比选公告

|  |  |
| --- | --- |
| 一、项目基本情况 | |
| 采购项目名称 | 成华区中医医院信息系统等级保护测评服务采购项目 |
| 采购方式 | 比选 |
| 项目限价 | 13万元 |
| 采购需求 | 详见附件 |
| 二、比选申请人资格要求 | |
| 1、在中华人民共和国境内依法注册的法人或者其他组织；  2、具有良好的商业信誉和健全的财务会计制度；  3、具有履行合同所必须的设备和专业技术能力；  4、具有依法缴纳税收和社会保障资金的良好记录；  5、参加本次比选活动前三年内，在经营活动中没有重大违法记录；  6、比选申请人还符合法律、行政法规规定的其他强制性条件；  7、本项目不接受联合体参与。 | |
| 三、报名或比选文件领取方式 | |
| 时间： | 2023年5月26日9:00日-2023年5月30日17:00 |
| 地点： | 成华区中医医院采购办 |
| 报名资料： | 营业执照、法人授权委托书（留下联系方式）、法人身份证复印件、被授权人身份证复印件 |
| 方式： | （1）现场报名：持以上报名资料，在成华区中医医院采购办报名（上午9:00-12:00，下午13:30-17:00，节假日除外）  （2）网络渠道报名：申请人将报名资料以扫描件通过电子邮箱（chqzyyy@163.com）方式进行报名 |
| 四、响应文件递交 | |
| 截止时间： | 2023年5月31日10:00 |
| 地点： | 成华区中医医院采购办 |
| 五、比选 | |
| 时间： | 另行通知 |
| 地点： | 成华区中医医院四楼会议室 |
| 六、其他补充事宜 | |
| 无 |  |
| 七、本项目询问联系方式 | |
| 联系人 | 秦老师 028-60828099 |

**项目编号：CG-2023-016**

医院信息系统等级保护测评服务**采购项目**

**比选文件**

**比选人: 成都市成华区中医医院**

**2023年5月**

**目 录**

**[第一章 比选邀请 - 4 -](#_Toc68619132)**

**[第二章 比选申请书 - 35 -](#_Toc68619133)**

**[第三章 资格证明文件 - 9 -](#_Toc68619134)**

**[第四章 比选需求 - 11 -](#_Toc68619135)**

**[第五章 评审办法 - 27 -](#_Toc68619136)**

# 第一章 比选邀请

**成都市成华区中医医院**拟对**医院信息系统等级保护测评服务采购项目**进行**公开比选，兹邀请相关比选申请人参加比选**。

1. **项目名称：**医院信息系统等级保护测评服务**采购项目**
2. **项目编号：CG-2023-016**
3. **项目概况：**本项目共1个包

项目限价：13万元

01包：成都市成华区中医医院医院信息系统等级保护测评服务采购

注：超过项目限价的报价将作为无效响应处理。

**四、比选申请人资格要求：**

1、在中华人民共和国境内依法注册的法人或者其他组织；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必须的设备和专业技术能力；

4、具有依法缴纳税收和社会保障资金的良好记录；

5、参加本次比选活动前三年内，在经营活动中没有重大违法记录；

6、比选申请人还符合法律、行政法规规定的其他强制性条件；

7、本项目不接受联合体参与。

**五、比选报名、比选文件领取时间、地点：**

比选报名及比选文件领取时间：自2023年5月26日至2023年5月30日上午9:00-12:00，下午13:00- 17:00（北京时间）

比选报名及比选申请文件递交地点：成都市成华区中医医院（成都市成华区长秀路133号）

比选报名及比选文件领取要求：本项目比选文件领取不收取费用。报名资格不得转让，否则视为无效。比选申请人参与报名登记时须持有效介绍信、营业执照或其他组织机构证明复印件、身份证复印件，并加盖公章

**六、比选时间和地点：**

**比选申请文件递交截止时间和比选时间：2023年5月31日10:00（北京时间）**

比选申请文件必须在比选截止时间前送达开标地点。逾期送达或没有密封的比选申请文件不予接收。本次比选不接受邮寄的比选申请文件。

**比选地点：成都市成华区中医医院（成都市成华区长秀路133号）**

**七、本项目网上发布地址：**

比选公告、变更、结果发布均在成都市成华区中医医院网站以公告形式发布。

**八、比选人的有关信息：**

**比选人：成都市成华区中医医院**

地址：成都市成华区长秀路133号

联系人：秦涛

联系电话：028-60828099

## 比选申请人须知

## 1、比选文件

比选申请人应仔细阅读本比选文件，按比选文件的规定和本比选文件第二章要求的格式编写比选申请书。

## 2、比选申请响应报价（实质性要求）

2.1所有报价一律以人民币报价。比选人不接受任何非人民币币种的报价。

2.2比选申请人的报价是其响应本项目要求的全部工作内容的价格体现，包括比选申请人完成本项目所需的一切费用。其中项目执行过程中产生的差旅费均包含在本次报价中。

## 3、比选申请书

3.1 比选申请书的编制

3.1.1 比选申请书的格式

比选申请书应按第二章“比选申请书格式”进行编写，至少包括“比选申请书格式”的各项内容。本比选文件要求提供的证明文件，比选申请人必须提供；本比选文件没有要求提供的证明文件，比选申请人认为需要提供的，也可以提供。

3.1.2 比选申请书应全部用不褪色的墨水（粉）书写或打印，不得有任何涂改。比选申请书副本应由正本复制而成（包括证明文件）。

3.1.3 比选申请书必须用中文书写，包括正本一份、副本一份。正本和副本的封面上应清楚的标记“正本”和“副本”的字样。正副本内容应完全一致，如不一致时，以正本为准。

3.2 比选申请书的签署

3.2.1比选申请人应在比选申请书封面加盖单位公章。

3.2.2 比选申请书的密封与标识

比选申请书的正本与副本应一起包装，比选申请书的外包装应保证其密封性。封套上应清楚地载明比选申请人的名称、项目名称。

3.2.3 未按以上要求密封和加写标记的比选申请书将不予受理。

3.3比选申请书的递交

比选申请书应该在比选邀请中规定的比选申请书提交截止时间前提交。迟到的比选申请书比选人将拒绝接收。

## 4、比选响应有效期（实质性要求）

4.1比选响应有效期为90天。

4.2 特殊情况下，比选人可于比选响应有效期满之前要求申请人同意延长有效期，要求与答复均应为书面形式。拒绝延长比选响应有效期的申请人不得再参与该项目后续比选活动。同意延长比选响应有效期的申请人不能修改其比选申请文件，关于保证金的有关规定在延长的比选响应有效期内继续有效。

4.3 在比选响应有效期内，比选申请人将依法接受其比选申请文件的约束。

## 5、评审

5.1 评审小组

评审工作由比选人组建的评审小组负责，评审小组成员人数为3人（含3人）以上单数。

5.2 比选活动在比选文件约定的地方进行。

5.3 比选程序

比选人在监督人员监督的情况下，在比选文件规定地点、时间当场开封所有比选申请书，按照以下程序进行：

5.3.1 对比选申请文件进行审查，剔除无效申请文件；

**有下列情况之一的视为无效比选申请文件，除此之外，评审小组不得再以不符合比选文件中规定的其他实质性要求来判定无效申请文件：**

a未按比选文件规定盖章或签字的；

b比选申请文件中的报价高于本项目预算或最高限价或未按比选文件规定进行报价的；

c比选申请文件不满足本项目实质性要求的。

5.3.2重新组织

本次比选活动中，出现下列情形之一的，予以重新组织：

（1）比选申请人少于3家的；

（2）出现影响比选公正的违法、违规行为的；

5.4 评审小组有权对比选申请书提出澄清，比选申请人应予以配合，若不予以配合的，比选申请书无效。

## 6、中选通知书发放

比选人将在结果公告发布后通知中选的比选申请人领取中选通知书。

## 7、合同签订（实质性要求）

7.1 中选通知书发出之日起30日内，比选人与中选人订立书面合同。

7.2 中选人与比选人签订合同后，合同双方应严格执行合同条款，履行合同规定的义务，保证合同的顺利完成。

# 第二章 资格证明文件

## 一、比选申请人应提交的资格证明材料

**（一）比选申请人资格和资质性要求的相关证明材料：**

1、在中华人民共和国境内依法注册的法人或者其他组织的证明材料（①比选申请人若为企业法人的，提供统一社会信用代码营业执照，未换证的企业也可同时提供营业执照、税务登记证、组织机构代码证；②比选申请人若为事业法人，提供统一社会信用代码法人登记证书，未换证的事业法人也可同时提交事业法人登记证书和组织机构代码证；③比选申请人若为其他组织，提供对应主管部门颁发的准许执业证明文件或营业执照。以上证件均提供复印件）

2、具有良好的商业信誉和健全的财务会计制度的证明材料可提供承诺函原件，格式详见第二章“承诺函”}。

3、具有依法缴纳税收和社会保障资金的良好记录的证明材料{可提供承诺函原件，格式详见第二章“承诺函”}。

4、具备履行合同所必需的设备和专业技术能力的证明材料（可提供承诺函原件，格式详见第二章“承诺函”）；

5、参加比选活动前三年内在经营活动中没有重大违法记录的证明材料（可提供承诺函原件，格式详见第二章“承诺函”）；

6、比选申请人还符合法律、行政法规规定的其他强制性条件。（可提供承诺函原件，格式详见第二章“承诺函”）

**（二）其他类似效力要求相关证明材料：**

1、非法定代表人参与比选并签署响应文件时，提供法定代表人授权书原件以及法定代表人和授权代表的身份证复印件（提供身份证有困难的，也可提供户口本或军官证或护照等身份证明材料）；

2、法定代表人直接参与比选并签署响应文件时，提供法定代表人证明书原件和法定代表人身份证复印件（提供身份证有困难的，也可提供户口本或军官证或护照等身份证明材料）。

注：

1、以上要求的资料复印件均必须加盖比选申请人单位的公章（鲜章）。

第三章 比选需求

**前提：本章中所有内容均为本项目的实质性要求条款，比选申请人不满足的，符合性审查时将不予通过，其比选申请文件将被否决。**

1、项目情况

本单位为了提升系统的安全保护能力、加强信息安全管理，根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》、《GB/T 22239-2019 网络安全技术信息系统安全等级保护基本要求》等法规和标准的要求，对所属的《HIS信息系统》、《医院信息集成平台》但不限于对指定系统进行开展网络安全等级保护测评工作，并配合医院对后期新上系统进行备案。

通过测评，准确反映待测信息系统的安全防护能力现状，分析排查所涉及信息系统的信息安全隐患，提出安全整改建议；同时提升系统安全防护能力，优化、加强系统信息安全管理，确保本单位网络安全建设工作满足国家法律法规、标准规范的要求，信息系统达到相应安全等级的防护水平。

2、项目依据

项目依据国家《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《信息安全等级保护管理办法》（公通字[2007]43号）、《中华人民共和国国家标准GB/T 22239-2019 信息安全技术信息系统安全等级保护基本要求》、《中华人民共和国国家标准信息安全技术信息系统安全等级保护测评要求》、《中华人民共和国国家标准信息安全技术信息系统安全等级保护测评过程指南》、《中华人民共和国国家标准GB/T 20984-2007信息安全风险评估规范》等法规要求进行网络安全等级保护测评项目。

3、项目内容

本次需要测评的系统包括被测系统运行密不可分的物理环境、网络环境、主机及相关系统、安全管理制度等。本项目中测评目的和测评内容，必须与信息安全等级保护要求的基本安全控制要求相一致。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 单位 | 数量 | 备注 |
| 1 | HIS系统和信息集成平台等级保护（三级）测评服务 | 个 | 1 | 测评及备案 |
| 2 | Lis系统等级保护（三级）  检测服务 | 个 | 1 | 仅安全检测 |
| 3 | EMR系统等级保护（三级）  检测服务 | 个 | 1 | 仅安全检测 |

**技术服务要求：**

3.1差距测评，至少包括：

安全技术测评。包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心方面的安全测评。

安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。

形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题以、整改意见。

3.2协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

3.3等级测评，至少包括：

按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。

编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。

3.4针对本院的LIS及EMR系统进行漏洞扫描，出具报告形成相关问题整改意见并协助完成漏洞整改工作。

## 3.5服务内容指标

### 三级系统通用指标要求

| **分类** | **子类** | **基本要求** |
| --- | --- | --- |
| 安全物理环境 | 物理位置选择 | a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内;  b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。 |
| 物理访问控制 | 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。 |
| 防盗窃和防破坏 | a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识;  b) 应将通信线缆铺设在隐蔽安全处。  c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。 |
| 防雷击 | a) 应将各类机柜、设施和设备等通过接地系统安全接地。  b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。 |
| 防火 | a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火;  b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料;  c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。 |
| 防水和防潮 | a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透;  b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透;  c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。 |
| 防静电 | a) 应采用防静电地板或地面并采用必要的接地防静电措施;  b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。 |
| 温湿度控制 | 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 |
| 电力供应 | a) 应在机房供电线路上配置稳压器和过电压防护设备;  b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求;  c）应设置冗余或并行的电力电缆线路为计算机系统供电。 |
| 电磁防护 | a) 电源线和通信线缆应隔离铺设，避免互相干扰;  b）应对关键设备实施电磁屏蔽。 |
| 安全通信网络 | 网络架构 | a) 应保证网络设备的业务处理能力满足业务高峰期需要;  b) 应保证网络各个部分的带宽满足业务高峰期需要;  c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址;  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 | 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，应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全区域边界 | 边界防护 | a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信;  b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制;  c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制;  d) 应限制无线网络的使用,保证无线网络通过受控的边界设备接入内部网络。 |
| 访问控制 | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信;  b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化;  c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出;  d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力;  e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 |
| 入侵防范 | a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为;  b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为;  c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析;  d) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 |
| 恶意代码和垃圾邮件防范 | a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新;  b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。 |
| 安全审计 | a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;  b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;  c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等;  d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。 |
| 可信验证 | 可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 安全计算环境 | 身份鉴别 | a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换;  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;  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来实现。 |
| 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，访间控制策略规定主体对客体的访问规则;  f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级;  g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。 |
| 安全审计 | a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计;  b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;  c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等;  d）应对审计进程进行保护，防止未经授权的中断。 |
| 入侵防范 | a) 应遵循最小安装的原则，仅安装需要的组件和应用程序;  b) 应关闭不需要的系统服务、默认共享和高危端口;  c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制;  d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求;  e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞;  f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 |
| 恶意代码防范 | 应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。 |
| 可信验证 | 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证， 并在应用程序的关键执行环节进行动态可信验证，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) 应采用校验技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等;  b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。 |
| 数据保密性 | a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等;  b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。 |
| 数据备份恢复 | a) 应提供重要数据的本地数据备份与恢复功能;  b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地;  c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。 |
| 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除;  b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。 |
| 个人信息保护 | a) 应仅采集和保存业务必需的用户个人信息;  b) 应禁止未授权访问和非法使用用户个人信息。 |
| 安全管理中心 | 系统管理 | a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计;  b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。 |
| 审计管理 | a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计;  b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |
| 安全管理 | a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计;  b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 |
| 集中管控 | a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控;  b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理;  c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测;  d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求;  e）应对安全策路、恶意代码、补丁升级等安全相关事项进行集中管理;  f）应能对网络中发生的各类安全事件进行识别、报警和分析。 |
| 安全管理制度 | 安全策略 | 应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。 |
| 管理制度 | a) 应对安全管理活动中的主要管理内容建立安全管理制度;  b) 应对管理人员或操作人员执行的日常管理操作建立操作规程;  c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。 |
| 制定和发布 | a) 应指定或授权专门的部门或人员负责安全管理制度的制定;  b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。 |
| 评审和修订 | 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 |
| 安全管理机构 | 岗位设置 | a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权;  b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责;  c）应设立系统管理员、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 | a）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;  b) 应配备专职安全管理员，不可兼任。 |
| 授权和审批 | a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等;  b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度;  c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。 |
| 沟通和合作 | a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题;  b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通;  c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 |
| 审核和检查 | a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况;  b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等;  c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。 |
| 安全管理人员 | 人员录用 | a) 应指定或授权专门的部门或人员负责人员录用;  b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核;  c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 |
| 人员离岗 | a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备;  b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。 |
| 安全意识教育和培训 | a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施;  b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训;  c）应定期对不同岗位的人员进行技能考核。 |
| 外部人员访问管理 | a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案;  b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案;  c) 外部人员离场后应及时清除其所有的访问权限;  d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。 |
| 安全建设管理 | 定级和备案 | a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由;  b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定;  c) 应保证定级结果经过相关部门的批准;  d) 应将备案材料报主管部门和相应公安机关备案。 |
| 安全方案设计 | a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施;  b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，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;  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，并定期审定和更新候选产品名单。 |
| 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门和隐蔽信道。 |
| 工程实施 | a) 应指定或授权专门的部门或人员负责工程实施过程的管理;  b) 应制定安全工程实施方案控制工程实施过程;  c）应通过第三方工程监理控制项目的实施过程。 |
| 测试验收 | a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告;  b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 |
| 系统交付 | a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点;  b) 应对负责运行维护的技术人员进行相应的技能培训;  c) 应提供建设过程文档和运行维护文档。 |
| 等级测评 | a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改;  b) 应在发生重大变更或级别发生变化时进行等级测评;  c) 应确保测评机构的选择符合国家有关规定。 |
| 服务供应商选择 | a) 应确保服务供应商的选择符合国家的有关规定;  b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务;  c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。 |
| 安全运维管理 | 环境管理 | a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理;  b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定;  c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。 |
| 资产管理 | a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容;  b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施;  c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。 |
| 介质管理 | a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点;  b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 |
| 设备维护管理 | a) 应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理;  b) 应对配套设施、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;  c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密;  d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。 |
| 漏洞和风险管理 | a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补;  b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。 |
| 网络和系统安全管理 | a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限;  b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制;  c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定;  d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等;  e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容;  f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为;  g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库;  h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据;  i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道;  j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。 |
| 恶意代码防范管理 | a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等;  b）应定期验证防范恶意代码攻击的技术措施的有效性。 |
| 配置管理 | a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和 补丁信息、各个设备或软件组件的配置参数等;  b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 |
| 密码管理 | a) 应遵循密码相关国家标准和行业标准;  b) 应使用国家密码管理主管部门认证核准的密码技术和产品。 |
| 变更管理 | a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施;  b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程;  c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。 |
| 备份与恢复管理 | a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等;  b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等;  c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。 |
| 安全事件处置 | a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件;  b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等;  c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训;  d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。 |
| 应急预案管理 | a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容;  b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容;  c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练;  d）应定期对原有的应急预案重新评估，修订完善。 |
| 外包运维管理 | a) 应确保外包运维服务商的选择符合国家的有关规定;  b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容;  c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确;  d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。 |

## 4.1完成项目所需提交的文档清单

在本项目完成后，服务方须提供以下文档资料：

* 《信息系统安全问题汇总及整改建议》
* 《网络安全等级保护等级测评报告》及过程资料

## 4.2技术标准和规范

* 《中华人民共和国计算机信息系统安全保护条例》(国务院令147号)
* 《信息安全等级保护管理办法》
* 《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定级指南》（GB/T22240-2020）
* 《信息系统安全等级保护基本要求》（GB/T22239-2019）
* 《信息系统安全等级保护测评要求》（GB/T28448-2019）
* 《信息系统安全等级保护测评过程指南》（GB/T28449-2018）

## 4.3安全要求

成交供应商在项目实施过程中，必须遵守以下技术原则：

4.3.1保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购方的行为，否则采购方有权追究供应商的责任。

4.3.2 标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

4.3.3 规范性原则：供应商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制，测评出具的报告须符合公安部颁布的《信息系统安全等级测评报告模板》。

4.3.4 可控性原则：等保测评服务的进度要按照招标文件 的要求，保证采购方对于测评工作的可控性。

4.3.5 整体性原则：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。

4.3.6安全性原则：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得对现有信息系统的正常运行、业务的正常开展产生任何影响。

4.3.7.测评机构资质及人员要求：

从事信息系统检测评估相关工作人员无违法记录。

工作人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。

测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。

## 5.商务及其他要求

5.1服务地点：成都市成华区长秀路133号，成华区中医医院。

5.2服务时间：签订合同后30天完成等保测评及备案（不含整改时间）。

5.3付款方式：签订合同收到合法发票后5个工作日支付10%的合同款项，出具整改建议10个工作日支付30%的合同款项，出具等保测评报告经验收合格后10个工作日支付60%的合同款项。

5.4质量保证及售后服务

5.4.1供应商在测评期间对系统进行检查、诊断，即使发现问题隐患，通过系统调整等手段，保持系统稳定、高效的运行

成交供应商和制造商应当为医院提供技术援助电话，解答医院在使用中遇到的问题，及时为医院提出解决问题的建议。

5.5.2现场响应

医院遇到使用及技术问题，电话咨询不能解决的，成交供应商或制造商应在12小时内采取相应响应措施；无法在12小时内解决的，应在48小时内派出专业人员进行技术支持。

5.5.3技术升级

在质保期内，如果成交供应商和制造商的产品技术升级，成交供应商应及时通知医院，如医院有相应要求，成交供应商和制造商应对医院进行升级服务。

5.5.4质保期外服务要求

质量保证期过后，成交供应商和制造商应同样提供免费电话咨询服务，并应承诺提供产品上门维护服务。

质量保证期过后，医院需要继续由原成交供应商和制造商提供售后服务的，成交供应商和制造商应以优惠价格提供售后服务。

5.5.5备品备件及易损件

供应商和制造商售后服务中，维修使用的备品备件及易损件应为原厂配件，未经医院同意不得使用非原厂配件，常用的、容易损坏的备品备件及易损件的价格清单须在响应文件中列出。

6.验收

（1）按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）的要求进行验收，验收标准以合同、比选文件及响应文件的约定及要求、相关法律法规的规定和国家（行业）标准为准。

7.其他：未尽事宜在合同中约定。

第四章 评审办法

## 1、总则

1.1比选人将根据比选特点组建评审小组，采取综合评分法。

1.2 评审工作应遵循公平、公正、科学及择优的原则，并以相同的评审程序和标准对待所有的比选申请人。

1.3 评审小组按照比选文件规定的评审方法和标准进行评审，并独立履行下列职责：

（1）审查比选申请文件是否符合比选文件要求，并作出评价；

（2）要求比选申请人对比选申请文件有关事项作出解释或者澄清；

（3）推荐中选候选人名单；

（4）向比选人或者有关部门报告非法干预评审工作的行为。

## 2、评审程序

2.1比选申请文件初审。初审分为资格性检查和符合性检查。

2.1.1资格性检查。依据法律法规和比选文件的规定，对比选申请文件中的第三章资格证明进行审查，以确定比选申请人具备比选资格。

|  |  |  |
| --- | --- | --- |
| 序号 | 资格性检查内容 | 通过/不通过 |
|  | 在中华人民共和国境内依法注册的法人或者其他组织的证明材料 |  |
|  | 具有良好的商业信誉和健全的财务会计制度的证明材料 |  |
|  | 具有依法缴纳税收和社会保障资金的良好记录的证明材料 |  |
|  | 具备履行合同所必需的设备和专业技术能力的证明材料 |  |
|  | 参加比选活动前三年内在经营活动中没有重大违法记录的证明材料 |  |
|  | 比选申请人还符合法律、行政法规规定的其他强制性条件 |  |
|  | 非法定代表人参与比选并签署响应文件时，提供法定代表人授权书原件以及法定代表人和授权代表的身份证复印件 |  |
|  | 法定代表人直接参与比选并签署响应文件时，提供法定代表人证明书原件和法定代表人身份证复印件 |  |

2.1.2符合性检查。从比选申请文件的有效性、完整性和对比选文件的响应程度进行审查，以确定是否对比选文件的实质性要求作出响应，不满足的作无效响应处理。

|  |  |  |
| --- | --- | --- |
| 序号 | 符合性检查内容 | 通过/不通过 |
|  | 未按比选文件规定盖章或签字的 |  |
|  | 比选申请文件中的报价高于本项目预算或最高限价或未按比选文件规定进行报价的 |  |
|  | 比选申请文件不满足本项目实质性要求的 |  |
|  | 发现在比选过程中有弄虚作假情形的 |  |

2.2澄清有关问题。对比选申请文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评审小组可以书面形式（应当由评审小组专家签字）要求比选申请人作出必要的澄清、说明或者纠正。比选申请人的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，并不得超出比选申请文件的范围或者改变比选申请文件的实质性内容。

2.3比较与评价。按比选文件中规定的评审方法和标准，对资格性检查和符合性检查合格的比选申请文件进行商务和技术评估，综合比较与评价。

2.4推荐中选候选人名单。中选候选人比选人需要确定，但必须按顺序排列中选候选人。

2.5编写评审报告。评审报告是评审小组根据全体评审成员签字的原始评审记录和评审结果编写的报告。

## 3、定标及定标程序

3.1 评审小组将评审情况写出书面报告，并按比选申请人综合得分由高到低的顺序推荐不少于3家（含3家）中选候选人。

3.2 比选人按照推荐的中选候选人顺序确定中选人，不能认为比选人只能确定第一中选候选人为中选人，比选人有正当理由的，可以确定后一顺序中选候选人为中选人，依次类推。

3.3 根据比选人确定的中选人，向中选人发出中选通知书。

3.4 比选人不解释中选或落选原因，不退回比选申请文件和其他资料。

## 4、评审细则及标准（综合评分法）

4.1 综合评分明细表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **评分**  **因素** | **分值** | **评分依据** | **备注** |
| 1 | 报价20% | 20分 | 以本次最低有效比选报价为基准价，报价得分=(基准价／比选报价)×20。 |  |
| 2 | 技术能力22% | 10分 | 技术方案：  1.安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个方面  2.安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维管理等五个大方面  以上共十大测评项，全部满足得10分，缺少一项或不适用于本项目得扣1分 |  |
| 3 | 12分 | 实施能力：  根据供应商提供得技术手段工具配置情况进行打分：  1.供应商具有等保检测工具箱1套得1分。  2.供应商具有一体化评估平台1套得1分。  3.供应商拥有自研网络安全等保测评信息管理系统软件著作权得2分。  4.供应商拥有随机数检测工具系统软件著作权得2分。  5.供应商拥有网络安全漏洞扫描安全系统著作权得2分。  6.供应商拥有网络信息安全检查监管系统软件著作权得2分。  7.供应商拥有网络安全数据后台实时监控软件著作权得2分 | 注：测评工具提供工具购买发票凭证复印件、并加盖公章。软件著作权提供中华人民共和国国家版权局颁发得著作权登记证书复印件并加盖公章。提供复印件加盖供应商公章 |
| 4 | 测评团队能力要求  48% | 21分 | 项目总测评师：  供应商为本项目配备的总测评师网络安全等级测评是高级证书得3分，此项最多3分。  1.2项目总测评师同时具有互联网安全评估师高级证书（CIISA)、信息安全工程师（软考类）、国家重要信息系统保护人员证书得（CIIPT）、商用密码应用安全性评估人员能力合格证书、系统架构师（高级）、实验室质量管理师证书全部满足得18分，缺少一项扣3分。 |  |
| 5 | 12分 | 项目经理  2.1项目经理具有信息安全等级测评师高级证书得2分。  2.22.2项目经理同时具有注册信息安全专业人员证书（CISP)、网络工程师（高级）、软件性能测评师高级、系统架构师、信息安全保障人员认证证书(CISAW)-风险管理（专业级）全部满足得10分，缺少一项扣2分。 | 1.拟配人员需提供属于本单位人员的证明材料；  2.提供证书复印件加盖供应商单位公章；  3.拟派项目组负责人与现场测评经理不得兼任；  4.测评人员款项中拟派的其余人员，同一人员拥有多个证书的以最高单项积分，不累加得分。 |
| 6 | 15分 | 测评人员：  供应商为本项目拟派的其余人员具有以下资质：具有互联网安全评估师证书（CIISA)得3分，具有商用密码应用安全性评估人员能力合格证书得3分，具有国家重要信息系统保护人员证书（CIIP-A)得3分，具有信息安全保障人员认证证书(CISAW)得3分，具有注册网络安全渗透评估专业人员证书(NSATP-A)得3分。 |  |
| 7 | 履约经验10% | 10分 | 供应商自2020年1月1日至今每有一个等保测评相关案例得2分，最多得10分。 | 提供合同复印件加盖公章 |

注： 评分的取值按四舍五入法，保留小数点后两位。

## 5、计算错误的修改

5.1 比选申请文件中如果出现计算上或累加上的算术错误，可按以下原则进行修改：

（1）用数字表示的金额和用文字表示的金额不一致，应以文字表示的金额为准。

（2）单价和数量的乘积与总价不一致时，以单价为准，并修正总价。

（3）单价金额小数点有明显错误的，以总价为准，修正单价。

5.2 按上述修正错误的方法调整的比选报价应对比选申请人具有约束力。如果比选申请人不接受修正后的价格，其比选将被拒绝。

## 6、评审专家在比选评审活动中承担以下义务：

6.1 遵纪守法，客观、公正、廉洁地履行职责。

6.2 按照比选文件的规定要求对比选申请人的资格条件和比选申请人提供的产品价格、技术、服务等方面严格进行评判，提供科学合理、公平公正的评审意见，参与起草评审报告，并予签字确认。

6.3 保守秘密。不得透露比选文件咨询情况，不得泄漏比选申请人的比选申请文件及知悉的商业秘密，不得向比选申请人透露评审情况。

# 第六章 采购合同（样例）

一、定义

（一）甲方（需方）即重庆医科大学附属永川医院。

（二）乙方（供方）即成交供应商，是指成交后提供合同货物和服务的自然人、法人及其他组织。

（三）合同是指由甲乙双方按照比选文件和响应文件的实质性内容，通过协商一致达成的书面协议。

（四）合同价格指以成交价格为依据，在供方全面履行合同义务后，需方应支付给供方的金额。

（五）技术资料是指合同货物及其相关的设计、制造、监造、检验、验收等文件（包括图纸、各种文字说明、标准）。

二、货物内容

合同包括以下内容：货物名称、型号规格、技术参数、数量（单位）等内容。

三、合同价格

（一）合同价格即合同总价。

（二）合同价格包括合同货物、技术资料、合同货物的税费、运杂费、保险费、包装费、装卸费及与货物有关的供方应纳的税费，所有税费由乙方负担。

（三）合同货物单价为不变价。

四、转包或分包

（一）本合同范围的货物，应由乙方直接供应，不得转让他人供应；

（二）非经甲方书面同意，乙方不得将本合同范围的货物全部或部分分包给他人供应；

（三）如有转让和未经甲方同意的分包行为，甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

五、质量保证及售后服务

（一）乙方应按比选文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

（二）乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

1、更换：由乙方承担所发生的全部费用。

2、贬值处理：由甲乙双方合议定价。

3、退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

（三）如在使用过程中发生质量问题，乙方应同本项目“第四篇 比选项目服务需求”对质量保证及售后服务内容的约定。

（四）在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

六、付款

（一）本合同使用货币币制如未作特别说明均为人民币。

（二）付款方式：银行转账。

（三）付款方法：同本项目“第三篇 项目商务要求”中关于付款方式的约定。

七、检查验收

（一）供方应随货物提供合格证和质量证明文件，如是国外进口的货物还须提供入关证明。

（二）货物验收

供方所交货物的各种质量指标不得低于供方提供样品的质量指标（无样品时按供方响应文件中所提供的“技术文件”执行），售后服务质量要求按照比选文件和响应文件的内容执行。供方交货时，需方可根据需要随机抽取一部分货物送有关权威检测部门检测，如检测不合格，供方负责赔偿需方一切损失。

（三）货物验收报告应由需方、供方经办人签字，以此作为支付凭据。

八、索赔

供方对货物与合同要求不符负有责任，并且需方已于规定交货内和质量保证期内提出索赔，供方应按需方同意的下述一种或多种方法解决索赔事宜。

（一）供方同意需方拒收货物并把拒收货物的金额以合同规定的同类货币付给需方，供方负担发生的一切损失和费用，包括利息、运输和保险费、检验费、仓储和装卸费以及为保管和保护被拒绝货物所需要的其它必要费用。

（二）根据货物的疵劣和受损程度以及需方遭受损失的金额，经双方同意降低货物价格。

九、知识产权

（一）甲方在中华人民共和国境内使用乙方提供的货物及服务时免受第三方提出的侵犯其专利权或其它知识产权的起诉。如果第三方提出侵权指控，乙方承担由此而引起的一切法律责任和费用。

（二）若涉及软件开发等服务类项目知识产权的，知识产权归医院所有。

十、合同争议的解决

（一）当事人友好协商达成一致

（二）在60天内当事人协商不能达成协议的，可提请医院当地仲裁机构仲裁。

十一、违约责任

按《中华人民共和国民法典》有关条款，或由供需双方约定。

十二、合同生效及其它

（一）合同生效及其效力应符合《中华人民共和国民法典》有关规定。

（二）合同应经当事人法定代表人或委托代理人签字，加盖双方合同专用章或公章。

（三）合同所包括附件，是合同不可分割的一部分，具有同等法法律效力。

（四）合同需提供担保的，按《中华人民共和国担保法》规定执行。

（五）本合同条件未尽事宜依照《中华人民共和国民法典》，由供需双方共同协商确定。

# 第七章 比选申请书模板

1、比选申请人在编制比选申请书时应使用本章所附格式并符合有关要求；本章未规定格式的，由比选申请人根据实际情况自主编制。

2、比选申请书应在比选申请书封面和《法定代表人授权书》中的“比选申请人”一栏填上比选申请人的全称并在名称上加盖比选申请人单位章。

3、比选申请书中的表格或空格如填写不下，可编辑扩充或另附页。除形式外，比选申请人不得改变其内容要求。本章所附格式，比选申请人为编制比选申请书可以复印或编辑。

4、比选申请人应按照比选申请书格式的要求编制比选申请书。比选申请书密封后按规定的时间和地点提交。

**XX项目**

**比**

**选**

**申**

**请**

**书**

**比选申请人：（全称并加盖单位公章）**

**X年X月X日**

## 1、法定代表人/单位负责人授权书

**（适用于非法定代表人直接参与）**

本授权委托书声明：我（姓名）系（比选申请人名称）的法定代表人，现授权（姓名）为我单位委托代理人，以本单位的名义参加（项目名称）的比选活动。委托代理人在比选活动的合法代表，以我方名义全权处理该项目有关比选、签订合同以及执行合同等一切事宜。

委托代理人无转委托权。特此委托。

授权人(法定代表人):（签字）联系电话：

委托代理人：（签字）手机：

委托代理人部门：职务：

单位电话：传真：

比选申请人：（全称并加盖公章）

日期：年 月 日

（须附法定代表人和授权代表身份证复印件）

## 法定代表人/单位负责人证明书

**（适用于法定代表人/单位负责人直接参与）**

比选申请人单位名称：

单位性质：

成立时间：年月日

经营期限：

姓名：性别：年龄：职务：

系（比选申请人名称）的法定代表人/单位负责人。

特此证明。

比选申请人：（单位公章） 。

日 期： 。

**注：1、比选申请人为法人单位时提供“法定代表人证明书”，比选申请人为其他组织时提供“单位负责人证明书”。**

**2、法定代表人/单位负责人直接参与比选并签署响应文件时才须提供；**

**3、应附法定代表人/单位负责人身份证（正反面）复印件；（提供身份证有困难的，也可提供户口本或军官证或护照等身份证明材料）**

**2、商务应答表**

项目名称：

项目编号：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 产品名称 | 比选要求  技术参数 | 供应  技术参数 | 差异或响应 | 差异说明 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：1、应对技术方案中的所有条款进行逐一应答，还需在“比选文件对应页码”栏内写明技术支持文件的页码。

2、若无差异，请在“响应或差异”处填写响应。

3、若有差异，请在“响应或差异”处填写差异，技术参数优于比选文件要求的在“差异原因”处填写正偏离；相应技术参数低于比选文件要求的在“差异原因”处填写负偏离。

|  |  |
| --- | --- |
| 供应商全称 |  |
| 供应商投报总价  （人民币） | 大写： 小写： |
| 备注： | |

2.1报价表

**注：** 1.实行一次性报价。

比选申请人： （加盖公章）

法定代表人或授权代表：

日 期： 年 月 日

2.2分项报价明细表

项目名称：

采购项目编号：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目名称 | 制造商名称 | 数量 | 单价（元） | 小计（元） |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 合计  （人民币） |  | | | |

供应商： 供应商法人授权代表：（公章）

（签名） 年 月 日

## 3、承诺函

致成都市成华区中医医院：

本公司（公司名称）参加（项目名称）（比选编号）的比选活动，特别针对以下条款，郑重承诺：

1、在中华人民共和国境内依法注册的法人或者其他组织；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必须的设备和专业技术能力；

4、具有依法缴纳税收和社会保障资金的良好记录；

5、参加本次比选活动前三年内，在经营活动中没有重大违法记录；

6、比选申请人还符合法律、行政法规规定的其他强制性条件；

7、我方完全同意比选文件第一章比选申请人须知中关于“比选报价”、“比选响应有效期”、“合同签订”的实质性要求，并承诺严格按照比选文件要求履行。

本单位对上述承诺的内容事项真实性负责。如经查实上述承诺的内容事项存在虚假，我单位愿意接受以提供虚假材料谋取中选追究法律责任。

如违反以上承诺，本公司愿承担一切法律责任。

比选申请人名称：（盖章）

法定代表人或授权代表（签字）：

比选日期：X年X月X日

注：1.可自行提供具有有效签字和盖章的格式，但承诺函的内容至少应该包含本格式中涉及的承诺内容。

## 4、营业执照或其他组织的证明材料

## 5、比选申请人认为可提供的其他证明材料

**（服务方案）比选评分表要求提供的内容**

1.定级备案服务方案

2.测评实施方案

3.项目负责结构（人员安排）

4.应急处置预案

5.售后服务方案

（格式自拟）

**附件1递交响应文件签收表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **递交比选文件签收表** | | | | | |
| **项目名称：** |  | | | **比选编号：** |  |
| **比选时间：** |  | | | **比选地点：** |  |
| **包号** | **比选申请人** | **递交时间** | **密封合格与否**  **（签收人确认）** | **联系人** | **联系方式** |
|  |  | 年 月 日  时 分 | □是  □否 |  | 电话： |
| 传真： |
| 手机： |
|  |
| 签收人： |  | | | | |
| 备注：本递交表一式两份，接收人签字后生效，由递交人和接收人各执一份。请以正楷字填写，各项目内容，“递交时间”、“联系人”、请在现场签收时填写。 | | | | | |