方叁份，乙方壹份，具有同等法律效力，自双方法定代表人签字或盖章，并加盖公章之日起生效。

2. 竞争性磋商文件、响应文件也是合同的组成部分，具有同等法律效力，合同中未约定的以竞争性磋商文件、响应文件为准。

甲 方

乙 方

单位名称：

单位名称：

地 址：

地 址：

法定代表人：

法定代表人：

联系电话：

联系电话：

开 户 行：

开 户 行：

账 号：

账 号：

纳税人识别号：

纳税人识别号：

签订日期： 年 月 日

签订地点：西安市