

招 标 文 件

(货物类)

采购项目名称：网络安全建设提升项目

采购项目编号：**SZT2024-SN-SC-ZC-HW-0345**

陕西省肿瘤医院

陕西中技招标有限公司共同编制

2024年05月14日

第一章 投标邀请

陕西中技招标有限公司（以下简称“代理机构”）受陕西省肿瘤医院委托，拟对网络安全建设提升项目进行国内公开招标，兹邀请符合本次招标要求的供应商参加投标。

一、采购项目编号：SZT2024-SN-SC-ZC-HW-0345

二、采购项目名称：网络安全建设提升项目

三、招标项目简介

网络安全建设提升、三级等保测评服务

四、供应商参加本次政府采购活动应具备的条件

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）落实政府采购政策需满足的资格要求：

1.执行政府采购促进中小企业发展的相关政策

采购包2（三级等保测评服务）：属于专门面向中小企业采购。

（三）本项目的特定资格要求：

采购包1：

1、法定代表人授权委托书：供应商应授权合法的人员参加投标全过程，其中法定代表人直接参加投标的，须出具法定代表人身份证，并与营业执照上信息一致。法定代表人授权代表参加投标的，须出具法定代表人授权书及授权代表身份证

2、不接受联合体投标：本项目不接受联合体投标，（投标主体为单一供应商，无需提供声明函）

采购包2：

1、法定代表人授权委托书：供应商应授权合法的人员参加投标全过程，其中法定代表人直接参加投标的，须出具法定代表人身份证，并与营业执照上信息一致。法定代表人授权代表参加投标的，须出具法定代表人授权书及授权代表身份证

2、不接受联合体投标：本项目不接受联合体投标，（投标主体为单一供应商，无需提供声明函）

五、电子化采购相关事项

本项目实行电子化采购，使用的电子化交易系统为：陕西省政府采购综合管理平台的项目电子化交易系统（以下简称“项目电子化交易系统”），登录方式及地址：通过陕西省政府采购网（<http://www.ccgp-shaanxi.gov.cn/>）首页供应商用户登录陕西省政府采购综合管理平台（以下简称“政府采购平台”），进入项目电子化交易系统。供应商应当按照以下要求，参与本次电子化采购活动。

（一）供应商应当自行在陕西省政府采购网-办事指南查看相应的系统操作指南，并严格按照操作指南要求进行系统操作。在登录、使用政府采购平台前，应当按照要求完成供应商注册和信息完善，加入政府采购平台供应商库。

（二）供应商应当使用纳入陕西省政府采购综合管理平台数字证书互认范围的数字证书及签章（以下简称“互认的证书及签章”）进行系统操作。供应商使用互认的证书及签章登录政府采购平台进行的一切操作和资料传递，以及加盖电子签章确认采购过程中制作、交换的电子数据，均属于供应商真实意思表示，由供应商对其系统操作行为和电子签章确认的事项承担法律责任。

已办理互认的证书及签章的供应商，校验互认的证书及签章有效性后，即可按照系统操作要求进行身份信息绑定、权限设置和系统操作；未办理互认的证书及签章的供应商，按要求办理互认的证书及签章并校验有效性后，按照系统操作要求进行身份信息绑定、权限设置和系统操作。互认的证书及签章的办理与校验，可查看陕西省政府采购网-办事指南-CA及签章服务。

供应商应当加强互认的证书及签章日常校验和妥善保管，确保在参加采购活动期间互认的证书及签章能够正常使用；供应

商应当严格互认的证书及签章的内部授权管理，防止非授权操作。

（三）供应商应当自行准备电子化采购所需的计算机终端、软硬件及网络环境，承担因准备不足产生的不利后果。

（四）政府采购平台技术支持：

在线客服：通过陕西省政府采购网-在线客服进行咨询

技术服务电话：029-96702

CA及签章服务：通过陕西省政府采购网-办事指南-CA及签章服务进行查询

六、招标文件获取时间、方式及地址

（一）招标文件获取时间：详见采购公告

（二）在招标文件获取开始时间前，采购人或代理机构将本项目招标文件上传至项目电子化交易系统，向供应商提供。供应商通过项目电子化交易系统获取招标文件。成功获取招标文件的，供应商将收到已获取招标文件的回执函。未成功获取招标文件的供应商，不得参与本次采购活动，不得对招标文件提起质疑。

成功获取招标文件后，采购人或代理机构进行澄清或者修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或代理机构将通过项目电子化交易系统发布澄清或者修改后的招标文件，供应商应当重新获取招标文件；澄清或者修改后的招标文件发布日期距提交投标文件截止日期不足15日的，采购人或代理机构顺延提交投标文件的截止时间。供应商未重新获取招标文件或者未按照澄清或者修改后的招标文件编制投标文件进行投标的，自行承担不利后果。

注：获取的招标文件主体格式包括pdf、word两种格式版本，其中以pdf格式为准。

七、投标文件提交截止时间及开标时间、地点、方式

（一）投标文件提交截止时间及开标时间：详见采购公告

（二）投标文件提交方式、地点：供应商应当在投标文件提交截止时间前，通过项目电子化交易系统提交投标文件。成功提交的，供应商将收到已提交投标文件的回执函。

（三）本项目采取网上开标，即采购人或代理机构通过项目电子化交易系统“开标/开启大厅”组织在线开标。

八、本投标邀请在陕西省政府采购网以公告形式发布

九、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—信用融资平台（<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。

十、联系方式

采购人：陕西省肿瘤医院

地址：西安市雁塔区雁塔西路309号

邮编：710000

联系人：陈老师

联系电话：029-85276353

代理机构：陕西中技招标有限公司

地址：西安市高新区高新四路1号高科广场A1001室

邮编：710000

联系人：王馨、李文俊

联系电话：029-88364979-807

采购监督机构：财政厅政府采购管理处

联系人：柴老师、杨老师

联系电话：029-68936409、029-68936410

第二章 投标人须知

2.1 投标人须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	<p>本项目各包采购预算金额如下：</p> <p>采购包1：980,000.00元</p> <p>采购包2：340,000.00元</p> <p>投标人的采购包投标报价高于采购包采购预算的，其投标文件将按无效处理。</p>
2	最高限价（实质性要求）	<p>详见第三章。</p> <p>投标人的采购包投标报价高于最高限价的，其投标文件将按无效处理。</p>
3	评标方法	<p>采购包1：综合评分法</p> <p>采购包2：综合评分法</p> <p>（详见第五章）</p>
4	是否接受联合体	<p>采购包1：不接受</p> <p>采购包2：不接受</p> <p>如以联合体投标的，联合体各方均应当具备本招标文件要求的资格条件和能力。</p> <p>（1）联合体各方均应具有承担本项目必备的条件，如相应的人力、物力、资金等。</p> <p>（2）招标文件对投标人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。</p> <p>（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较甲级更低的乙级，则该联合体资质等级为乙级。</p>
5	落实节能、环保、无线局域网认证产品政策	<p>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。</p> <p>2.本项目采购的如有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。</p> <p>3.本项目采购的如有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，本项目采购的如有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。</p> <p>4.响应产品属于中国政府采购网公布的《无线局域网认证产品政府采购清单》且在有效期内的，按《财政部国家发展改革委信息产业部关于印发无线局域网产品政府采购实施意见的通知》（财库〔2005〕366号）要求优先采购。</p>

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）	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五章。
7	充分、公平竞争保障措施（实质性要求）	<p>核心产品允许有多个，不同供应商提供了任意一个相同品牌的核心产品，即视为提供相同品牌的供应商。</p> <p>使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。</p> <p>采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照随机抽取方式确定一个参加评标的投标人，其他投标无效。</p> <p>核心产品清单详见第三章。</p> <p>在符合性审查环节提供核心产品品牌不足3个的，视为有效投标人不足3家。</p>
8	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。投标人提交的书面说明，应当加盖投标人公章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。
9	投标保证金	<p>采购包1保证金金额：19,000.00元</p> <p>采购包2保证金金额：6,800.00元</p> <p>缴交渠道：转账、支票、汇票等（需通过实体账户、户名及开户行信息）</p> <p>开户名称：陕西中技招标有限公司（向我公司转账时，请备注清楚项目编号后四位）</p> <p>开户银行：招商银行西安分行营业部</p> <p>银行账号：1299 1681 2810 001</p>
10	标书费信息	免费获取
11	履约保证金（实质性要求）	<p>采购包1：不缴纳</p> <p>采购包2：不缴纳</p>
12	投标有效期（实质性要求）	提交投标文件的截止之日起不少于90天。

13	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 代理服务收费标准的：中标供应商应向采购代理机构缴纳招标代理服务费。招标代理服务费的收取参见国家计委颁布的《招标代理服务收费管理暂行办法》（计价格[2002]1980号）和（发改办价格[2003]857号）收费标准，按照预算金额差额定率累进法计算后计取。
14	采购结果公告	采购结果将在陕西省政府采购网予以公告。
15	中标通知书	采购结果公告发布的同时，采购人或代理机构通过项目电子化交易系统向中标供应商发出中标通知书；中标供应商通过项目电子化交易系统获取中标通知书。
16	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。
17	进口产品	不允许
18	是否组织潜在供应商现场考察	采购包1：组织现场踏勘：否 采购包2：组织现场踏勘：否
19	特殊情况	出现下列情形之一的，采购人或者采购代理机构应当中止电子化采购活动，并保留相关证明材料备查： （一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用； （二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的； （三）其他无法保证电子化交易的公平、公正和安全的情况。 出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法废标。

2.2总则

2.2.1适用范围

一、本招标文件仅适用于本次公开招标采购项目。

二、本招标文件的最终解释权由陕西省肿瘤医院和陕西中技招标有限公司享有。对招标文件中供应商参加本次政府采购活动应当具备的条件，招标项目技术、服务、商务及其他要求，评标细则及标准由陕西省肿瘤医院负责解释。除上述招标文件内容，其他内容由陕西中技招标有限公司负责解释。

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陕西省肿瘤医院。

二、“投标人”是指按照采购公告规定获取了招标文件，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陕西中技招标有限公司。

四、“网上开标”是指代理机构通过项目电子化交易系统在线完成签到、开标、唱标和记录等活动，供应商通过项目电子化交易系统在线完成投标文件解密、参与开标活动。

五、“电子评标”是指通过项目电子化交易系统在线完成资格审查小组和评审小组组建，开展资格和符合性审查、比较与评价、出具评标报告、推荐中标候选人等活动。

2.3招标文件

2.3.1招标文件的构成

一、招标文件是投标人准备投标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。招标文件用以阐明招标项目所需的资质、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。本招标文件包括以下内容：

- （一）投标邀请；
- （二）投标人须知；
- （三）招标项目技术、服务、商务及其他要求；
- （四）资格审查；
- （五）评标办法；
- （六）投标文件格式；
- （七）拟签订采购合同文本。

二、投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面做出实质性响应所产生的风险由投标人承担。

2.3.2 招标文件的澄清和修改

一、在投标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招标文件进行必要的澄清或者修改。

二、澄清或者修改的内容为招标文件的组成部分，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，投标人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。更正内容可能影响投标文件编制的，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招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

2.4 投标文件

2.4.1 投标文件的语言

一、投标人提交的投标文件以及投标人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。投标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，评标委员会将其视为无效材料。

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投标人的不利后果，由投标人承担。

2.4.2 计量单位

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3 投标货币

本次项目均以人民币报价。

2.4.4 知识产权

一、投标人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，由投标人承担所有相关责任。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、投标人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，投标人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、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法使用该知识产权的相关费用。

2.4.5 投标文件的组成

投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应。

投标文件具体内容详见第六章。

2.4.6 投标文件格式

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

2.4.7 投标报价（实质性要求）

一、投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

二、投标人每种货物及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、投标文件报价出现前后不一致的，按照招标文件第五章评标办法规定予以修正，修正后的报价经投标人通过项目电子化交易系统进行确认，并加盖投标人（法定名称）电子签章，投标人未在规定时间内确认的，其投标无效。

2.4.8 投标有效期（实质性要求）

投标有效期详见第二章“投标人须知前附表”，投标文件未明确投标有效期或者投标有效期小于“投标人须知前附表”中投标有效期要求的，其投标文件按无效处理。

2.4.9 投标文件的制作、签章和加密（实质性要求）

一、投标文件应当根据招标文件进行编制，投标人应通过陕西省政府采购网-办事指南-CA及签章服务下载投标（响应）客户端，使用客户端编制投标文件。

二、投标人应按照客户端操作要求，对应招标文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合招标文件对应项的要求的，其投标文件作无效处理。

三、投标人完成投标文件编制后，应按照招标文件第一章明确的签章要求，使用互认的证书及签章对投标文件进行电子签章和加密。

四、招标文件澄清或者修改的内容可能影响投标文件编制的，代理机构将重新发布澄清或者修改后的招标文件，投标人应重新获取澄清或者修改后的招标文件，按照澄清或者修改后的招标文件进行投标文件编制、签章和加密。

2.4.10 投标文件的提交

一、（实质性要求）投标人应当在投标文件提交截止时间前，通过项目电子化交易系统完成投标文件提交。

二、在投标文件提交截止时间后，采购人或者代理机构不再接受投标人提交投标文件。投标人应充分考虑影响投标文件提交的各种因素，确保在投标文件提交截止时间前完成提交。

2.4.11 投标文件的补充、修改、撤回（实质性要求）

投标文件提交截止时间前，投标人可以补充、修改或者撤回已成功提交的投标文件；对投标文件进行补充、修改的，应当先行撤回已提交的投标文件，补充、修改后重新提交。

供应商投标文件撤回后，视为未提交过投标文件。

2.5 开标、资格审查、评标和中标

2.5.1 开标及开标程序

一、本项目为网上开标项目。网上开标的开始时间为投标文件提交截止时间。成功提交或解密电子投标文件的投标人不足3家的，不予开标，采购人或代理机构将作废标处理。

二、开标准备工作

开标/开启前30分钟内，供应商需登录项目电子化交易系统-“供应商开标大厅”-进入开标选择对应项目包组操作签到，签到完成后等待代理机构开标/开启。

三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为60分钟；投标人应在规定的解密时间内，使用互认的证书及签章通过项目电子化采购系统进行投标文件解密。

四、开标

解密时间截止或者所有投标人投标文件均完成解密后（以发生在先的时间为准），由代理机构通过项目电子化交易系统对投标人名称、投标文件解密情况、投标报价进行展示。

开标过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。投标人对开标过程和开标记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对投标人提出的询问或者回避申请应当及时处理。

投标人完成投标文件解密后，自主决定是否参加网上在线开标，未参加的，视同认可开标结果。

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）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询投标人在投标文件提交截止时间前的信用记录并保存信用记录结果网页截图，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，以一个投标人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

详见招标文件第四章。

2.5.4 评标

详见招标文件第五章。

2.5.5 中标通知书

一、采购人或者评标委员会确认中标供应商后，代理机构在陕西省政府采购网发布中标结果公告、通过项目电子化交易系统发出中标通知书，中标供应商通过项目电子化交易系统获取中标通知书。

二、中标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中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标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、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。

二、采购人和中标人签订的采购合同不得对招标文件确定的事项以及中标人的投标文件作实质性修改。

2.6.2 合同分包和转包（实质性要求）

2.6.2.1 合同分包

一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。分包供应商履行的分包项目的品牌、规格型号及技术要求等，必须与中标的品牌、规格型号及技术要求一致。

二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于中标人的主要合同义务。

三、采购合同实行分包履行的，中标人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。

四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。

采购包1：不允许合同分包。

采购包2：不允许合同分包。

2.6.2.2 合同转包

一、严禁中标人将本项目转包。本项目所称转包，是指将本项目转给他人或者将本项目全部肢解以后以分包的名义分别转给他人的行为。

二、中标人转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3 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，可以与中标人协商签订补充合同，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。

2.6.4 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。

2.6.5 履约验收方案

采购包1：

验收依据 (1)本合同及附件文本所约定的验收标准；(2)招标文件、投标文件、澄清表（函）；(3)国家相应的标准、规范。

采购包2：

验收依据 (1)本合同及附件文本所约定的验收标准；(2)招标文件、投标文件、澄清表（函）；(3)国家相应的标准、规范。

2.6.6 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 评标活动纪律要求

采购人、代理机构应保证评标活动在严格保密的情况下进行，采购人、代理机构、投标人和评标委员会成员应当严格遵守政府采购法律法规规章制度和本项目招标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评标过程和结果。对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

2.7.2 投标人不得具有的情形（实质性要求）

一、有下列情形之一的，视为投标人串通投标：

- （一）不同投标人的投标文件由同一单位或者个人编制；
- （二）不同投标人委托同一单位或者个人办理投标事宜；
- （三）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；
- （四）不同投标人的投标文件异常一致或者投标报价呈规律性差异；
- （五）不同投标人的投标文件相互混装。

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他投标人；

四、与采购人或代理机构、其他投标人恶意串通；

五、向采购人或代理机构、评标委员会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谈判；

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。

投标人有上述情形的，按照规定追究法律责任，具备一至十一条情形之一的，其投标文件无效，或取消被确认为中标供应

商的资格或认定中标无效。

2.8 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，供应商对招标文件中采购需求的询问、质疑由 陕西中技招标有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由陕西中技招标有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 陕西中技招标有限公司 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、不影响投标文件的编制的情形）。

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详见附件一）

（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（针对招标文件提出的质疑，需提交从项目电子化交易系统获取的招标文件回执单）。

答复主体：代理机构

联系人：李工

联系电话：029-88364979-846

地址：西安市高新区高新四路1号高科广场A1001室

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详见附件二）

第三章 招标项目技术、服务、商务及其他要求

（注：当采购包的评标方法为综合评分法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

（注：当采购包的评标方法为最低评标价法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1采购项目概况

网络安全建设提升、三级等保测评服务

3.2采购内容

采购包1:

采购包预算金额（元）：980,000.00

采购包最高限价（元）：980,000.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额 （元）	计量 单位	所属行业	是否核 心产品	是否允许 进口产品	是否属于 节能产品	是否属于环境 标志产品
1	机房超融合及灾备一体扩容	1.000	980,000.00	项	软件和信息技术服务业	是	否	否	否

采购包2:

采购包预算金额（元）：340,000.00

采购包最高限价（元）：340,000.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额 （元）	计量 单位	所属行业	是否核 心产品	是否允许进 口产品	是否属于节 能产品	是否属于环境 标志产品
1	网络安全等保测评	1.000	340,000.00	项	软件和信息技术服务业	否	否	否	否

3.3技术要求

采购包1:

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

标的名称：机房超融合及灾备一体扩容

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<h2>第一部分 项目采购内容</h2> <p>一、采购项目：陕西省肿瘤医院网络安全建设提升项目</p> <p>二、数量：1套</p> <p>三、预算价：98万</p> <p>四、质保期：三年</p> <p>五、交货安装期：合同签订后60个工作日</p> <p>六、验收方式：分为两个阶段验收，第一阶段验收：设备上架调试完成后进行功能性验收。第二阶段验收：在功能性验收合格后，进行试运行阶段验收。</p> <p>七、付款方式：两个阶段验收合格后，支付合同款项100%。</p> <p>八、采购设备清单</p> <table><tr><th>序号</th><th>功能模块</th><th>简要描述</th><th>数量</th></tr><tr><td>1</td><td>灾备一体机扩容</td><td>1、扩容3块*4TB SATA硬盘并配置相应的软件； 2、并且对现有备份一体机平台进行续保。</td><td>1套</td></tr><tr><td>2</td><td>内网超融合扩容</td><td>配置1个超融合节点。</td><td>1套</td></tr><tr><td>3</td><td>外网环境改造设备</td><td>新增2台外网核心交换机（核心产品）。</td><td>1套</td></tr><tr><td>4</td><td>UPS电源</td><td>配置数据中心机房专用UPS模块化电源</td><td>1套</td></tr><tr><td>5</td><td>UPS电池</td><td>UPS电池：配置80块12V 100AH电池。</td><td>1套</td></tr><tr><td colspan="3">总计</td><td></td></tr></table> <p>九、所有新建系统需与原有系统无缝对接。</p>	序号	功能模块	简要描述	数量	1	灾备一体机扩容	1、扩容3块*4TB SATA硬盘并配置相应的软件； 2、并且对现有备份一体机平台进行续保。	1套	2	内网超融合扩容	配置1个超融合节点。	1套	3	外网环境改造设备	新增2台外网核心交换机（核心产品）。	1套	4	UPS电源	配置数据中心机房专用UPS模块化电源	1套	5	UPS电池	UPS电池：配置80块12V 100AH电池。	1套	总计			
	序号	功能模块	简要描述	数量																									
	1	灾备一体机扩容	1、扩容3块*4TB SATA硬盘并配置相应的软件； 2、并且对现有备份一体机平台进行续保。	1套																									
	2	内网超融合扩容	配置1个超融合节点。	1套																									
	3	外网环境改造设备	新增2台外网核心交换机（核心产品）。	1套																									
	4	UPS电源	配置数据中心机房专用UPS模块化电源	1套																									
	5	UPS电池	UPS电池：配置80块12V 100AH电池。	1套																									
	总计																												
		<h2>第二部分 技术参数及服务要求</h2> <h3>技术参数</h3> <h4>灾备一体机扩容</h4> <p>2020年医院采购了1台鼎甲的DK2110备份一体机设备，用于医院核心业务数据的备份。</p> <p>该设备配置为：2U机架式, 1*XEON E5-2620 v4（2.1GHz,8核16线程），2*240GB SSD,4*4 T 3.5寸 7200RPM/SATA; 2*32G DDR4 RAM, 2*1GE 电口,双千兆光纤网卡,1G阵列卡+超级电容。默认包含以下模块：备份存储服务器【V8.0】，虚拟机备份/恢复服务器【V8.0】 国外厂家虚拟化软件，传统数据库 备份/恢复代理模块【V8.0】，开源数据库备份/恢复代理模块【V8.0】，群件备份/恢复代理模块【V8.0】，Oracle Rac备份/恢复代理模块【V8.0】，Oracle Data Guard 备份/恢复代理模块【V8.0】，Oracle 双机备份/恢复代理模块【V8.0】，整机备份/裸机恢复模块（BMR）【V8.0】，服务器文件备份/恢复代理模块【V8.0】，数据库容灾演练模块【V8.0】。Oracle、MySQL数据库连续日志保护模块1个【V8.0】。</p> <p>在过去三年的使用过程中，该设备很好地承载了医院核心业务的数据备份作用，有效保障了核心业务数据的安全性。</p> <p>现有鼎甲备份一体机部署于体检中心机房，作为整个业务系统的备份设备，实现行政楼机房核心业务系统环境、VMware虚拟化、物理机、数据库、文件等数据的备份与恢复。</p>																											

文件备份：文件备份保护兼容不同操作系统平台下文件的备份、同步和恢复。

数据库备份保护：提供了数据库的热备份处理，数据备份期间不影响业务对数据库的使用，保障业务的连续性。

虚拟机保护：实现对VMware虚拟平台中的虚拟机进行备份，包括对多宿主机集群环境中的虚拟机进行备份。

备份一体机经过三年多使用，随着业务数据量的逐年增长，备份一体机的容量空间已经无法承载现有业务备份需求，需要进行容量扩容进一步满足业务增长需要。

另外基于备份系统自身安全性及勒索病毒感染风险，建议增加离线磁带库离线备份，磁带介质不受网络及文件系统病毒感染，采用物理存储机制安全级别更高，进一步保证数据安全性。

技术要求如下：

根据现有虚拟化、数据库、文件数据总体容量进行计算，并考虑后期业务增量的数据量，本次对现有备份一体机进行磁盘容量扩容，增加配置3块4TB硬盘，可用容量可≥10TB。

同时对现有备份一体机购买软硬件维保。

序号	项目	技术参数
1	DK2110备份一体机存储容量扩容	在原设备配置基础上增配3块4TB硬盘，重新RAID，RAID后的可用容量可增加10TB，扩容后设备功能与扩容前一致并能保证正常使用。
2	DK2110备份一体机软硬件维保服务	提供3年软硬件维保，维保服务的人员必须为所投产品制造商人员

内网超融合扩容

2020年医院采购了1套DELL EMC的VXRail P570超融合资源池，该超融合资源配置为：

超融合云平台VXRail P570：体系架构：采用计算与存储超融合集群软硬件一体化架构设计，整个集群可平滑、不停业务的在线扩展；集群配置：本次项目集群整体总计包含5个VXRail P570节点，机箱整体采用冗余架构设计，冗余电源、风扇模块；

由于现有超融合资源池的内存利用率比较高，为满足整体架构稳定及后续业务需求，现需要扩容一个超融合资源节点。

本次新增1个节点的超融合资源，该节点资源技术要求如下：

类型	项目	技术参数要求
产品定位	平台兼容性	本次扩充超融合系统将承载我院核心内网医疗数据中心业务，须与现有超融合平台平滑对接，保证数据的连通性和互通性（须提供与现有超融合平台对接的可行性证明及良好运行的兼容性证明）。（提供承诺函）
架构要求	集群规模	采用横向扩展架构，当前配置1个节点，集群支持≥64个节点；
	部署架构	存储虚拟化与计算虚拟化结合，不需要为分布式存储单独安装部署控制虚拟机；
	数据可靠性	节点磁盘无需做RAID，通过副本镜像方式保证数据可靠性，可选择1副本、2副本、3副本、4副本；也可以通过纠删码方式保证数据可靠性；
	计算组件	支持Intel Xeon 第三代英特尔至强可扩展处理器；每个节点配置≥2颗Intel中央处理器(≥26核, ≥2.2GHz)； 每个节点本次配置≥1024GB DDR4内存；

硬件要求	网络组件	每个节点配置≥4个万兆以太网网络端口含光模块； 每个节点配置≥1个1000Mb千兆以太网网络作为管理使用；
	存储组件	本次每个节点配置≥2块480GB SSD固态硬盘作为操作系统和虚拟化软件使用； 本次每个节点配置≥2块1.6TB高耐久性固态硬盘作为读写缓存空间； 本次每个节点配置≥10块8TB数据盘作为容量存储空间；
软件要求	服务器虚拟化	本次配置每节点≥2颗CPU服务器虚拟化软件,虚拟化平台具备虚拟机容错机制，使应用在服务器发生故障的情况下也能够持续可用。本次配置并激活虚拟化环境管理软件一套；
	存储虚拟化	本次配置每节点≥2颗CPU分布式存储虚拟化软件；
	软件定义网络	配置软件分布式交换机功能；
集群管理	系统管理	采用单一界面实现统一的超融合平台管理，超融合平台的管理和虚拟机的管理不能够采用分离的管理界面，支持Web界面方式进行管理，可在同一界面管理计算和存储资源。
	大数据分析 与人工智能 功能	针对互联互通评级中要求具备大数据分析AI功能，可以实现对现有超融合一体机系统的性能与容量的预测分析，了解当前系统的使用状况和未来的整体发展趋势，可以为整体系统的健康状况做出评估并打分；
集群保护	OracleRAC支持	超融合平台软件支持OracleRAC；
	冗余电源	配置≥2个热插拔冗余电源；
	集群双活	支持双活功能，分布式存储集群服务节点可以跨数据中心部署，能在两个集群之间做到自动的故障切换，RPO为0；
服务要求	实施服务	包含超融合平台设计，规划，实施，业务验证以及相关培训等服务；

外网环境改造

目前医院外网核心已使用11年之久，已无法满足日益增长的业务需求，而且目前现网核心仅有1台，老化的核心设备随时可能出现故障，当外网核心宕机时，全院外网及互联网业务将整体瘫痪，故医院迫切需要对外网问题进行解决。

本次项目建设外网核心交换机技术要求如下：

序号	项目	技术参数
1	设备性能	▲包转发率≥400Mpps，交换容量≥1Tbps
2	硬件描述	配置千兆以太网电口≥48个，万兆以太网光口≥12，双电源；
3	IP路由	支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6
4	虚拟化堆叠	支持虚拟化堆叠技术，可以将多台交换机组合在一起，从逻辑上组合成一台虚拟交换机。
5	配置	配置堆叠线缆≥1条，≥7个千兆单模光模块。

UPS电源主机

医院现有的UPS电源主机运行已经超出设备使用的年限，设备稳定性及可靠性均不能满足医院的业务开展要求，现需要对该UPS电源主机进行更换。

更换的UPS电源主机技术要求如下：

序号	项目	具体功能要求
1	UPS类型	在线式双变换式（含显示面板）
2	电源容量	≥120kVA
3	输入频率范围（Hz）	40Hz-70Hz；
4	输入功率因数	>0.99满载，输出功率因数为1；
5	输入电流失真 THDi:	<3%（线性载满载），<5%（非线性载满载）
6	市电与旁路	市电与电池电源转换时间：≤10ms；
7	保护功能	UPS具有交流输入过、欠压保护，输出短路保护，过温度保护，电池电压低保护等功能，并在异常时发出告警。
8	电源模块	配置3块30KVA模块，实现2+1冗余。

UPS电池

目前我院UPS电池已超出其使用年限，电池老化存在安全隐患。

UPS电池组对我院中心机房核心设备及系统的运行起着应急供电的安全保障作用，目前现用电池已超出其设计的使用年限，电池老化存在安全隐患，需更新电池组，消除安全隐患，为设备提供稳定的电力，保证设备正常运行。

技术要求如下：

序号	项目型号	描述
1	蓄电池组	12V100AH，80节
2	电池直流开关箱	直流DC750V3P250A
3	电池线缆	BVR70
4	附件	配置所需电池架、汇流箱，包含现有电池的拆除、搬运及本次采购的电池的安装。

服务要求

1、服务响应时间：从服务需求提出，即用户方开始拨打服务方热线服务电话后开始计时。现场工程师不能解决的问题须联系厂家。问题要求服务提供方承诺在服务需求提出后5分钟之内提供电话响应或在线支持服务，并于0.5小时内到达现场，2小时内恢复系统运行，4小时内彻底排除设备故障。

		<p>2、培 训：提供≥1天现场系统运行维护培训。</p> <p>3、厂商交付：提供厂商工程师实施服务。</p> <p>4、硬件巡检：提供每季度≥1次的硬件设备运行情况检查。</p> <p>5、系统巡检：提供每季度≥1次的系统健康检查。</p> <p>6、微码升级：建立硬件微码档案，制订升级方案，根据需要协助用户方实施升级工作。</p> <p>7、备份及恢复：协助医院制定完善的备份及恢复方案，并提供本项目的应急方案。</p> <p>8、保修及免费升级：提供3年厂商免费保修、现场技术支持及软件免费升级服务。</p> <p>9、辅材及配件：免费提供本项目所需辅材及配件。</p> <p>10、现有超融合平台系统升级：本次新增超融合节点扩容实施时，需要将现有的超融合平台升级到最新的软件版本。</p> <p>11、售后服务：由于目前医院灾备一体机及内网超融合承载着医院的核心业务系统及数据，对其进行相应扩容，技术复杂度大，且有一定的数据丢失及业务中断的风险，因此需要投标商提供灾备一体机及内网超融合扩容设备厂家的售后服务。</p>
--	--	---

采购包2：

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

标的名称：网络安全等保测评

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<div>项目服务内容</div> <div>项目周期：一年</div> <div>验收方式：项目验收分两个阶段。第一阶段：等保测评验收；第二阶段：安全服务验收。</div> <div>付款方式：安全服务半年后且等保测评验收合格支付50%，安全服务一年后验收合格支付50%。</div> <div>预算金额：34万元</div> <table><tr><th>序号</th><th>系统名称</th><th>系统级别</th></tr><tr><td>1</td><td>集成平台</td><td>三级</td></tr><tr><td>2</td><td>互联网医院</td><td>三级</td></tr><tr><td>3</td><td>医院核心业务系统（HIS、PACS、LIS、EMR）</td><td>三级</td></tr><tr><td>4</td><td>OA系统</td><td>二级</td></tr><tr><td>5</td><td>门户网站</td><td>二级</td></tr></table> <div>系统调研：在系统相关人员的协助下，对上述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。</div> <div>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。</div> <div>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，配合采购单位安全整改工作。</div> <div>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。</div> <div>配合验收：整理项目过程中所有相关的过程文档，提交系统相关人员。</div> <div>其他要求</div> <div>1. 测评人员要求：本项目的测评人员需具有1年或1年以上测评工作经验，项目负责人、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，须由采购单位同意。</div> <div>2. 人员配备：投标方参与此项目不少于10人，其中现场测评人员不得少于6人。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。</div> <div>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。</div>	序号	系统名称	系统级别	1	集成平台	三级	2	互联网医院	三级	3	医院核心业务系统（HIS、PACS、LIS、EMR）	三级	4	OA系统	二级	5	门户网站	二级
	序号	系统名称	系统级别																
1	集成平台	三级																	
2	互联网医院	三级																	
3	医院核心业务系统（HIS、PACS、LIS、EMR）	三级																	
4	OA系统	二级																	
5	门户网站	二级																	
	<div>项目技术标准及要求</div> <div>总体要求</div> <div>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。</div>																		

第一阶段：等级保护

网络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，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

服务商在测评过程中要求按照《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 网络安全等级保护实施指南》（GB/T25058-2019）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《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/T28449-2018）等相关的标准规范开展等级测评工作，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（三级）

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)机房地应选择在具有防震、防风 and 防雨等能力的建筑内；
		b)机房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	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	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。
		a)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

	防水防潮	b)应采取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	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	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。	
	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	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；

安全区域边界		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	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、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	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	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	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；

					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、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； 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	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	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	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	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。
					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；

			剩余信息保护	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		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		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。
	安全管理		安全管理	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		集中管控	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			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		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理制度体系。
	制定和发布		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			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。
				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；

				安全管理机构	岗位设置	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、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	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	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	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	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	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。
						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；

					外部人员访问管理	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	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	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	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	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面和隐蔽信道。
							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；

	工程实施	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	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	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	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) 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。
	服务供应商管理	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，并对其变更服务进行控制。		
	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。
	资产管理	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；
		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。
	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；

安全运维管理

	<p>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；</p> <p>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。</p>
漏洞和风险管理	<p>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；</p> <p>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。</p>
网络和系统安全管理	<p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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。</p>
恶意代码防范管理	<p>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；</p> <p>b) 应定期验证防范恶意代码攻击的技术措施的有效性。</p>
配置管理	<p>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；</p> <p>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。</p>
密码管理	<p>a) 应遵循密码相关国家标准和行业标准；</p> <p>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。</p>

			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	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	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、储存要求，对IT基础设施中断服务的应急保障要求等。

等级保护技术要求（二级）

安全层面	安全控制点	测评指标
	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。

安全物理环境	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。
安全通信网络	网络架构	a) 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；
		b) 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于段。
	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；

安全计算环境			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		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。
	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。
	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。		

安全管理人员	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。
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。
	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。

安全运维管理	服务供应商选择	<p>a)应确保服务供应商的选择符合国家的有关规定；</p> <p>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。</p>
	环境管理	<p>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；</p> <p>b)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；</p> <p>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。</p>
	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。
	介质管理	<p>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；</p> <p>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。</p>
	设备维护管理	<p>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；</p> <p>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。</p>
	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	<p>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；</p> <p>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；</p> <p>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；</p> <p>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；</p> <p>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。</p>
	恶意代码防范管理	<p>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；</p> <p>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；</p>
	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	<p>a)应遵循密码相关国家标准和行业标准；</p> <p>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。</p>

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，并进行应急预案的演练。
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。

	<p>第二阶段：渗透测试</p> <p>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。</p> <p>第三阶段：建设整改咨询及安全加固（不涉及硬件）</p> <p>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。</p> <p>医院在依据相关《信息系统安全建设整改建议》开展建设整改工作时，服务方提供建设整改过程中相关的咨询服务。</p> <p>医院对信息系统安全整改建议进行确认，并依照建议协助我方进行漏洞修复，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，然后协助我方分步实施安全整改工作。</p> <p>第四阶段：售后服务</p> <p>为期一年的售后服务工作中，服务方将向陕西省肿瘤医院提供包括应急响应、安全监测、配合检查、电话支持、安全咨询等服务在内的安全维保服务。具体服务内容如下：</p>
--	---

3.4 商务要求

3.4.1 交货时间

采购包1：
合同签订后60个工作日内

采购包2：
一年

3.4.2 交货地点

采购包1：
陕西省肿瘤医院

采购包2：
陕西省肿瘤医院

3.4.3 支付方式

采购包1：
一次付清

采购包2：
分期付款

3.4.4 支付约定

采购包1：付款条件说明：两个阶段验收合格后，支付合同款项100%。，达到付款条件起 30 日内，支付合同总金额的 100.00%。
《信息系统安全等级测评报告》；

采购包2：付款条件说明：安全服务半年后且等保测评验收合格支付50%，达到付款条件起 30 日内，支付合同总金额的 50.00%。
《信息系统整改建议书》；

4.《信息系统渗透测试报告》

采购包2：付款条件说明：安全服务一年后验收合格支付50%，达到付款条件起 30 日内，支付合同总金额的

50.00%。

3.4.5验收标准和方法

采购包1:

分为两个阶段验收，第一阶段验收：设备上架调试完成后进行功能性验收。第二阶段验收：在功能性验收合格后，进行试运行阶段验收。

采购包2:

项目验收分两个阶段。第一阶段：等保测评验收；第二阶段：安全服务验收。

3.4.6包装方式及运输

采购包1:

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

采购包2:

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

3.4.7质量保修范围和保修期

采购包1:

三年

采购包2:

一年

3.4.8违约责任与争议解决的方法

采购包1:

1、本合同履行期间，任何一方发生了不可抗力事件，以致不能履行或不能如期履行本合同，各方协商一致后，发生不可抗力事件的一方可以免除履行本合同的责任或推迟履行本合同。 2、本合同约定的不可抗力事件包括以下范围：(1)自然原因引起的事件，如地震、洪水、飓风、寒流、火山爆发、大雪、水灾、冰灾、暴风雨等；(2)社会原因引起的事件，如战争、罢工、政府禁令、封锁、疫情等； 3、发生不可抗力的一方，应于不可抗力发生后5天内以书面形式通知对方，通报不可抗力的详尽情况，提交不可抗力影响履行程度的官方证明文件。未尽告知义务的，不免除违约责任。

采购包2:

1、本合同履行期间，任何一方发生了不可抗力事件，以致不能履行或不能如期履行本合同，各方协商一致后，发生不可抗力事件的一方可以免除履行本合同的责任或推迟履行本合同。 2、本合同约定的不可抗力事件包括以下范围：(1)自然原因引起的事件，如地震、洪水、飓风、寒流、火山爆发、大雪、水灾、冰灾、暴风雨等；(2)社会原因引起的事件，如战争、罢工、政府禁令、封锁、疫情等； 3、发生不可抗力的一方，应于不可抗力发生后5天内以书面形式通知对方，通报不可抗力的详尽情况，提交不可抗力影响履行程度的官方证明文件。未尽告知义务的，不免除违约责任。

3.5其他要求

1、为顺利推进政府采购电子化交易平台试点应用工作，供应商需要在线提交所有通过电子化交易平台实施的政府采购项目的投标文件，同时，线下提交投标文件正本 壹 份、副本壹套、电子版壹 套（U盘一套标明供应商名称，随正本密封）。若系统电子投标文件与纸质投标文件不一致的，以系统电子投标文件为准。 2、定标环节采购人有权对响应文件承诺响应的内容进行复核，如有虚假响应，一经发现，取消成交资格并上报财政主管部门，列入政府采购黑名单。

第四章 资格审查

资格审查由采购人或代理机构组建的资格审查小组依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格，并出具资格审查报告。

资格审查标准及要求如下：

4.1 一般资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函
2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	资格响应表
3	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，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函
2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	资格响应表
3	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，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函

4.2 特殊资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
----	----------	---------	------

1	法定代表人授权委托书	供应商应授权合法的人员参加投标全过程，其中法定代表人直接参加投标的，须出具法定代表人身份证，并与营业执照上信息一致。法定代表人授权代表参加投标的，须出具法定代表人授权书及授权代表身份证	资格响应表
2	不接受联合体投标	本项目不接受联合体投标，（投标主体为单一供应商，无需提供声明函）	投标函

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
1	法定代表人授权委托书	供应商应授权合法的人员参加投标全过程，其中法定代表人直接参加投标的，须出具法定代表人身份证，并与营业执照上信息一致。法定代表人授权代表参加投标的，须出具法定代表人授权书及授权代表身份证	（2）商务及技术偏离表
2	不接受联合体投标	本项目不接受联合体投标，（投标主体为单一供应商，无需提供声明函）	投标函

4.3落实政府采购政策资格审查

采购包1:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
1	本采购包专门面向中小企业采购	参与的供应商（联合体）提供的货物全部由符合政策要求的中小企业制造。	中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

第五章 评标办法

5.1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》《政府采购货物和服务招标投标管理办法》《陕西省政府采购评审专家管理实施办法》等法律法规，结合采购项目特点制定本评标办法。

二、评标工作由代理机构负责组织，具体评标事务由采购人或代理机构依法组建的评标委员会负责。评标委员会由采购人代表和评审专家组成。

三、评标工作应遵循公平、公正、科学及择优的原则，并以相同的评标程序和标准对待所有的投标人。

四、本项目采取电子评标，通过项目电子化交易系统完成评标工作。评标委员会成员、采购人、代理机构和投标人应当按照本招标文件规定和项目电子化交易系统操作要求开展或者参加评标活动。

五、评标过程中的书面材料往来均通过项目电子化交易系统传递，投标人通过互认的证书及签章加盖其电子印章后生效。出现无法在线签章的特殊情况，评标委员会成员可以线下签署评标报告，由代理机构对原件扫描后以附件形式上传。

六、评标过程应当独立、保密，任何单位和个人不得非法干预评标活动。投标人非法干预评标活动的，其投标文件将作无效处理；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标活动的，将依法追究其责任。

5.2评标委员会

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、评标委员会成员应当满足并适应电子化采购评审的工作需要，使用已身份认证并具备签章功能的证书，登录项目电子化交易系统进入项目评审功能模块确认身份、签到、推荐评标委员会组长。采购人代表可以使用采购人代表专用签章确认评审意见。

三、评标委员会成员获取解密后的投标文件，开展评标活动。出现应当回避的情形时，评标委员会成员应当主动回避；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投标文件，按规定重新组建评标委员会，解封投标文件后，开展评标活动。

四、评标委员会按照招标文件规定的评标程序、评标方法和标准进行评标，并独立履行下列职责：

- （一）熟悉和理解招标文件；
- （二）审查供应商投标文件等是否满足招标文件要求，并作出评价；
- （三）根据需要要求采购组织单位对招标文件作出解释；根据需要要求供应商对投标文件有关事项作出澄清、说明或者更正；
- （四）推荐中标候选供应商，或者受采购人委托确定中标供应商；
- （五）起草评标报告并进行签署；
- （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。

5.3 评标方法

采购包1：综合评分法

采购包2：综合评分法

5.4评标程序

5.4.1熟悉和理解招标文件和停止评标

一、评标委员会正式评审前，应当对招标文件进行熟悉和理解，内容主要包括招标文件中供应商资格资质性要求、采购项

目技术、服务和商务要求、评审方法和标准以及可能涉及签订政府采购合同的内容等。

- 二、本招标文件有下列情形之一的，评标委员会应当停止评标：
- （一）招标文件的规定存在歧义、重大缺陷的；
 - （二）招标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，但是招标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中小企业发展的范围，但是招标文件未依法体现促进中小企业发展相关规定的；
 - （五）招标文件规定的评标方法是综合评分法、最低评标价法之外的评标方法，或者虽然名称为综合评分法、最低评标价法，但实际上不符合国家规定；
 - （六）招标文件将投标人的资格条件列为评分因素的；
 - （七）招标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标情形的，评标委员会应当通过项目电子化交易系统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，评标委员会不得以任何方式和理由停止评标。

出现上述应当停止评标情形的，采购组织单位应当通过项目电子化交易系统书面告知参加采购活动的供应商，并说明具体原因，同时在陕西省政府采购网公告。采购组织单位认为评标委员会不应当停止评标的，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。

5.4.2符合性审查

评标委员会依据本招标文件的实质性要求，对符合资格的投标文件进行审查，以确定其是否满足本招标文件的实质性要求。本项目符合性审查事项，必须以本招标文件的明确规定的实质性要求作为依据。

在符合性审查过程中，如果出现评标委员会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招标文件规定。

符合性审查标准见下表（按以下顺序审查）：
采购包1：

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	1.在评标过程中，评标委员会认为投标人报价低于采购预算50%或者低于其他有效投标人报价算术平均价40%，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。	开标一览表（1）开标一览表及分项报价表 标的清单

2	质保期	三年	(1) 商务及技术偏离表
3	交货安装期	合同签订后60个工作日	(1) 商务及技术偏离表 投标文件封面
4	付款方式	两个阶段验收合格后, 支付合同款项100%。	(1) 商务及技术偏离表 投标文件封面
5	投标文件有效期	90日历天	(1) 商务及技术偏离表 投标文件封面

采购包2:

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	<p>1.在评标过程中，评标委员会认为投标人报价低于采购预算50%或者低于其他有效投标人报价算术平均价40%，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。</p> <p>2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	<p>开标一览表 标的清单</p> <p>(2) 开标一览表及分项报价表</p>
2	服务周期	一年	(2) 商务及技术偏离表
3	付款方式	安全服务半年后且等保测评验收合格支付50%，安全服务一年后验收合格支付50%。	投标文件封面 (2) 商务及技术偏离表
4	投标文件有效期	90日历日	投标文件封面 (2) 商务及技术偏离表

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标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招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

二、对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当要求投标人作出必要的澄清、说明或更正，并给予投标人必要的反馈时间。投标人应当按评标委员会的要求进行澄清、说明或者更正。投标人的澄清、说明或者更正不得超出投标文件的范围或者改变投标文件的实质性内容。澄清、说明或者更正不影响投标文件的效

力，有效的澄清、说明或者更正材料是投标文件的组成部分。

三、投标人的澄清、说明或者更正需进行电子签章，应当不超出投标文件的范围、不实质性改变投标文件的内容、不影响投标人的公平竞争、不导致投标文件从不响应招标文件变为响应招标文件的条件。下列内容不得澄清：

- （一）投标人投标文件中不响应招标文件规定的技术参数指标和商务应答；
- （二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料。
- （三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

- （一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
- （二）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；
- （三）单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价；
- （四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

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

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

六、代理机构宣布评标结束前，投标人应通过项目电子化交易系统随时关注评标消息提示，及时响应评标委员会发出的澄清、说明或更正要求。投标人未能及时响应的，自行承担不利后果。

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.4.4比较与评价

评标委员会应当按照招标文件规定的评标细则及标准，对符合性检查合格的投标文件进行商务和技术评估，综合比较和评价。

5.4.5复核

评分汇总结束后，评标委员会应当进行复核，对拟推荐为中标候选供应商、报价最低、投标文件被认定为无效等进行重点复核。

评标结果汇总完成后，评标委员会拟出具评标报告前，代理机构应当组织不少于2名工作人员，在采购监督人员的监督之下，依据有关的法律制度和招标文件对评标结果进行复核，出具复核报告。

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

- （一）分值汇总计算错误的；
- （二）分项评分超出评分标准范围的；
- （三）评标委员会成员对客观评审因素评分不一致的；
- （四）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评标，重新评标改变评标结果的，书面报告本级财政部门。

5.4.6确定中标候选人名单

采购包1：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包2：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人

为排名第一的中标候选人。

5.4.7编写评标报告

评标报告是评标委员会根据全体评标成员签字的评标记录和评标结果编写的报告，其主要内容包括：

一、招标公告刊登的媒体名称、开标日期和地点；

二、投标人名单和评标委员会成员名单；

三、评审方法和标准；

四、开标记录和评审情况及说明，包括投标无效供应商名单及原因；

五、评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人

六、其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者补正，评标委员会成员的更换等；

七、报价最高的投标人为中标候选人的，评标委员会应当对其报价的合理性予以特别说明。

评标委员会成员应当在评标报告中签字或加盖电子签章确认，对评标过程和结果有不同意见的，应当在评标报告中写明并说明理由。签字但未写明不同意见或者未说明理由的，视同无意见。拒不签字或加盖电子签章又未另行说明其不同意见和理由的，视同同意评标结果。

5.5评标争议处理规则

评标委员会在评标过程中，对于符合性审查、对投标人文件作无效投标处理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，但不得违背法律法规和招标文件规定。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。持不同意见的评标委员会成员认为认定过程和结果不符合法律法规或者招标文件规定的，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

5.6评标细则及标准

一、评标委员会只对通过资格审查的投标文件，根据招标文件的要求采用相同的评标程序、评分办法及标准进行评价和比较。

二、评标委员会成员应依据招标文件规定的评分标准和方法独立评审。

5.6.1评分办法

若采用综合评分法的，由评标委员会各成员对通过资格检查和符合性审查的投标人的投标文件进行独立评审。 投标报价得分=（评标基准价 / 投标报价）×100

评标总得分=F1×A1+F2×A2+.....+Fn×An

F1、F2.....Fn分别为各项评审因素的得分；

A1、A2、.....An 分别为各项评审因素所占的权重（A1+A2+.....+An=1）。

评标过程中，不得去掉报价中的最高报价和最低报价。

因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

5.6.2评分标准

采购包1：

评审因素		评审标准			
分值构成		详细评审70.00分 报价得分30.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	产品选型	<p>供应商提供投标产品的产品选型方案，至少包含：1、产品的稳定性；2、数据的开放性和兼容性；3、投标产品配置齐全等。方案各项内容全面详细、阐述条理清晰、技术先进、功能配置合理，能有效保障本项目实施得6分，每有一项缺项扣2分，每有一处内容存在缺陷，扣1分，扣完为止。备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	6.00	主观	<p>（1）服务方案及供应商认为有必要提供的其他内容</p>
	技术指标和配置	<p>根据招标文件要求认真审核投标文件中技术参数响应和提供的佐证材料。投标产品的基本功能、产品技术参数和配置完全满足或优于招标文件要求的，得满分12分；其中“▲”标注参数为重要技术参数。每负偏离一项扣2分，直至本项扣完为止；非“▲”参数为一般参数，每负偏离一项扣1分，直至本项扣完为止。注：带“▲”参数需提供佐证材料并加盖公章。（佐证材料不限于：检测报告、功能说明书、功能截图等内容，证明材料需加盖公章，未提供相关证明材料不得分。）</p>	12.00	客观	<p>（1）服务方案及供应商认为有必要提供的其他内容</p> <p>（1）商务及技术偏离表</p>

超融合技术方案	<p>供应商提供针对本项目的超融合技术方案，方案针对本项目实施提出：</p> <p>1、提供新增超融合节点与医院现有内网超融合平台的对接方案、架构优化方案；</p> <p>2、数据迁移、应急演练方案。方案各项内容全面详细、阐述条理清晰详尽、符合本项目采购需求、能有效保障本项目实施的得6分，每有一个缺项扣3分，每有一处内容存在缺陷，扣1分，扣完为止。说明：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	6.00	主观	(1) 服务方案及供应商认为有必要提供的其他内容
备份一体机扩容方案	<p>供应商提供针对本项目的备份一体机扩容方案，方案针对本项目实施提出：</p> <p>1、对目前通用的各类操作系统环境提供具体可行的兼容方案；</p> <p>2、对系统迁移、数据库迁移等有具体可行的解决方案；</p> <p>3、有切实可行的信息安全防护体系等。方案各项内容全面详细、阐述条理清晰详尽、符合本项目采购需求、能有效保障本项目实施的得6分，每有一个缺项扣2分，每有一处内容存在缺陷，扣1分，扣完为止。说明：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	6.00	主观	(1) 服务方案及供应商认为有必要提供的其他内容
质量控制	<p>供应商提供质量控制措施。</p> <p>1、质量控制方法和措施、流程，控制重点思路清晰明确得3分；</p> <p>2、质量控制措施内容无针对性，有缺陷得1分；</p> <p>3、未提供不得分。</p>	3.00	主观	(1) 服务方案及供应商认为有必要提供的其他内容

项目负责人简历表	拟派项目负责人具有相关行业 2 年以上从业经验，提供项目负责人简历表。需对从业经验有描述内容，描述内容不符或无描述内容此项不得分。	1.00	客观	(1) 人员表
项目负责人	拟派项目负责人具备计算机或软件能力相关技术证书，提供 1 个中级工程师证书得 1 分，提供 1 个高级工程师证书得 2 分，满分 2 分。（多个中级工程师证书仅计 1 分）须同时提供供应商为其缴纳的社保缴费证明，未提供不得分。	2.00	客观	(1) 人员表
团队人员	提供团队人员（除项目负责人外）计算机或软件能力相关技术证书，提供 1 个中级工程师证书得 0.5 分，提供 1 个高级工程师证书得 1 分。 备注：相同人员不重复计分，满分 3 分。须同时提供供应商为其缴纳的社保缴费证明，未提供不得分。	3.00	客观	(1) 人员表
团队配备方案	供应商结合项目实际情况提供针对本项目的团队配备方案，内容至少包括： 1 、人员配备齐全、结构合理，安排计划及分配工作情况表； 2 、人员配备能力完备等； 3 、内控制度：具有管理组织机构、问责机制、监督机制、自查制度。内容全面详细、阐述条理清晰，能有效保障本项目实施得 6 分，每有一项缺项扣 2 分，每有一处内容存在缺陷，扣 1 分，扣完为止。备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任何一种情形。	6.00	主观	(1) 服务方案及供应商认为有必要提供的其他内容

售后服务方案	提供针对本项目提供售后服务方案，内容至少包含： 1. 售后时间的及时性； 2. 故障服务管理方案； 3. 硬件巡检、系统巡检措施。方案内容全面详细、阐述条理清晰、配置合理，能有效保障本项目实施得 6分 ，每有一项缺项扣 2分 ，每有一处内容存在缺陷，扣 1分 ，扣完为止。说明：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。	6.00	主观	(1) 服务方案及供应商认为有必要提供的其他内容
培训服务方案	供应商提供针对本项目的培训服务方案，内容至少包括： 1. 人员培训； 2. 培训内容； 3. 、提供 ≥1 天现场系统运行维护培训方案。方案内容全面详细、阐述条理清晰、配置合理，能有效保障本项目实施得 6分 ，每有一项缺项扣 2分 ，每有一处内容存在缺陷，扣 1分 ，扣完为止。备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。	6.00	主观	(1) 服务方案及供应商认为有必要提供的其他内容
合理化建议	供应商提供针对本项目的重难点分析及合理化建议。 1. 、内容合理、阐述条理清晰得 3分 ； 2. 、内容未贴合项目实际情况进行论述得 1分 ； 3. 、未提供不得分。	3.00	主观	(1) 服务方案及供应商认为有必要提供的其他内容
业绩	提供 2021年1月1日 以来类似项目合同，每提供一个得 2分 ，满分 10分 。以合同（至少包含合同首页、金额、签字盖章页等）签订日期为准，提供合同复印件加盖公章。	10.00	客观	业绩一览表

价格分	价格分	满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）×投标报价总分	30.00	客观	开标一览表 标的清单
-----	-----	---	-------	----	---------------

价格扣除

序号	情形	适用对象	比例	说明	关联格式
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件

采购包2:

评审因素		评审标准			
分值构成		详细评审100.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	项目理解	<p>供应商提供针对本项目的整体理解方案。 1、充分理解本项目服务需求对项目现状和整体认知的理解，思路清晰明确得6分； 2、理解方案完整合理，但还有可以优化空间得3分； 3、方案内容有缺陷、表述前后不一致、套用其他项目方案或与项目需求匹配性差得1分； 4、未提供不得分。</p>	6.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容
	测评方案	<p>供应商提供项目测评方案。 方案内容至少包含:1、测评流程； 2、测评指标； 3、测评方法； 4、系统安全层面测评全面等内容。 方案所涉及的测评方案周密健全完善，项目工作成果科学严谨，项目服务全流程具体可行，运作流程流畅，能有效保障本项目实施得8分，每有一项缺项扣2分，每有一处内容存在缺陷，扣1分，扣完为止。 备注:缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致，套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	8.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容
	渗透测试方案	<p>供应商提供项目渗透测试方案。 方案内容至少包含:1、渗透测试流程； 2、渗透测试技术； 3、渗透测试风险控制等内容。 方案所涉及的渗透测试方案周密健全完善，项目工作成果科学严谨，项目服务全流程具体可行，运作流程流畅，能有效保障本项目实施得9分，每有一项缺项扣3分，每有一处内容存在缺陷，扣1分，扣完为止。 备注:缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致，套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	9.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容

建设整改咨询及安全加固方案	<p>供应商提供针对本项目建设整改咨询及安全加固方案，内容至少包含：</p> <p>1、提供建设整改过程中相关的咨询服务；</p> <p>2、协助采购人进行安全加固，制定安全整改方案和计划，实施安全整改工作。方案内容全面详细、阐述条理清晰、配置合理，能有效保障本项目实施得6分，每有一项缺项扣3分，每有一处内容存在缺陷，扣1分，扣完为止。</p> <p>备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	6.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容
进度要求	<p>供应商提供针对本项目不同阶段工作的进度要求，提供进度计划，计划包含：</p> <p>1、时间节点控制；</p> <p>2、资源配置计划；</p> <p>3、重点环节进度控制等等。切合项目具体情况，能有效保障本项目实施得6分，每有一项缺项扣2分，每有一处内容存在缺陷，扣1分，扣完为止。备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	6.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容

详细评审

拟投入人员方案	供应商提供针对本项目拟投入的工作组成员的情况说明及证明材料。 方案内容至少包含:1、拟投入本项目所有测评人员需具有1年或1年以上测评工作经验（提供承诺函）； 2、拟投入的工作组成员不少于10人，其中现场测评人员不得少于6人；3、工作组成员管理组织架构，人员分工和工作职责划分、业务管理流程等内容。方案所涉及的拟投入的工作组成员管理组织架构清晰，人员分工和工作职责划分明确、业务管理流程详细，能有效保障本项目实施得6分，每有一项缺项扣2分，每有一处内容存在缺陷，扣1分，扣完为止。备注:缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致，套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。	6.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容
实施保障	供应商需具备网络安全等级保护测评与检测的能力，具备《网络安全等级保护测评与检测评估机构服务认证证书》得2分，未提供不得分。	2.00	客观	(2) 服务方案及供应商认为有必要提供的其他内容
项目负责人	拟承担本项目的项目负责人具备高级测评师证书、注册信息安全专业人员（CISP）证书提供1份得1分，满分2分，未提供不得分。	2.00	客观	(2) 人员表
拟派项目经理	拟派项目经理具备高级测评师证书、信息安全保障人员（CISAW）风险管理方向认证证书提供1份得1分，满分2分，未提供不得分。（相同人员证书不重复计分）	2.00	客观	(2) 人员表
拟投入本项目渗透测试工程师	拟投入本项目渗透测试工程师应具备渗透相关专业资质证书，每提供一个得1分，满分2分。（相同人员证书不重复计分）	2.00	客观	(2) 人员表

拟派项目质量负责人	拟派项目质量负责人具备中级或以上测评师证书、CIIP-A证书提供1份得1分，满分2分，未提供不得分。（相同人员证书不重复计分）	2.00	客观	（2）人员表
项目组其他成员	项目组其他成员（不包含项目负责人、项目经理、质量负责人及渗透测试工程师），具备中级及以上专业技术人员资质证书，提供1个得0.5分，满分3分。（相同人员证书不重复计分）	3.00	客观	（2）人员表
保密方案	供应商提供针对本项目的保密方案，方案至少包含：1、保密管理制度；2、对数据和信息安全保密；3、其他保密措施等。切合项目具体情况，提出责任明确，服务定位，能有效保障本项目实施得6分，每有一项缺项扣2分，每有一处内容存在缺陷，扣1分，扣完为止。备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。	6.00	主观	（2）服务方案及供应商认为有必要提供的其他内容
应急方案	供应商提供针对本项目的应急方案，方案至少包含：1、对后期服务的保证措施、能够处理各类紧急事项的措施；2、保证项目实施，能够保证在规定的时间内解决问题；3、提供常规应急响应及灾难恢复服务。切合项目具体情况，提出责任明确，服务定位，能有效保障本项目实施得6分，每有一项缺项扣2分，每有一处内容存在缺陷，扣1分，扣完为止。备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。	6.00	主观	（2）服务方案及供应商认为有必要提供的其他内容

	售后服务方案	<p>供应商提供针对本项目的售后服务方案，方案至少包含：1、提供电话支持服务，并及时提出解决问题的建议和操作方法；2、配合检查服务、安全咨询服务。切合项目具体情况，提出责任明确，服务定位，能有效保障本项目实施得6分，每有一项缺项扣3分，每有一处内容存在缺陷，扣1分，扣完为止。</p> <p>备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。</p>	6.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容
	合理化建议	<p>供应商针对本项目有明确的合理化建议。1、合理化建议内容合理，针对性强、明确、全面得3分；2、合理化建议内容不完善、表述前后不一致、套用其他项目内容等得1分；3、未提供不得分。</p>	3.00	主观	(2) 服务方案及供应商认为有必要提供的其他内容
	业绩	<p>提供2021年1月1日以来同类项目业绩，每提供一个得2分，满分10分。以合同（至少包含合同首页、金额、签字盖章页等）签订日期为准，提供合同复印件加盖公章。</p>	10.00	客观	业绩一览表
	价格	<p>满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：投标报价得分 = (评标基准价/投标报价) × 15</p>	15.00	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
无					

说明：

- 1、评分的取值按四舍五入法，保留小数点后两位；
- 2、评分标准中要求提供复印件的证明材料须清晰可辨。

若采用最低评标价法的，投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人。采用最低评标价法评标时，除了算术修正和落实政府采购政策需进行的价格扣除外，不能对投标人的投标价格进行任何调整。

5.7 废标

本次政府采购活动中，出现下列情形之一的，予以废标：

- 一、符合专业条件的投标人或者对招标文件作实质响应的投标人不足三家的；
- 二、出现影响采购公正的违法、违规行为的；
- 三、投标人的报价均超过了采购预算，采购人不能支付的；
- 四、因重大变故，采购任务取消的；

废标后，代理机构将在“陕西省政府采购网”上公告。对于评标过程中废标的采购项目，评标委员会应当对招标文件是否存在不合理条款进行论证，并出具书面论证意见。

5.8定标

5.8.1 定标原则

采购人在评标报告确定的中标候选人名单中按顺序确定**1**名中标人。中标候选人并列的，由采购人采取随机抽取的方式确定中标人。

5.8.2定标程序

一、评标委员会在项目电子化交易系统中编制评标情况，生成评标报告。

二、代理机构在评标结束之日起**2**个工作日内将评标报告送采购人。

三、采购人在收到评标报告后**5**个工作日内，按照评标报告中推荐的中标候选人顺序确定中标供应商。逾期未确认的，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标供应商。

四、根据确定的中标供应商，代理机构在陕西省政府采购网上发布中标结果公告，通过项目电子化交易系统向中标供应商发出中标通知书。

5.9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。

5.10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，不得修改或细化采购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，除因配合答复处理供应商的询问、质疑和投诉等事项外，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。

第六章 投标文件格式

采购包1:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：开标一览表

详见附件：标的清单

详见附件：（1）服务方案及供应商认为有必要提供的其他内容

详见附件：（1）开标一览表及分项报价表

详见附件：（1）人员表

详见附件：（1）商务及技术偏离表

详见附件：业绩一览表

详见附件：资格响应表

采购包2:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：开标一览表

详见附件：标的清单

详见附件：（2）开标一览表及分项报价表

详见附件：（2）商务及技术偏离表

详见附件：业绩一览表

详见附件：资格响应表

详见附件：（2）人员表

详见附件：（2）服务方案及供应商认为有必要提供的其他内容

第七章 拟签订合同文本

详见附件：合同格式与主要条款.docx

