陕西中技招标有限公司
SHAANXI ZHONGJI TENDERING CO.,LTD

# 西安市中医医院等级保护测评项目

# 竞争性磋商文件

项目编号： SZT2025-SN-XC-ZC-FW-0717

采购代理机构：陕西中技招标有限公司

日　　期：二零二五年九月

# 目　录

**第一部分　竞争性磋商公告 ..... 3**

**第二部分　磋商须知前附表 ..... 6**

**第三部分　磋商须知 ..... 11**

A 总则 ..... 11
1. 适用范围 ..... 11
2. 定义 ..... 11
3. 合格的供应商 ..... 11
4. 合格服务 ..... 11
5. 费用 ..... 12
B 磋商文件说明 ..... 12
6．磋商文件的构成 ..... 12
7．磋商文件的澄清 ..... 12
8．磋商文件的修改 ..... 12
C．响应文件的编写 ..... 13
9．响应文件编制的原则 ..... 13
10．磋商语言 ..... 13
11．计量单位 ..... 13
12．响应文件的组成 ..... 13
13．响应文件格式 ..... 13
14．磋商报价 ..... 14
15．磋商货币 ..... 14
16．证明供应商资格的证明文件 ..... 14
17．证明的合格性和符合磋商文件规定的文件 ..... 14
18．磋商保证金 ..... 14
19．磋商有效期 ..... 14
20．响应文件的签署及格式 ..... 14
D．响应文件的递交 ..... 15
21．响应文件的数量、包装和标记 ..... 15
22．磋商截止时间 ..... 15
23．响应文件的修改与撤回 ..... 15
E．磋商 ..... 16
24．磋商 ..... 16
25．磋商小组 ..... 16
26．响应文件的审核 ..... 17
27．响应文件的澄清 ..... 18
28．响应文件的比较和评价 ..... 18
29．评审原则及主要方法 ..... 19
30．与采购人、采购代理机构和磋商小组接触 ..... 24
F．授予合同 ..... 24
31．定标及合同授予 ..... 24
32．接受和拒绝任何或所有磋商的权力 ..... 24
33．履约保证金 ..... 24
34．腐败和欺诈行为 ..... 25
35. 招标代理服务费 ..... 25

**第四部分　合同一般条款 ..... 26**

**第五部分　附件--响应文件格式 ..... 31**

响应文件目录 ..... 32
附件 1　磋商响应函 ..... 33

附件 2 磋商报价表 ..... 34
附件 3 分项报价表 ..... 35
附件 4 商务偏离表 ..... 36
附件 5 服务方案 ..... 37
附件 6 服务承诺 ..... 38
附件 7 供应商为本项目提供的资格证明文件 ..... 39
附件 8 法定代表人授权委托书 ..... 48
附件 9 本项目不接受联合体磋商 ..... 50
附件 10 供应商参加政府采购活动承诺书 ..... 51
附件 11 供应商诚信承诺书 ..... 52
附件 12 关于非西安市中医医院职工及其亲属投资开办或控股的企业书面声明 ..... 53
附件 13 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 ..... 54
附件 14 其他相关资料 ..... 55
**第六部分 采购内容及要求 ..... 56**

# 第一部分　竞争性磋商公告

西安市中医医院等级保护测评项目竞争性磋商公告

项目概况

等级保护测评项目采购项目的潜在供应商应在西安市高新区高新四路 1 号高科广场 A1001 室获取采购文件，并于 2025 年 09 月 25 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：SZT2025-SN-XC-ZC-FW-0717

项目名称：等级保护测评项目

采购方式：竞争性磋商

预算金额：250,000.00 元

采购需求：

合同包 1(等级保护测评项目)：

合同包预算金额：250,000.00 元

合同包最高限价：250,000.00 元

| 品目号 | 品目名称 | 采购标的 | 数量（单位） | 技术规格、参数及要求 | 品目预算(元) |
|---|---|---|---|---|---|
| 1-1 | 测试评估认证服务 | 等级保护测评 | 1(项) | 详见采购文件 | 250,000.00 |

本合同包不接受联合体投标

合同履行期限：自入场后 40 个日历日完成现场测评工作，不包含整改时间。

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(等级保护测评项目)落实政府采购政策需满足的资格要求如下：

本项目为专门面向中小企业采购的采购项目。

3.本项目的特定资格要求：

合同包 1(等级保护测评项目)特定资格要求如下：

1.供应商提供有效的《网络安全服务认证证书等级保护测评服务认证》。

三、获取采购文件

时间：2025 年 09 月 12 日 至 2025 年 09 月 18 日，每天上午 08:30:00 至 12:00:00，下午 13:00:00 至 17:30:00 （北京时间）

途径：西安市高新区高新四路 1 号高科广场 A1001 室

方式：现场获取

售价： 0 元

四、响应文件提交

截止时间： 2025 年 09 月 25 日 14 时 30 分 00 秒 （北京时间）

地点：西安市高新区高新四路 1 号高科广场 A 座 5 楼 0503 第 八 会议室

五、开启

时间： 2025 年 09 月 25 日 14 时 30 分 00 秒 （北京时间）

地点：西安市高新区高新四路 1 号高科广场 A 座 5 楼 0503 第 八 会议室

六、公告期限

自本公告发布之日起 3 个工作日。

七、其他补充事宜

（一）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。

（二）落实政府采购政策：

1.财政部、工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知-财库〔2020〕46 号;2.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;3.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;4.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；5.财政部 发展改革委 生态环境部 国家市场监督管理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；6.财政部生态环境部关于印发环境标志产品政府采购品目清单的通知-财库〔2019〕18 号；7.财政部发展改革委关于印发节能产品政府采购品目清单的通知 -财库〔2019〕19 号；8.财政部 农业农村部 国家乡村振兴局关于运用政府采购政策支持乡村产业振兴的通知-财库〔2021〕19 号；9.财政部、农业农村部、国家乡村振兴局、中华全国

供销合作总社关于印发《关于深入开展政府采购脱贫地区农副产品工作推进乡村产业振兴的实施意见》的通知-财库〔2021〕20 号；10.陕西省财政厅关于落实政府采购支持中小企业政策有关事项的通知-陕财办采函〔2022〕10 号；11.陕西省财政厅关于进一步加强政府绿色采购有关问题的通知-陕财办采〔2021〕29 号；12.陕西省财政厅关于印发《陕西省中小企业政府采购信用融资办法》-陕财办采〔2018〕23 号；13.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；14.陕西省财政厅 中国人民银行西安分行关于深入推进政府采购信用融资业务的通知-陕财办采〔2023〕5 号；15.西安市财政局关于促进政府采购公平竞争优化营商环境的通知-市财函〔2021〕431 号；16.西安市财政局关于贯彻落实<西安市政府采购信用担保及信用融资工作实施方案（试行）>有关事宜的通知-市财发〔2015〕4 号

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：西安市中医医院

地址：凤城八路 69 号

联系方式：029-89626819

2.采购代理机构信息

名称：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 A 座 1001 室

联系方式：029-87304326

3.项目联系方式

项目联系人：李毓菲、杨艳、单博、李娜、史肖霞

电话：029-87304326-872

# 第二部分　磋商须知前附表

| 序号 | 条款号 | 编列内容 |
|---|---|---|
| 1 | 磋商公告 | 项目名称：西安市中医医院等级保护测评项目<br>项目编号： SZT2025-SN-XC-ZC-FW-0717 |
| 2 | 资金来源 | 已落实 |
| 3 | 磋商公告 | 采购人：西安市中医医院<br>采购代理机构：陕西中技招标有限公司 |
| 4 | 磋商保证金 | 根据《西安市财政局关于促进政府采购公平竞争优化营商环境》（市财函【2020】617号文），本次项目无需缴纳磋商保证金。 |
| 5 | 磋商有效期 | 响应文件从磋商之日起，有效期为90日历天。 |
| 6 | 响应文件份数及格式 | 供应商应制作响应文件，提交壹套正本“响应文件”、贰套副本“响应文件”（响应文件不退还）及电子版文件（电子文件需提供word版本及签字盖章后PDF两种格式，单独密封）一份。若正本和副本不符，以正本为准。响应文件应编制目录及页码。供应商应在响应文件封面及响应文件密封文件袋正面注明“正本”、“副本”、“电子版”。供应商应在响应文件封面及密封文件袋表面加盖单位公章。以保证响应文件密封性完整。 |
| 7 | 响应文件的包装和标记 | 响应文件牢固装订成册，不可插页抽页。是指用适当的办法以保证响应文件不至于散开或用简单办法不能将任何一页在没有任何损坏的情况下取出或插入。 |
| 8 | 磋商报价 | 磋商报价中应充分考虑本服务的各项内容，包括完成项目所发生的服务全部税费以及合同包含的所有风险、责任等所有费用，投标人漏报或不报，采购人或采购代理 |

| 序号 | 条款号 | 编列内容 |
| --- | --- | --- |
| | | 机构将视为有关费用已包括在投标报价中而不予支付。 |
| 9 | 服务期限 | 自入场后40个日历日完成现场测评工作,不包含整改时间。 |
| 10 | 服务地点 | 甲方指定地点 |
| 11 | 付款方式 | 银行转账，无预付款，完成交付内容后经由成交供应商提出验收申请，经采购人验收合格并取得签署的书面验收报告（递交备案证书、测评报告）后，采购人向成交供应商支付合同总金额的95%，项目通过验收后满1年支付合同总金额的5%。本项目报价一次性包死，医院不承担其他任何费用。 |
| 12 | 踏勘 | 不踏勘 |
| 13 | 合同签订 | 成交供应商与采购人签订合同。 |
| 14 | 供应商投诉质疑 | 供应商提出质疑应符合中华人民共和国财政部令第94号《政府采购质疑和投诉办法》的规定：<br>1、提出质疑的供应商应当是参与所质疑项目采购活动的供应商。<br>2、供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、采购代理机构提出质疑，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。<br>供应商应知其权益受到损害之日，是指：<br>（1）对可以质疑的采购文件提出质疑的，为收到采购文件之日；<br>（2）对采购过程提出质疑的，为各采购程序环节结束之日； |

| 序号 | 条款号 | 编列内容 |
| --- | --- | --- |
| | | （3）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。<br>3、供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括：<br>3.1 供应商的姓名或者名称、地址、邮编、联系人及联系电话；<br>3.2 质疑项目的名称、编号；<br>3.3 具体、明确的质疑事项和与质疑事项相关的请求；<br>3.4 事实依据；<br>3.5 必要的法律依据；<br>3.6 提出质疑的日期。<br>质疑函应采用财政部颁布的《政府采购供应商质疑函范本》。<br>供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。<br>4、供应商可以委托代理人进行质疑。其授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。<br>5、有下列情形之一的，属于无效质疑，采购代理机构和采购人不予受理：<br>5.1 质疑供应商不是参与所质疑项目采购活动的供应商；<br>5.2 未在法定质疑期内发出质疑的；<br>5.3 质疑未以书面形式提出；<br>5.4 质疑函没有合法有效的签字、盖章或授权的； |

| 序号 | 条款号 | 编列内容 |
| --- | --- | --- |
| | | 5.5 以非法手段取得证据、材料的；<br>5.6 质疑答复后，同一质疑人就同一事项再次提出质疑的；<br>5.7 不符合法律、法规、规章和政府采购监管机构规定的其他条件的。<br>6、质疑答复<br>采购人、采购代理机构在收到质疑函后七个工作日内做出答复。<br>7、质疑接收方式：供应商以书面形式将质疑函原件和必要的证明材料送至接收部门，法定代表人、主要负责人、自然人提交质疑函须提交其身份证复印件，代理人提交质疑函须提交授权委托书及授权人和被授权人身份证复印件。质疑函应采用财政部颁发的《政府采购供应商质疑函范本》。<br>接收部门：企业管理部<br>接 收 人：戴经理<br>联系电话：029-87304326-856<br>地 址：西安市高新区高新四路 1 号高科广场 A 座 1001 室<br>8、投诉人在全国范围 12 个月内三次以上投诉查无实据的，由财政部门列入不良行为记录名单。<br>9、投诉人有下列行为之一的，属于虚假、恶意投诉，由财政部门列入不良行为记录名单，禁止其 1 至 3 年内参加政府采购活动：<br>（一）捏造事实；<br>（二）提供虚假材料；<br>（三）以非法手段取得证明材料。证据来源的合法性存在明显疑问，投诉人无法证明其取得方式合法的，视为 |

| 序号 | 条款号 | 编列内容 |
| --- | --- | --- |
| | | 以非法手段取得证明材料。 |
| 15 | 信用信息 | 供应商通过“信用中国”网站(www.creditchina.gov.cn)和中国政府采购网(www.ccgp.gov.cn) 查询相关主体信用记录，采购人、采购代理机构现场对供应商信用信息进行查询。对被列入失信被执行人、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，采购代理机构将拒绝其参与政府采购活动。处罚期限届满的除外。） |
| 16 | 供应商失信行为 | 供应商有《陕西省政府采购领域供应商违法失信“黑名单”信息共享和联合惩戒实施办法》第四条规定的情形之一的，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任，同时纳入黑名单系统。 |

备注：磋商文件其他部分内容与本须知前附表内容不一致的，以本须知前附表内容为准。

# 第三部分　磋商须知

## A 总则

### 1. 适用范围

1.1 本磋商文件仅适用于本磋商公告中所叙述项目的服务采购。

1.2 本次采购项目中采购人，采购代理机构、供应商、磋商小组的相关行为按照《政府采购竞争性磋商采购方式管理暂行办法》、规章及采购项目所在地有关法规、规章的约束，其权利受到上述法律法规的保护。

1.3 磋商文件解释权归采购代理机构所有。

### 2. 定义

2.1 “采购人”系指西安市中医医院。

“采购代理机构”系指陕西中技招标有限公司。

2.2 “供应商”系指响应采购人要求提交响应文件的响应单位。

2.3 “服务”系指磋商文件规定供应商须承担相关工作。

### 3. 合格的供应商

3.1 供应商应符合《政府采购竞争性磋商采购方式管理暂行办法》及相关条款及有关的中国法律和法规。

3.2 凡符合供应商资格要求且有能力提供采购服务的供应商均可投标。

3.3 供应商必须在磋商公告载明的地点购买磋商文件并登记备案，未经购买磋商文件并登记备案的潜在供应商均无资格参加本次磋商。

3.4 只有在法律上和财务上独立，合法运作，并独立于采购代理机构和采购人的供货人才能参加磋商。

3.5 供应商之间如果存在下列情形之一的，不得同时参加本项目磋商：

3.5.1 法定代表人为同一个人的两个及两个以上法人公司；

3.5.2 母公司、全资子公司及其控股公司；

3.5.3 参加投标的其他组织之间存在特殊的利害关系的；

3.5.4 法律和行政法规规定的其他情形。

### 4. 合格服务

4.1 合同中提供的所有有关的服务，均应来自国家有关政府采购规定的服务的合格来源，本合同的支付也仅限于这些服务。

**5. 费用**

5.1 供应商应承担所有与编写和提交响应文件有关的费用，无论磋商过程中的做法和结果如何，采购人和采购代理机构在任何情况下均无义务和责任承担这些费用。

# B 磋商文件说明

**6．磋商文件的构成**

6.1 磋商文件用以阐明所需提供的服务、采购、磋商程序和合同条件。磋商文件包括：

6.1.1 竞争性磋商公告；

6.1.2 磋商须知前附表；

6.1.3 磋商须知；

6.1.4 合同一般条款；

6.1.5 附件—响应文件格式；

6.1.6 采购内容及要求。

6.2 供应商应认真阅读磋商文件中所有的事项、格式条款和规范要求等。供应商没有对磋商文件全面做出实质性响应是供应商的风险。

**7．磋商文件的澄清**

7.1 任何要求对磋商文件澄清的供应商，应在购买磋商文件后以书面形式通知采购代理机构。采购代理机构将以书面形式予以答复，涉及变更或修正内容在采购发布媒体上发布更正公告，并以书面形式通知所有磋商文件收受人，且作为磋商文件的组成部分。

**8．磋商文件的修改**

8.1 在磋商文件要求提交响应文件截止时间前，无论出于何种原因，采购人可主动地或在解答供应商要求澄清的问题时对磋商文件进行修改。

8.2 澄清或者修改磋商文件可能影响响应文件编制的，在提交首次响应文件截止之日3个工作日前，以书面形式通知所有接收磋商文件的供应商，不足3个工作日的，顺延提交首次响应文件截止时间。

8.3 为使供应商在准备响应文件时，有充分的时间对磋商文件的修改进行研究考虑，采购人可自行决定，酌情推迟磋商截止日期，并以书面形式通知所有已购买磋商文件的供应商。

8.4 磋商文件的修改书将构成磋商文件的一部分，对采购人和供应商都具有约束力。

## C．响应文件的编写

### 9．响应文件编制的原则

9.1 供应商应在认真阅读磋商文件所有内容的基础上，按照磋商文件的要求编制完整的响应文件。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。

9.2 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。

9.3 响应文件须对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。

### 10．磋商语言

10.1 由供应商编写的响应文件和往来信件应以中文书写。

### 11．计量单位

11.1 除在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。

### 12．响应文件的组成

12.1 所有服务方案只允许供应商有一个磋商方案，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/或报价的，其磋商将被拒绝。

12.2 供应商编写的响应文件应包括下列部分：

12.2.1 磋商响应函、磋商报价表以及所有附件内容。

12.2.2 按照供应商须知出具的供应商资格证明文件。

12.2.3 按照供应商须知出具的报价符合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。

12.2.4 磋商文件要求供应商提供的其他内容。

### 13．响应文件格式

13.1 供应商应按磋商文件中提供的响应文件格式填写“磋商响应函”、“磋商报价表”以及其他相关文件。

**14. 磋商报价**

14.1 供应商应按照磋商文件要求进行报价，不得将采购内容拆开投标。

14.2 凡本磋商文件要求（或允许）及供应商认为需要进行磋商报价的各项费用项目（不论是否要求进入投标），若投标时未报或未在响应文件中予以说明，采购人将认为这些费用供应商已计取，并包含在报价中（项目内容、项目量调整除外）。

**15. 磋商货币**

15.1 采购人只接受人民币作为唯一磋商货币。

**16. 证明供应商资格的证明文件**

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

**17. 证明的合格性和符合磋商文件规定的文件**

17.1 供应商应对磋商文件中的各项条款做出清晰准确的答复。

17.2 证明服务质量与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：

17.2.1 公司简介；

17.2.2 公司资质；

17.2.3 人员、业绩证明材料。

**18. 磋商保证金**

18.1 根据《西安市财政局关于促进政府采购公平竞争优化营商环境》（市财函【2020】617 号文），本次项目无需缴纳磋商保证金。

**19. 磋商有效期**

19.1 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。

19.2 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。

**20. 响应文件的签署及格式**

20.1 响应文件正本应打印或用不褪色的墨水书写，并加盖单位公章。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，造成非实质性响应磋商文件的响应文件将会被认定为无效磋商。正本与副本不一致时以正本为准。

20.2 以电话、传真、电子邮件形式的磋商将被拒绝。

## D．响应文件的递交

### 21．响应文件的数量、包装和标记

21.1 供应商制作壹份正本“响应文件”、贰份副本“响应文件”、壹份电子版文件。每套“响应文件”封面应注明“正本”、“副本”、“电子版文件”，一旦正本与副本不符，以正本为主。

21.2 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，不致因搬运、堆放等原因散开。磋商时，供应商应当将响应文件封装，所有密封袋正面和响应文件封面须标明项目名称、项目编号、供应商名称及“正本”、“副本”、“电子版文件”等字样。

21.3 所有响应文件的密封袋应加盖供应商公章。

21.4 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。

### 22．磋商截止时间

22.1 所有响应文件都必须按“磋商公告”中规定的响应文件递交截止时间前送达磋商文件规定的递交地址。

22.2 出现第 8.3 款因磋商文件的修改推迟磋商截止日期时，则按采购人修改通知规定的时间递交。

22.3 在响应文件递交截止时间之后的任何响应文件将被拒绝接收。

### 23．响应文件的修改与撤回

23.1 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，并以书面形式通知采购代理机构。补充或修改的内容作为响应文件的组成部分。

23.2 供应商对响应文件的补充修改，应按照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。

23.3 在磋商截止期之后，供应商不得对其磋商做任何修改。

23.4 已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。采购人、采购代理机构按照规定退还退出磋商的供应商磋商保证金。

23.5 无论供应商成交与否或者废标，其响应文件概不退还。

## E. 磋商

### 24. 磋商

24.1 采购代理机构按磋商公告中规定的时间和地点接受供应商递交的响应文件。供应商的法定代表人或其授权的代表签到，并参加磋商。

24.2 供应商和监标人查验响应文件密封情况并签字确认。

24.3 磋商开始时，磋商小组所有成员集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

24.4 开标程序:

24.4.1 介绍参会各方人员；

24.4.2 介绍供应商；

24.4.3 宣布开标纪律；

24.4.4 签署拒绝商业贿赂承诺书；

24.4.5 由供应商法定代表人或其委托代理人、监标人检查响应文件的密封情况，并对密封情况确认；

24.4.6 开标；

24.4.7 宣布休会，进入评审和磋商阶段；

24.4.8 会议结束。

### 25. 磋商小组

25.1 采购人将根据本次采购项目的特点，按照《政府采购竞争性磋商采购方式管理暂行办法》等有关规定组建磋商小组。

25.2 磋商小组成员由采购人及有关技术、经济等方面的专家组成，负责评审活动。

25.3 磋商小组成员对各供应商响应文件进行审查、质疑、评估和比较，并推荐出成交候选人。

25.4 磋商小组负责具体评审事务，并独立履行下列职责：

1）审查、评价响应文件是否符合磋商文件的商务、技术等实质性要求；

2）要求供应商对响应文件有关事项做出澄清或者说明；

3）对响应文件进行比较和评价；

4）确定成交候选人名单，以及根据采购人委托直接确定成交人；

5）向采购人、采购代理机构或者有关部门报告评审中发现的违法行为。

**26．响应文件的审核**

26.1 响应文件的资格性审查：依据法律法规和磋商文件的规定，采购人或其委托的采购代理机构对响应文件中的资格证明文件等进行审查，审查内容为文件中所列的供应商资格条件。

26.2 响应文件符合性审查：依据磋商文件的规定，磋商小组从响应文件的有效性、完整性和对磋商文件的响应程度进行审查，以确定是否对磋商文件的实质性内容作出响应。其内容包括并不局限以下部分：

26.2.1 法定代表人直接参加的，须提供身份证；法定代表人授权他人参加的，须提供法定代表人授权委托书，被授权人提供近 3 个月在投标单位所缴纳的社保证明资料；

26.2.2 本项目不接受联合体磋商；

26.2.3 供应商按要求提供“关于非西安市中医医院职工开办或控股的企业书面声明”、“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”、“供应商参加政府采购活动承诺书”、“供应商诚信承诺书”；

26.2.4 服务期限完全响应；

26.2.5 付款方式完全响应；

26.2.6 响应文件的数量合格；

26.2.7 响应文件有效期合格；

26.2.8 响应文件的签字盖章合格；

26.2.9 磋商文件规定的其他要求。

26.3 经过对供应商及响应文件的资格性、符合性审查，出现下列情况者（但不限于），按无效处理。

26.3.1 供应商没有经过正常渠道获取磋商文件或供应商的名称与获取磋商文件单位的名称不符；

26.3.2 响应文件没有法定代表人授权书（法人直接参加除外）或授权书的合法性或有效性不符合磋商文件规定；

26.3.3 供应商资质或符合性不符合要求的；

26.3.4 响应文件未按磋商文件规定有效签字和盖章的；

26.3.5 磋商有效期不足的；

26.3.6 磋商内容出现漏项或数量与要求不符、技术参数严重偏离的；

26.3.7 响应文件的合同主要条款响应与磋商文件要求不一致（付款、验收等项），附加了采购人难以接受的条件；

26.3.8 规定不接受选择方案和选择报价（包括交叉折扣）的，供应商提供了选择方案和/或选择报价（包括交叉折扣）；

26.3.9 磋商报价超出采购预算的或与市场价偏离较大，低于成本，形成不正当竞争；

26.3.10 提供虚假证明，开具虚假资质，出现虚假应答，除按无效标处理外，还进行相应的处罚；

26.3.11 供应商有违法违规行为的。

**27．响应文件的澄清**

27.1 在评审期间，磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。

27.2 供应商应采用书面形式进行澄清或说明,但不得超出响应文件的范围或改变响应文件的实质性内容。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字。

**28．响应文件的比较和评价**

28.1 磋商小组在评审过程中，发现响应文件出现下列情况之一者，按以下原则修正：

28.1.1 磋商报价表内容与响应文件中报价内容不一致的，以磋商报价表为准；

28.1.2 大写金额和小写金额不一致的，以大写金额为准；

28.1.3 如果以单价计算的结果与总价不一致，则以单价为准修改总价；单价金额小数点有明显错位的，应以总价为准，并修改单价；

28.1.4 如果用文字表示的数值与用数字表示的数值不一致，以文字表示的值为准。

28.1.5 对不同文字文本响应文件的解释发生异议的，以中文文本为准；

28.1.6 正本与副本不一致的，以正本为准；

28.1.7 对于响应文件中不构成实质性偏差的小的不正规、不一致或不规则，采购人可以接受，但这种接受不能损害或影响任何供应商的相对排序。

28.2 如果磋商实质上没有响应磋商文件的要求，其磋商将被拒绝，供应商不得通过修正或撤消不合要求的偏离或保留从而使其磋商成为实质上响应的磋商。

28.3 评审程序：采取逐项分步评审方式，每一步评审不符合者，不进入下一步评审，先进行资格性审查，再进行符合性审查。

28.4 磋商小组根据各磋商供应商响应文件响应情况决定是否与各供应商进行磋商，磋商方式为磋商小组所有成员集中与单一供应商分别进行磋商，并给与参加磋商的供应商平等的磋商机会。

28.5 通过符合性审查的供应商应当在磋商小组规定的时间内提交最后报价，并由法定代表人或其授权人签字，所有报价现场不对供应商公布。最终磋商报价为不可更改价格，最后报价是供应商响应文件的有效组成部分，作为磋商小组推荐成交候选供应商的依据。

28.6 磋商小组认为供应商的最后报价或者某些分项报价明显不合理或者低于成本，有可能影响产品质量和不能诚信履约的，要求其在磋商小组规定的期限内提供书面文件予以解释说明，并提交相关证明材料；如果其不能在磋商小组规定时间内够提供相关材料证明其报价的合理性，其最后报价为无效报价。

**29. 评审原则及主要方法**

29.1 磋商小组将遵循公平、公正和择优的原则，对所有供应商的响应文件评审，都采用相同的程序和标准。

29.2 评审过程的保密：在响应文件的评审、比较、成交候选供应商推荐以及授予合同的过程中，供应商向采购人和磋商小组施加影响的任何行为，都将会导致其报价被拒绝。

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

## 评分标准

| 评分因素 | 内容 | 分值 |
|---|---|---|
| 价格 | 实质性满足磋商文件要求且报价最低者为磋商基准价，其价格分值为满分 20 分。<br>报价得分=（磋商基准价/投标报价）*价格分值 | 20 |
| 服务方案 | 供应商根据国家相关标准并结合本项目实际需求，提供完整的等级保护测评服务方案，内容包括：①系统调研②现场测评③分析整改④结论报告⑤配合验收。<br>1.提供的方案内容完全满足采购需求，思路清晰，逻辑缜 | 20 |

| | | |
|---|---|---|
| | 密，科学高效每项计 4 分；<br>2.提供的方案内容基本满足需求，思路清晰，科学合理每项计 3 分；<br>3.提供的方案内容基本满足需求，描述完整每项计 2 分；<br>4.提供的方案内容不详尽或不适用于本项目，每项计 1 分；<br>5.未提供不计分。 | |
| 风险防范措施 | 供应商针对本项目提供整个测评项目实施过程中的风险防范措施，并明确保密责任与赔偿承诺。承诺配合验收，通过主管部门技术评审工作。<br>1.供应商提供详细的风险防范措施方案，保密性强，配合度高得 6 分。<br>2.供应商提供风险防范措施方案较完善，保密性较弱得 4 分。<br>3.供应商提供风险防范措施方案不够完善，保密性及配合度较差得 2 分。<br>4.供应商未提供相关内容得 0 分。 | 6 |
| 项目质量管控措施 | 供应商针对本项目提供严格的项目质量管理、过程控制及监控手段，能确保技术人员按照相应的操作指导规范实施测评。<br>1.供应商提供详细的质量管理、过程控制及监控手段等方案，符合标准，科学、合理、先进，可操作性强得 6 分。<br>2.供应商提供质量管理、过程控制及监控手段等方案较完善，符合标准，先进性较弱得 4 分。<br>3.供应商提供质量管理、过程控制及监控手段等方案较简单，可操作性较弱差得 2 分。<br>4.供应商未提供相关内容得 0 分。 | 6 |
| 项目经理 | 项目经理具备高级测评师、高级网络信息安全工程师证书。每具备一项证书得 1 分，共 2 分。（提供近 3 个月在投标单位的社保证明材料） | 2 |
| 团队人员技术能力基本要求 | 1.团队成员不少于 6 人，每增加 1 个人增加 0.5 分；最高 2 分。 | 4 |

| | | |
|---|---|---|
| （不包含项目经理） | 2.现场测评人员不得少于4人，其中至少包含1名高级测评师，中级测评师不得少于3人。每增加1名高级测评师加1分；每增加1名中级测评师加0.5分，最高2分。<br>提供人员相关证书证明资料。 | |
| 团队人员技术能力（不包含项目经理） | 项目组测评团队成员中具有（1）ITIL证书、（2）CISP-PTE证书、（3）CISSP或CISP证书、（4）网络安全应用检测专业测评人员（NSATP-A)证书、（5）信息安全保障人员认证证书（CISAW-应急服务），每提供一种证书得1分，共5分。<br>提供人员相关证书证明资料。 | 5 |
| 售后服务 | 为保障测评项目结束后的网络安全，为期一年的售后服务期限服务方须提供完善的售后服务，包括①应急响应服务②电话支持服务③配合检查服务④安全咨询服务⑤安全培训服务内容。<br>1.提供的方案内容完全满足采购需求，思路清晰，逻辑缜密，科学高效每项计4分；<br>2.提供的方案内容基本满足需求，思路清晰，科学合理每项计3分；<br>3.提供的方案内容基本满足需求，描述完整每项计2分；<br>4.提供的方案内容不详尽或不适用于本项目，每项计1分；<br>5.未提供不计分。 | 20 |
| 企业证书 | 1.供应商具备信息安全应急处理服务资质认证证书得1分，不提供不得分；<br>2.供应商具备信息安全风险评估服务资质认证证书得1分，不提供不得分；<br>3.供应商具备信息系统安全运维服务资质认证证书得1分，不提供不得分；<br>4.供应商具备信息安全管理体系认证 ISO27001 证书得1分，不提供不得分；<br>5.供应商具备信息技术服务管理体系认证 ISO20000 证 | 7 |

| | | |
|---|---|---|
| | 书，得 1 分，不提供不得分；<br>6.供应商参加公安部或 CNAS 实验室组织的能力验证活动，3 年以上验证结果为满意得 2 分，3 年及以下验证结果为满意得 1 分。 | |
| 业绩 | 供应商具有 2022 年 1 月 1 日至今同类业绩，每个 2 分，最高累计至 10 分。<br>注：需提供完整合同及验收证明材料并加盖单位公章。 | 10 |

29.4 综合评分法中的价格统一采用低价优先法计算,既满足磋商文件要求且最后磋商报价最低的供应商价格为磋商基准价，其价格分为满分。

29.5 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 1-3 名成交候选供应商，并编写评审报告，评审得分相同的，按照最后报价由低到高的顺序推荐。

29.6 评审过程中，若出现本办法以外的特殊情况时，将暂停评审，有关情况待磋商小组确定后，再行评定。

29.7 **需要落实的政府采购政策**

29.7.1 根据财政部、工业和信息化部关于印发《政府采购促进中小企业发展管理办法》的通知(财库〔2020〕46 号)。

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

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

（二）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

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

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

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

中小企业参加政府采购活动，应当出具本办法规定的《中小企业声明函》（见附件），符合本办法规定的小微企业报价给予 10%的扣除，用扣除后的价格参加评审。否则不得享受相关政策。

供应商出具《中小型企业声明函》，并对声明的真实性负责。否则，按照有关规定予以处理。

29.7.2 监狱和戒毒企业应符合《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，并提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明和《监狱和戒毒企业声明函》。符合本办法规定的给予 10%的扣除，用扣除后的价格参加评审。

29.7.3 残疾人福利性单位应符合《三部门联合发布关于促进残疾人就业政府采购政策的通知》-财库〔2017〕141 号，并提供通知规定的《残疾人福利性单位声明函》，并对声明的真实性负责。

任何单位或者个人在政府采购活动中均不得要求残疾人福利性单位提供其他证明声明函内容的材料。符合本办法规定的给予 10%的扣除，用扣除后的价格参加评审。

中标、成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随中标、成交结果同时公告其《中小型企业声明函》、《监狱和戒毒企业声明函》、《残疾人福利性单位声明函》，接受社会监督。

供应商提供的声明函与事实不符的，依照《中华人民共和国政府采购法》第七十七条第一款的规定追究法律责任。

投标供应商应如实提供以上证明文件，如存在虚假应标，将取消其投标资格。

29.7.4 **专门面向中小企业采购的项目或者采购包，不再执行价格评审优惠的扶持政策。**

29.7.5 投标产品政府采购政策

29.7.5.1 节能产品根据《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51 号）的规定，以财库〔2019〕9 号为准。

29.7.5.2 环境标志产品根据《环境标志产品政府采购实施的意见》（财库[2006]90 号）的规定，以财库〔2019〕9 号为准。

29.7.5.3 依据品目清单和认证证书实施政府优先采购和强制采购。采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构应当依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。

29.7.5.4 节能产品、环境标志产品认证机构应当建立健全数据共享机制，及时向认证结果信息发布平台提供相关信息。中国政府采购网（www.ccgp.gov.cn）建立与认

证结果信息发布平台的链接，方便采购人和采购代理机构查询、了解认证机构和获证产品相关情况。

29.7.5.5 对于已列入品目清单的产品类别,采购人可在采购需求中提出更高的节约资源和保护环境要求，对符合条件的获证产品给予优先待遇。

29.7.5.6 获得上述认证的产品在投标时应提供有效证明材料。以上所有证明文件复印件须加盖供应商公章并注明“与原件一致”，否则不予计分。

**30．与采购人、采购代理机构和磋商小组接触**

30.1 供应商试图对采购人和磋商小组的评审、比较或授予合同的决定进行影响，都可能导致其磋商被拒绝。

## F．授予合同

**31．定标及合同授予**

31.1 采购代理机构应在评标结束后二个工作日内，将评标报告送采购人定标。

31.2 采购人在收到评标报告后五个工作日内,根据评标报告对评标过程及结果进行审核后确定成交供应商，复函采购代理机构。

31.3 采购代理机构在接到采购人的成交复函后，在采购信息发布媒体上公告，并按照规定向成交供应商发《成交通知书》。

31.4 采购代理机构向成交供应商发出《成交通知书》。

31.5《成交通知书》将作为签订合同的依据，磋商文件、成交供应商的响应文件和补充文件（如澄清、承诺等）等，均为有法律约束力的经济合同组成的一部分。

31.6《成交通知书》发出 30 天内，如果已成交的供应商不能按响应文件，包括补充文件（如澄清、承诺等）中承诺的条件履行签约行为，采购人有权取消其成交资格。

31.7 成交供应商如果因不可抗力或自身原因不能履行采购合同,采购人可与排位在成交供应商之后第一位的成交侯选人签订采购合同，以此类推。

**32．接受和拒绝任何或所有磋商的权力**

32.1 采购代理机构和采购人保留在授标之前任何时候接受或拒绝任何磋商，以及宣布磋商程序无效或拒绝所有磋商的权力，对受影响的供应商不承担任何责任，也无义务向受影响的供应商解释采取这一行动的理由。

**33．履约保证金**

33.1 本项目无履约保证金。

**34. 腐败和欺诈行为**

34.1 定义

34.1.1. “腐败行为”是指提供给予接受或索取任何有价值的东西来影响采购代理机构和/或采购人在采购过程或合同实施过程中的行为。

34.1.2. “欺诈行为”是指为了影响采购过程或合同实施过程而谎报事实，损害采购代理机构和/或采购人的利益，包括供应商之间相互串通（递交响应文件之前和之后），人为地使磋商丧失竞争性，剥夺采购人从自由公开竞争所能获得的权益。

34.2 如果采购代理机构和采购人认为供应商在本项目的竞争中有腐败或欺诈行为，其磋商将被拒绝。

**35. 招标代理服务费**

35.1 招标代理服务费：成交供应商应向采购代理机构交纳招标代理服务费。招标代理服务费收取参照国家计委颁布的《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）收费标准收取。

35.2 招标代理服务费的交纳方式：在领取成交通知书时按 35.1 的规定，向采购代理机构直接交纳服务费，采用现金或支票方式一次性交纳。

**开户名称：陕西中技招标有限公司**

**开户行名称：招商银行西安分行营业部**

**账号：129916812810001**

**转账事由： 项目编号（后四位）招标代理服务费**

# 第四部分　合同一般条款

# 西 安 市 中 医 医 院

# 服 务 合 同

甲　方：西安市中医医院

乙　方：

2025 年

中国　西安

# 服 务 合 同

制式

**甲方：西安市中医医院**

**乙方：**

根据《中华人民共和国民法典》及有关法律法规，甲乙双方本着平等互利的原则，经友好协商，签订本合同并信守下列条款，共同严格履行。

**一、合同内容**

甲方委托乙方就____系统进行网络安全等级保护测评服务。

**二、服务内容**

1.服务内容：

2.服务要求：

3.售后服务：

**三、服务时间**

合同测评服务从甲方要求开展测评工作之日起_____日历日内完成，售后服务期_____年，自验收合格之日起计算。

**四、服务准则**

**五、 服务价格及付款方式**

1. 本合同测评服务费含税总价为人民币___元整（ ____元）。

2. 本合同系统级别分项价格：

| 系统级别 | 单价（元） | 数量 | 小计 |
|---|---|---|---|
| 二级 | | | |
| 三级 | | | |
| 合计 | | | |

3. 乙方的账户名称、开户银行、银行账号以本合同提供的为准，如有变更，乙方应在合同规定的相关付款期限一周前以书面方式通知甲方并加盖财务专用章。

付款方式和时间：完成交付内容且递交纸质版及电子版资料后经由乙方提出验收申请，经甲方验收合格取得签署的书面验收报告（递交备案证书、测评报告）。甲方收到乙方出具的全额发票及验收申请且达到付款条件后30日内，甲方向乙方支付合

同总价的95%，即人民币_元整（即￥：___元 ）。

项目通过验收后满1年，甲方支付合同总价的5%，即人民币___元整（即￥：__元 ）。

4.乙方负责开具符合国家及本合同规定的相应数据额的6%增值税 普通 发票。

转账银行：

账号：

5.甲方付款前乙方应向甲方提供发票，否则甲方有权暂不付款且不承担任何违约责任。

**六、责任与义务**

1.甲方的权利和义务

（1）甲方应配合乙方的工作，按时提供相应的数据、信息和资料，并保证其正确性、真实性。乙方应在合同签订后2个工作日内向甲方提供测评所需的资料清单，甲方按清单内容提供资料。

（2）甲方未按照合同约定履行款项支付义务，逾期支付费用的，每逾期一日，以未付款为基数，按照万分之五/日标准承担至实际清偿之日的逾期付款违约金。

（3）甲方应该在乙方提交 纸质版及电子版资料后【 15 】工作日内组织验收。

2、乙方的权利和义务

（1）乙方保证提供给甲方的等级保护测评报告符合国家和公安部颁布标准及合同规定的要求。

（2）乙方保证在项目实施过程中甲方的网络正常运行。

（3）乙方保证向甲方提供的技术资料是清晰的、正确的、完整的。

（4）乙方保证提供的服务不侵犯任何第三方合法权益，否则由此引起的责任由乙方全部承担。

（5）如因乙方提供的相关资料或提供的技术资料错误，或乙方在现场的技术人员指导有错误而使报告不能达到要求，乙方负责修改，由此引起的费用由乙方承担。乙方每逾期一日，应按照合同金额1%向甲方支付违约金，逾期超过15日，甲方有权解除合同。

（4）（6）如因甲方提供的数据、信息和资料有误或不能如期提供，影响工作质量和进度，乙方无需承担逾期责任，甲方逾期15个工作日不提供约定的技术条件的，乙方有权解除合同。

**七、免责条款**

1、如果本协议的其中一方因受战争、火灾、洪水、地震、国内骚乱或其它灾害影响，而不能履行本协议，则履约时间应被延长，而且对于因延时而造成的损失，任何一方都不必承担责任。

2、受阻的一方应在不可抗力因素发生后尽可能短时间内通过传真、电话、邮件等形式通知另一方，并在此后十四天内，将有关部门签发的书面证明作为证据发送给另一方。否则，发生不可抗力一方不得以不可抗力进行抗辩，双方应按照本合同约定履行合同。

**八、其它条款**

1、延续或终止

本合同自双方代表人签字并加盖公章之日起生效，合同时效性为一年，合同期满后结束。

2、争议的解决

本合同引起的或与本合同有关的所有争议，双方应本着相互信任、以诚相待的原则友善协商，协商不成时，任何一方有权向甲方所在地人民法院诉讼解决。

3、本合同一式___份，甲方___份，乙方___份，合同附件具有同等法律效力。合同未尽事宜可日后签署补充协议，补充协议与本合同具有同等法律效力，补充协议内容中如有与本合同内容不同之处，以补充协议为准。

（以下无正文）

甲　方（盖章）　　乙　方（盖章）

单位名称：　　单位名称：

地　址：　　地　址：

法定代表人：（签章）　　法定代表人：（签章）

主管院长：（签字）

代理人：（签字）　　经办人：（签字）

经办人：（签字）

联系电话：　　联系电话：

签字日期：　　年　月　日　　签字日期：　　年　月　日

# 第五部分　附件--响应文件格式

正/副本/电子版文件

（封面）

# 西安市中医医院等级保护测评项目

# 磋商响应文件

项目编号： SZT2025-SN-XC-ZC-FW-0717

供应商名称：_____

（盖公章）

二零二五年___月

# 响应文件目录

# 附件1　磋商响应函

致：陕西中技招标有限公司

根据贵方为 项目名称、项目编号 采购服务的竞争性磋商文件，签字代表(全名、职务)经正式授权并代表(供应商名称、地址)提交包含下述内容的响应文件正本一份、副本二份、电子版文件一份。

(1) 磋商响应函；

(2) 磋商报价表；

(3) 按磋商须知要求提供的全部文件和磋商文件要求的响应文件；

(4) 供应商资格证明文件；

(5) 已交纳磋商保证金，金额为_____。

据此函，签字代表宣布同意如下：

1、供应商将按磋商文件的规定履行合同责任和义务；

2. 供应商已详细审查全部磋商文件，包括修改文件（如有的话）以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权利；

3. 磋商报价自递交响应文件截止之日起有效期为 90 个日历天；

4. 如果在规定的宣读磋商报价时间后，供应商在磋商有效期内撤回磋商报价；或成交后未按磋商文件中磋商须知规定的向采购代理机构交纳足额的招标代理服务费，其磋商保证金将被贵方没收；

5. 供应商同意提供按照贵方可能要求的与其报价有关的一切数据或资料,完全理解贵方不一定要接受最低价的磋商报价或收到的任何磋商报价。

6. 与本磋商有关的一切正式往来通讯请寄：

地址：_____　　邮编：_____

电话：_____　　传真：_____

供应商代表姓名、职务（印刷体）：_____

供应商名称：_____（公章）

法定代表人或被授权代表签字或盖章：_____

日期：　____年___月___日

# 附件2 磋商报价表

| | |
|---|---|
| 项目名称 | |
| 项目编号 | |
| 供应商 | |
| 磋商报价 | 人民币（小写）：_____元<br>大写金额：_____元 |
| 服务期限是否响应 | |
| 付款方式是否响应 | |

备注：

1.报价不得超出采购预算，如果超出采购预算，本次报价为无效报价。

2.服务期限是否响应、付款方式是否响应填写“是”或“否”。

**供应商：_____（公章）_____**

**法定代表人或被授权代表（签字或盖章）：_____**

**日期：_____**

# 附件3　分项报价表

供应商名称：_____项目编号：_____

| 序号 | | | | | |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| ... | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**供应商：_____（公章）_____**

**法定代表人或被授权代表（签字或盖章）：_____**

**日期：_____**

# 附件4 商务偏离表

供应商名称：_____项目编号：_____

| 序号 | 内容 | 磋商文件商务要求 | 响应文件商务响应 | 偏离 | 说明 |
|---|---|---|---|---|---|
| | 服务期限 | | | | |
| | 付款方式 | | | | |
| | 服务地点 | | | | |
| | | ... | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**注：**如全部响应磋商文件所提商务要求，在“磋商文件商务要求”及“响应文件商务响应”栏中填写“全部”字样，在“偏离情况”栏填入“无偏离”字样。除以上表中列明的偏离项之外，供应商完全响应磋商文件的所有商务条款。

**供应商：_____（公章）_____**

**日期：_____**

# 附件 5　服务方案

（格式自定）

# 附件6 服务承诺

致：（采购人）

我公司对参加此次“_____（项目名称）”所提供的服务做如下承诺：

（承诺内容）

**供应商：_____（公章）_____**

**日期：_____**

# 附件 7　供应商为本项目提供的资格证明文件

**一、满足《中华人民共和国政府采购法》第二十二条规定；**

1.具有独立承担民事责任的能力（企业法人应提供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、组织机构代码证等证明文件；其他组织应提供合法证明文件；自然人提供身份证明文件）；

2.具有良好的商业信誉和健全的财务会计制度（提供 2024 年度财务审计报告或开标前 3 个月内的银行资信证明或财政部门认可的政府采购专业担保机构出具的投标担保函）；

3.具有履行合同所必需的设备和专业技术能力的书面声明（格式详见附件）；

4.具有依法缴纳税收和社会保障资金的良好记录（提供开标前 12 个月内任一月份的社保和缴纳税收的证明，依法不需要缴纳社会保障资金、免税或无须缴纳税款的供应商，应提供相关证明文件)；

5.参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明（格式详见附件）

**二、落实政府采购政策需满足的资格要求：**

本项目为专门面向中小企业采购的采购项目。

**三、本项目的特定资格要求：**

供应商提供有效的《网络安全服务认证证书等级保护测评服务认证》

**注：资格证明文件须加盖供应商公章。**

**具有独立承担民事责任的能力（企业法人应提供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、组织机构代码证等证明文件；其他组织应提供合法证明文件；自然人提供身份证明文件）；**

具有良好的商业信誉和健全的财务会计制度（提供2024年度财务审计报告或开标前3个月内的银行资信证明或财政部门认可的政府采购专业担保机构出具的投标担保函）

**具有履行合同所必需的设备和专业技术能力；**

（采购人）：

（供应商名称） 于_____年_____月___日在中华人民共和国境内（详细注册地址）合法注册并经营，公司主营业务为_____，营业（生产经营）面积为_____，现有员工数量为_____，其中与履行本合同相关的专业技术人员有（专业能力、数量），本公司郑重承诺，具有履行本合同所必需的设备和专业技术能力。

| 履行合同所必需的设备清单 | | | | |
|---|---|---|---|---|
| 序号 | 设备或材料名称 | 品牌及型号 | 数量 | 备注（自购/租赁） |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| …. | | | | |

**供应商：_____（公章）_____**

**日期：_____**

**具有依法缴纳税收和社会保障资金的良好记录（提供开标前12个月内任一月份的社保和缴纳税收的证明,依法不需要缴纳社会保障资金、免税或无须缴纳税款的供应商，应提供相关证明文件)；**

提供社会保障资金缴纳记录证明文件

说明：

1、供应商须依法缴纳社会保障资金，须提供磋商截止时间前12个月内任意1个月的社会保障资金缴纳记录复印件并加盖供应商单位公章，新开户的供应商提供社保开户证明，自行编写无效。

2、国家、地方工商管理部门或者其他相关管理部门对社会保障资金缴纳（如免缴）有特别政策的，须提供相关政策文件复印件以及供应商满足相关政策文件的证明文件。

# 依法缴纳税收记录证明文件

说明：

1、供应商须提供磋商截止时间前 12 个月内任意 1 个月的依法缴纳税收记录（依法免税或无须缴纳税款的供应商，应提供相关证明文件)。

2、国家、地方工商管理部门或者其他相关管理部门对企业纳税有特别规定的，须提供相关政策性文件复印件和供应商满足政策文件规定的证明文件。

**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；**

（采购人）：

我方作为项目名称_____（项目编号：_____）的投标供应商，在此郑重声明：

1、在参加本次政府采购活动前3年内的经营活动中_____（填“没有”或“有”）重大违法记录。供应商在参加政府采购活动前3年内因违法经营被禁止在一定期限内参加政府采购活动，期限届满的，可以参加政府采购活动，但应提供期限届满的证明材料。

2、我方_____（填“未被列入”或“被列入”）失信被执行人名单。

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

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

如有不实，我方将无条件地退出本项目的采购活动，并遵照《中华人民共和国政府采购法》有关“提供虚假材料的规定”接受处罚。

特此声明。

**供应商：_____（公章）_____**

**日期：_____**

**本项目为专门面向中小企业采购的采购项目**

## 中小企业声明函（工程、服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：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*（软件和信息技术服务业）*；承建（承接）企业为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于*（中型企业、小型企业、微型企业）*；

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依 法承担相应责任。

企业名称（盖章）：

日 期：

从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

**根据《中小企业划型标准规定》软件和信息技术服务业**。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业;从业人员 10 人及以上,且营业收入 50 万元及以上的为小型企业;从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

**供应商提供有效的《网络安全服务认证证书等级保护测评服务认证》**

# 附件 8 法定代表人授权委托书

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，现代表公司授权的（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）项目编号为（项目编号）的投标活动。代理人在本次投标中所签署的一切文件和处理的一切有关事物，我公司均予承认。

本授权有效期：自投标截止之日起 90 日历天；特此声明。

| | |
|---|---|
| 法定代表人身份证复印件 | 授权代表身份证复印件 |
| 法定代表人身份证复印件 | 授权代表身份证复印件 |

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（法定代表人直接参加投标的，须出具法定代表人身份证）

**供应商名称：**_____（公章）

**法定代表人：**_____（签字或盖章）

**日期：**____年____月____日

**被授权人提供近 3 个月在投标单位所缴纳的社保证明资料；**

# 附件 9 本项目不接受联合体磋商

（采购人）：

我方作为项目名称_____（项目编号：_____）的投标供应商，在此郑重声明：

我单位参与本项目并非联合体，本项目由本公司独立承担。

特此声明。

**供应商：_____（公章）_____**

**日期：_____**

# 附件10供应商参加政府采购活动承诺书

**（供应商诚信承诺书）**

致：（采购人）

为了诚实、客观、有序地参与陕西省政府采购活动，愿就以下内容作出承诺：

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

二、参加采购代理机构组织的政府采购活动时，严格按照招标文件的规定和要求提供所需的相关材料，并对所提供的各类资料的真实性负责，不虚假应标，不虚列业绩。

三、尊重参与政府采购活动各相关方的合法行为，接受政府采购活动依法形成的意见、结果。

四、依法参加政府采购活动，不围标、串标，维护市场秩序，不提供“三无”产品、以次充好。

五、积极推动政府采购活动健康开展，对采购活动有疑问、异议时，按法律规定的程序实名（加盖单位章和法定代表人签名）反映情况，不恶意中伤、无事生非，以和谐、平等的心态参加政府采购活动。

六、认真履行中标人应承担的责任和义务，全面执行采购合同规定的各项内容，保质保量地按时提供采购物品。

若本企业（单位）发生有悖于上述承诺的行为，愿意接受《中华人民共和国政府采购法》和《中华人民共和国政府采购法实施条例》中对供应商的相关处理。

本承诺是项目投标文件的组成部分。

**供应商：**_____（公章）_____

**日期：**_____

# 附件 11 供应商诚信承诺书

格式自定

内容包括但不限于：

1.供应商与其他投标单位无交叉控股股东、无交叉兼任高级管理人员及涉嫌联合围标、串标行为，无采购单位和招标代理机构职工在该单位兼职的情况，不向采购单位和代理机构相关人员输送利益等行贿行为，一旦中标必须坚守诚信、认真履约等。

2.供应商未被列入相关部门“黑名单”以及有行贿、串标等违法违规行为。

进入相关部门“黑名单”的供应商以及有行贿、串标等违法违规行为并经查实的供应商不能参与采购人采购项目的投标活动。对“黑名单”中供应商采取“一票否决”及“随时叫停”机制，在报名、资格审核、评审、公示、合同签订等各环节一旦发现并查实有行贿等违法违规行为的，立即取消其相关资格且终止合同签订。

# 附件 12 关于非西安市中医医院职工及其亲属投资开办或控股的企业书面声明

西安市中医医院：

我单位参与_____（代理机构名称）组织的项目名称 _____（项目编号：_____）的采购项目，我单位郑重声明：我方非西安市中医医院职工及其亲属投资开办或控股的企业，如有虚假，承担相应责任。特此声明！

供应商全称(盖章)：

法人代表或授权代表（签字或盖章）：

日期：

注：

1、 供应商未提供或提供虚假声明，都将作为无效投标处理。

2、 本承诺书列入符合性审查，承诺内容及格式不得更改。

3、 若在定标阶段发现交候选人为采购人单位职工及其亲属投资开办或控股的企业，则取消其成交候选人资格。

# 附件13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

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、不向政府采购人、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、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：_____（公章）_____**

**日期：_____**

# 附件 14　其他相关资料

供应商认为对其投标有利的其它证明。

# 第六部分　采购内容及要求

## 一、项目概况

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，对医院医疗信息系统、集成平台系统、数据中心系统、互联网医院、官方网站系统等系统实施网络安全等级保护测评工作。

## 二、服务内容

对以下信息系统在“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”等方面的开展测评工作。

| 序号 | 系统名称 | 系统级别 |
|---|---|---|
| 1 | 医疗信息系统 | 三级 |
| 2 | 集成平台系统 | 三级 |
| 3 | 数据中心系统 | 三级 |
| 4 | 互联网医院 | 三级 |
| 5 | 官方网站系统 | 二级 |

## 三、技术要求

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。

1.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。

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，配合采购单位安全整改工作。

**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，提交系统相关人员。

测评标准：

**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 | 1.物理位置选择 | 1.1 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； |
| | | 1.2 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。 |
| | 2.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。 |
| | 3.防盗窃和防破坏 | 3.1 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； |
| | | 3.2 应将通信线缆铺设在隐蔽安全处； |
| | 4.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。 |
| | 5.防火 | 5.1 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； |
| | | 5.2 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； |
| | 6.防水和防潮 | 6.1 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗 |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | | 透； |
| | | 6.2 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。 |
| | 7.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。 |
| | 8.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。 |
| | 9.电力供应 | 9.1 应在机房供电线路上配置稳压器和过电压防护设备； |
| | | 9.2 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。 |
| | 10.电磁防护 | 电源线和通信线缆应隔离铺设，避免互相干扰。 |
| 安全通信网络 | 1.网络架构 | 1.1 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； |
| | | 1.2 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。 |
| | 2.通信传输 | 应采用校验技术保证通信过程中数据的完整性。 |
| | 3.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 | 1.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。 |
| | 2.访问控制 | 2.1 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； |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | | 2.2 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； |
| | | 2.3 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； |
| | | 2.4 应能根据会状态话信息对进出数据流提供明确的允许/拒绝访问的能力； |
| | 3.入侵防范 | 应在关键网络节点处监视网络攻击行为。 |
| | 4.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。 |
| | 5.安全审计 | 5.1 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； |
| | | 5.2 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； |
| | | 5.3 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。 |
| | 6.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 | 1.身份鉴别 | 1.1 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； |
| | | 1.2 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； |
| | | 1.3 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。 |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | 2.访问控制 | 2.1 应对登录的用户分配账户和权限； |
| | | 2.2 应重命名或删除默认账户，修改默认账户的默认口令； |
| | | 2.3 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； |
| | | 2.4 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。 |
| | 3.安全审计 | 3.1 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； |
| | | 3.2 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； |
| | | 3.3 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。 |
| | 4.入侵防范 | 4.1 应遵循最小安装的原则，仅安装需要的组件和应用程序； |
| | | 4.2 应关闭不需要的系统服务、默认共享和高危端口； |
| | | 4.3 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； |
| | | 4.4 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； |
| | | 4.5 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； |
| | 5.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。 |
| | 6.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 |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | | 审计记录送至安全管理中心。 |
| | 7.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。 |
| | 8.数据和备份恢复 | 8.1 应提供重要数据的本地数据备份与恢复功能； |
| | | 8.2 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。 |
| | 9.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。 |
| | 10.个人信息保护 | 10.1 应仅采集和保存业务必需的用户个人信息； |
| | | 10.2 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 | 1.系统管理 | 1.1 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； |
| | | 1.2 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。 |
| | 2.审计管理 | 2.1 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； |
| | | 2.2 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 | 1.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。 |
| | 2.管理制度 | 2.1 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 |
| --- | --- | --- |
| | | 2.2 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。 |
| | 3.制定和发布 | 3.1 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。 |
| | | 3.2 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。 |
| | 4.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 | 1.岗位设置 | 1.1 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； |
| | | 1.2 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。 |
| | 2.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。 |
| | 3.授权和审批 | 3.1 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； |
| | | 3.2 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。 |
| | 4.沟通和合作 | 4.1 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； |
| | | 4.2 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； |
| | | 4.3 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。 |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | 5.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。 |
| 安全管理人员 | 1.人员录用 | 1.1 应指定或授权专门的部门或人员负责人员录用； |
| | | 1.2 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。 |
| | 2.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。 |
| | 3.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。 |
| | 4.外部人员访问管理 | 4.1 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。 |
| | | 4.2 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； |
| | | 4.3 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 | 1.定级和备案 | 1.1 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； |
| | | 1.2 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； |
| | | 1.3 应保证定级结果经过相关部门的批准； |
| | | 1.4 应将备案材料报主管部门和相应公安机关备案。 |
| | 2.安全方案设计 | 2.1 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； |
| | | 2.2 应根据保护对象的安全保护等级进行安全方案设计； |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | | 2.3 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。 |
| | 3.产品采购和使用 | 3.1 应确保网络安全产品采购和使用符合国家的有关规定； |
| | | 3.2 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。 |
| | 4.自行软件开发 | 4.1 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； |
| | | 4.2 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。 |
| | 5.外包软件开发 | 5.1 应在软件交付前检测其中可能存在的恶意代码； |
| | | 5.2 应保证开发单位提供软件设计文档和使用指南。 |
| | 6.工程实施 | 6.1 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； |
| | | 6.2 应制定安全工程实施方案控制工程实施过程。 |
| | 7.测试验收 | 7.1 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； |
| | | 7.2 应进行上线前的安全性测试，并出具安全测试报告。 |
| | 8.系统交付 | 8.1 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； |
| | | 8.2 应对负责运行维护的技术人员进行相应的技能培训； |
| | | 8.3 应提供建设过程文档和运行维护文档。 |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | 9.等级测评 | 9.1 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； |
| | | 9.2 应在发生重大变更或级别发生变化时进行等级测评； |
| | | 9.3 应确保测评机构的选择符合国家有关规定。 |
| | 10.服务供应商选择 | 10.1 应确保服务供应商的选择符合国家的有关规定； |
| | | 10.2 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 | 1.环境管理 | 1.1 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； |
| | | 1.2 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； |
| | | 1.3 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。 |
| | 2.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。 |
| | 3.介质管理 | 3.1 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； |
| | | 3.2 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。 |
| | 4.设备维护管理 | 4.1 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； |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | | 4.2 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。 |
| | 5.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。 |
| | 6.网络和系统安全管理 | 6.1 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； |
| | | 6.2 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； |
| | | 6.3 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； |
| | | 6.4 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； |
| | | 6.5 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。 |
| | 7.恶意代码防范管理 | 7.1 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； |
| | | 7.2 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； |
| | | 7.3 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。 |
| | 8.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、 |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | | 各个设备或软件组件的配置参数等。 |
| | 9.密码管理 | 9.1 应遵循密码相关国家标准和行业标准； |
| | | 9.2 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。 |
| | 10.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。 |
| | 11.备份与恢复管理 | 11.1 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； |
| | | 11.2 应规定备份信息的备份方式、备份频度、存储介质、保存期等； |
| | | 11.3 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。 |
| | 12.安全事件处置 | 12.1 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； |
| | | 12.2 应制定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； |
| | | 12.3 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。 |
| | 13.应急预案管理 | 13.1 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； |
| | | 13.2 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。 |

| 安全层面 | 安全控制点 | 测评指标 |
| --- | --- | --- |
| | 14.外包运维管理 | 14.1 应确保外包运维服务商的选择符合国家的有关规定； |
| | | 14.2 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。 |

**等级保护技术要求（二级）**

| 层面 | 控制点 | 测评要求项 |
| --- | --- | --- |
| 安全物理环境 | 物理位置选择 | a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；<br>b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 |
| | 物理访问控制 | 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 |
| | 防盗窃和防破坏 | a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；<br>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，能够自动检测火情、自动报警，并自动灭火；<br>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；<br>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；<br>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。 |
| | 电磁防护 | 电源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 | 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；<br>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手段。 |
| | 通信传输 | 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。 |
| | 可信验证 | 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全区域边界 | 边界防护 | 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；<br>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；<br>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；<br>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。 |
| | 入侵防范 | 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。 |

| | | |
|---|---|---|
| | 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；<br>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；<br>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，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；<br>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；<br>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；<br>b）应重命名或删除默认账户，修改默认账户的默认口令；<br>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；<br>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；<br>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；<br>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；<br>b）应关闭不需要的系统服务、默认共享和高危端口；<br>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；<br>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；<br>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 | 应采用校验技术保证重要数据在传输过程中的完整性。 |
| | 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能；<br>b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。 |
| | 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；<br>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；<br>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；<br>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；<br>b）应对管理人员或操作人员执行的日常管理操作建立操作规程。 |
| | 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；<br>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；<br>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；<br>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；<br>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；<br>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。 |
| 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；<br>b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。 |
| | 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 | 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；<br>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；<br>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；<br>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；<br>c）应保证定级结果经过相关部门的批准；<br>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；<br>b）应根据保护对象的安全保护等级进行安全方案设计；<br>c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。 |
| | 产品采购和使用 | a）应确保网络安全产品采购和使用符合国家的有关规定；<br>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。 |
| | 自行软件开放 | 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；<br>b）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。 |
| | 外包软件开放 | a）应在软件交付前检测其中可能存在的恶意代码；<br>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；<br>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；<br>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；<br>b）应对负责运行维护的技术人员进行相应的技能培训；<br>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；<br>b）应在发生重大变更或级别发生变化时进行等级测评；<br>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；<br>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 | 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；<br>b）应建立机房安全管理制度，包括物理访问、物品进出和环境安全等方面；<br>c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 |
| | 资产管理 | 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 | 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；<br>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；<br>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。 |
| | 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；<br>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；<br>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；<br>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；<br>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。 |

| | | |
|---|---|---|
| | 恶意代码管理 | a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；<br>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；<br>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；<br>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；<br>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；<br>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；<br>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；<br>c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。 |

| | | |
|---|---|---|
| | 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；<br>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。 |
| | 外包软件管理 | a）应确保外包运维服务商的选择符合国家的有关规定；<br>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。 |

**注：本次系统测评项目需按照等级保护 2.0 测评标准执行。**

**测评流程：**

**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》。

**第二阶段：渗透检测**

渗透测试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。

渗透测试的报告是在发现和攻击阶段，保存测试记录并定期向系统管理员或管理部门报告。在测试结束后，编写报告描述被发现的漏洞、目前的风险等级，并就如何弥补发现的薄弱环节提供建议和指导，最终按照要求出具《渗透测试报告》。

**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。

之后依据相关《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。

## 四、服务要求

**人员配置**

1. 测评人员要求：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。

2. 人员配备：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，执行与完成测评工作，并根据适当情况增加测评人员。

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

**售后服务**

为期一年的售后服务工作中，服务方将向甲方提供包括应急响应、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：

（1）应急响应服务

针对本次项目，服务方提供7X24的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

（2）配合检查服务

服务方免费协助甲方响应公安机关、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。服务内容包括协助甲方准备、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，解答甲方在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过10分钟，到达现场时间不超过2小时，解决问题不超过24小时。

（4）安全咨询服务

服务方为甲方免费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，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合甲方做好业务系统全保障工作。

## 五、商务要求

（一）服务期限

工期：自入场后40个日历日完成现场测评工作，不包含整改时间。

（二）服务要求

1、在测评过程中，不得影响系统使用户单位的正常诊疗活动。

2、服务商须确保项目质量符合国家和行业质量标准。

3、服务商需配备相应的等保测评工程师，项目经理必须为高级测评师，项目经理和现场测评项目组其他成员均具有等保测评的资质认证。

4、服务商在实施过程中接触到的用户单位的涉密信息需严格保密并签订保密协议。

（三）款项结算

**付款方式：银行转账，无预付款，完成交付内容后经由中标人提出验收申请，经招标人验收合格并取得签署的书面验收报告（递交备案证书、测评报告）后，招标人向中标人支付合同总金额的95%，项目通过验收后满1年支付合同总金额的5%。本项**

**目报价一次性包死，医院不承担其他任何费用。**