**四川省严重精神障碍综合信息管理平台**

**2023年等级保护测评服务**

**招标文件**

四川省精神医学中心

1. **投标须知**
2. 1招标概况：

为了落实公安部、网信办应用系统安全等级保护要求，进一步增强系统安全防护能力，确保系统安全稳定运行，防止因系统安全事件引发安全事故，依据《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全等级保护管理办法》（公通字[2007]43号）和《中华人民共和国网络安全法》等标准规范，我中心拟开展2023年度四川省严重精神障碍综合信息管理平台等级保护三级测评工作。

本次安全等级保护测评服务范围为以下信息系统：

|  |  |
| --- | --- |
| 信息系统名称 | 定级 |
| 四川省严重精神障碍综合管理信息系统 | 3级 |

甲方：四川省精神医学中心

乙方：投标单位

欢迎有资质、有能力的供应商前来参与投标。

1.2 投标单位要求：

1.2.1 在中华人民共和国境内注册，具有独立法人资格；

1.2.2 具有良好的商业信誉和健全的财务会计制度；

1.2.3 具备履行合同所必需的设备和专业技术能力的证明材料；

1.2.4 参加采购活动前三年内，在经营活动中没有重大违法记录；

1.3质量要求：

1.3.1按国家有关规定、采购文件的技术参数、商务要求和供应商的响应文件及承诺以及合同约定标准进行验收。

1.4服务要求：投标人的服务承诺应按不低于招标文件中提出的所有服务要求的标准做出响应。其基本服务要求如下：

1.4.1符合本招标文件及招标人承诺的质量、技术和其他要求，符合国家相关的质量标准和出厂标准。

1.5 招标文件获取方式：登陆四川省精神医学中心官网（http://www.scsjsyxzx.com/),进入四川省精神医学中心门户网站，免费下载招标文件。

1.6 招标文件获取时间：发布招标公告之时起至2023.9.8。

1.7 投标文件递交时间：2023.9.8 17:00截止。

1.8 投标文件递交方式：密封装订，现场递交。

1.9项目限价： 5万元 。报价不得超过限价，报价应包含完成本次项目一切含税费用。

1.10签订合同以甲方版本为准。

1.11本文件规定外，招标人在招标期间发出的其他补充函件或文件修改均是招标文件的重要组成，对投标人起到约束作用。

1.12 投标人质疑：针对招标文件技术条款和专业商务条件的质疑由投标人于获取采购文件截止日期前书面向招标人提出，并由四川省精神医学中心受理和回复，投标人对招标文件提出质疑的，应在法定期限内，逾期不予受理。

地址：四川省成都市温江区芙蓉大道二段33号

电话：028-81020254

1. **投标要求**

2.1招标内容：详见投标须知；

2.2招标规格及数量：详见投标须知；

2.3投标要求：详见投标须知；

2.4技术要求：详见招标文件技术部分；

2.5供货要求：详见投标须知；

2.6其他约定：

2.6.1不论招标结果如何，投标人的投标文件不退回，且不对投标人作任何解释；

2.6.2投标产生的一切费用由投标人自行承担；

1. **投标文件的编制**

3.1投标文件的语言：招标人和投标人之间的所有函件往来必须使用汉语语言文字。

3.2投标文件的组成（部分文件要求及格式见附件）：

3.2.1 评标要素索引表

3.2.2 资格要求的响应

3.2.2 技术参数的响应

3.2.3 商务要求的响应

（投标文件每页资料必须逐页加盖公司鲜章）

3.4 投标文件正本一份，副本两份。

1. **招标、评选与中标通知书**

4.1.有下列情况之一都将被视为无效投标：

4.1.1投标文件未按照投标文件的要求编制。

4.1.2投标文件中的资料未加盖投标单位的公章。

4.1.3报价若高于限价报价作无效报价处理。

4.1.4**投标文件封面未按投标文件封面要求编制和封贴。**

4.2评标办法及标准：

4.2.1按照文件规定，只对确定为符合文件的资质要求且实质上响应文件要求的参选文件进行评价和比较。

4.2.2通过资格审查、技术部分和商务部分审查后，评审小组按照综合评分法确定成交人。**合格供应商不足三家，予以废标。**

4.2.3 发生评标委员会推荐排名第一供应商主动放弃中标、被质疑或举报等情况的，参照《关于采购人是否有权顺延确定中标或者成交供应商等问题的函》（财库便函〔2019〕154号）处理。

1. **资格要求、技术参数、商务要求**

注意：本章采购需求中标注“▲”号的条款为本次采购项目的实质性要求，投标人应全部满足。

**5.1资格要求**

5.1.1营业执照：①投标人若为企业法人：提供“统一社会信用代码营业执照”；②若为事业法人：提供“统一社会信用代码法人登记证书”；③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”；④投标人若为自然人：提供“身份证明材料”。以上均提供复印件。

5.1.2体现健全的财务制度的证明材料：①可提供2020-2022年度（任意一年）经审计的财务报告复印件（包含审计报告和审计报告中所涉及的财务报表和报表附注）；②也可提供2020-2022年度（任意一年）投标人内部的财务报表复印件（至少包含资产负债表）；③也可提供距文件递交截止日一年内银行出具的资信证明（复印件）；④投标人注册时间至文件递交截止日不足一年的，也可提供在工商备案的公司章程（复印件）；⑤非营利性单位或者社会团体或者其他机关事业单位以符合财务会计制度为准或者提供承诺函（格式自拟）；⑥供应商为自然人的提供承诺函（格式自拟）。

5.1.3提供投标人单位及其现任法定代表人、主要负责人在参加政府采购活动前三年内无行贿犯罪记录的承诺函（注：如经核实属虚假承诺的，将做无效投标处理）。

5.1.4投标人须提供依法缴纳税收和社会保障资金的承诺函原件或者近三个月依法缴纳税收和社会保障资金的证明材料复印件。

5.1.5法定代表人身份证复印件。

5.1.6法定代表人授权书（格式4）原件和授权代表身份证复印件（投标人代表为非法定代表人时提供）。

▲**5.2技术需求**

5.2.1测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度等基本要求，以及云计算安全、移动互联安全、物联网安全、工控制系统安全等扩展方面的要求。

5.2.2服务内容位协助业主单位进行信息系统的信息安全等级测评、定级和备案工作，具体内容如下：

5.2.2.1差距测评：

（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、安全管理中心方面的安全测评。

（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五个方面的安全测评。

5.2.2.2汇总差距测评结果并形成整改报告：

（1）依据差距测评结果，对差距测评结果进行汇总统计，包括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等；

（2）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；

（3）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；

（4）根据主要问题提出整改意见，制作整改意见报告。

5.2.2.3根据整改意见报告，协助业主单位完成整改工作，在安全整改全过程提供技术咨询服务；

5.2.2.4编制《网络安全等级测评报告》；

5.2.2.5协助业主单位将《网络安全等级测评报告》提交相关部门备案。

5.2.3在本项目完成后，服务方须提供以下文档资料：

5.2.3.1《信息系统安全问题汇总及整改建议》；

5.2.3.2《网络安全等级保护等级测评报告》及过程资料。

5.2.4测评内容与基本要求

| 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。 |

▲**5.3 商务要求**

**5.3.1服务期及地点：**

**5.3.1.1 服务期限：**合同签订后5个工作日内进场开始测评工作，本项目须于2023年12月31日前完成。

**5.3.1.2 服务地点**：采购人指定地点。

**5.3.2.付款方式**：投标人完成初次测评后，投标人对招标人提供的《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》及过程资料进行验收，验收合格后支付合同金额的100%，系统测评合格并于2023年12月31日前在公安部门完成备案可直接视为项目验收合格。

**5.3.3.履约保障金：**无。

**5.3.4验收标准：**按国家有关规定、《财政部关于进一步加强政府采购需求和履行验收管理的指导意见》（财库〔2016〕205号）文件、招标文件要求、投标人的投标文件及有关承诺以及合同约定标准进行验收。本项目主要预期成果为“四川省严重精神障碍综合管理信息系统”通过等级保护测评（三级），在2023年12月31日前取得符合要求的《信息系统安全等级保护备案证明》即可视为验收合格。

**5.3.5** **培训要求：**投标人结合本项目及招标人实际需要，提供技术培训方案。

**5.3.6 需满足的技术标准和规范：**

5.3.6.1《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)

5.3.6.2《信息安全等级保护管理办法》（公通字[2007]43号

5.3.6.3《计算机信息系统安全保护等级划分准则》（GB17859-1999）

5.3.6.4《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）

5.3.6.5《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019)

5.3.6.6《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）

5.3.6.7《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）

5.3.6.8《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）

5.3.6.9《信息安全技术信息安全风险评估规范》（GB/T20984-2015）

5.3.6.10《中华人民共和国网络安全法》

**5.3.7 需遵守的技术原则：**

5.3.7.1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。

5.3.7.2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。

5.3.7.3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》。

5.3.7.4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。

5.3.7.5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。

5.3.7.6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。

5.3.7.7测评机构资质及人员要求：

（1）从事信息系统检测评估相关工作人员无违法记录；

（2）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；

（3）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。

1. **评分标准表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **评分因素及权重** | **分　值** | | **评分标准** | **说 明** |
| 1 | 报价23% | 23分 | | 以满足招标文件要求且投标价格最低的投标报价作为基准价，其余投标报价得分=（基准价／投标报价）×23×100%。  (保留小数点后两位，第三位四舍五入) |  |
| 2 | 履约能力20% | 质量体系 | 10分 | 1.供应商通过质量体系认证，且认证范围包括“信息安全等级保护测试评估服务”得2分；  2.供应商通过信息安全管理系统认证，且认证范围包括“信息安全等级保护测试评估服务”得2分；  3.供应商通过环境管理体系认证，且认证范围包括“信息安全等级保护测试评估服务”得2分；  4.供应商通过职业健康安全管理系统认证，且认证范围包括“信息安全等级保护测试评估服务”得2分；  5.具有省级及以上质量技术监督部门颁发的检验检测机构资质认定证书（CMA）或中国合格评定国家认可委员会（CNAS）颁发的实验室认可证书得2分  注：认证范围不符合，不得分。 | 资质或资格证书加盖投标人公章，没有或不提供，不得分。 |
| 3 | 履约经验 | 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1分，最多得10分。 | 提供相关合同复印件或授权书加盖投标人公章。 |
| 4 | 测评团队能力要求44% | 项目总测评师 | 14分 | 供应商为本项目配备的总测评师网络安全等级测评师高级证书同时具备以下证书：  a.具有互联网安全评估师高级证书（CIISA）  b.计算机技术与软件专业资格信息安全工程师（软考类）、  c.国家重要信息系统保护人员证书的（CIIP-A）  d.商用密码应用安全性评估人员能力合格证书  e.系统架构师（高级）  f.网络信息安全工程证书  g.网络安全管理（I级）  全部满足得14分，缺少一项扣2分 | ①拟配人员需提供本单位投标截止前连续三个月社保证明材料；  ②提供证书复印件并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；  ④3.1款中拟派的其余测评人员，同一人拥有多个证书的以最高单项计分，不累加得分。 |
| 项目经理 | 14分 | 项目经理具有信息安全等级测评师高级证书同时具备以下证书：  a.注册信息安全专业人员证书（CISP）  b.信息安全保障人员认证证书（CISAW）认证方向：风险管理（专业级）  c.注册云安全系统认证专家 (CCSSP)  d.网络工程师（高级）  f.软件性能测评师高级  e.系统架构师（高级）  g.国家重要信息系统保护人员证书（CIIP-A）  全部满足得14分，缺少一项扣2分。 |
| 测评人员 | 16分 | 供应商为本项目拟派的其余测评人员具有以下资质：  a.互联网安全评估师证书（CIISA）  b.商用密码应用安全性评估人员能力合格证书  c.国家重要信息系统保护人员证书（CIIP-A）  d.信息系统审计师证书（ISA）  e.具有国家网络安全应用检测专业测评人员证书（NSATP-A）  f.网络信息安全工程证书  g.网络安全技术（I级）  h.注册渗透测试专家（CISP-PTS）  全部满足得16分，缺少一项扣2分，同一种证书不重复计分。 |
| 5 | 技术能力13% | 技术方案 | 5分 | a.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；  b.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方面；  以上共有十大测评项，全部满足得5分，缺少一项扣0.5分。 |  |
| 实施能力 | 8分 | 根据供应商提供的技术手段工具配置情况进行打分：  a.等保检测专用工具箱  b.一体化评估平台  c.网络安全等保测评信息管理系统  d.随机数检测工具系统得  e.网络安全漏洞扫描安全系统  f.网络信息安全检查监管系统  g.网络安全数据后台实时监控软件  h.网络安全密码测评数据分析系统  全部满足得8分，缺少一项扣1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的著作权登记证书复印件并加盖公章。 |

**第七部分 联系方式**

5.1采购联系人：何老师028-81020254

5.2技术联系人：王老师028-81020070

5.3纪检联系人：孙老师028-81020036

附件1

**报价单**

我单位作为投标人,对此次招标活动中我方所承诺的条款已经完全明确,也深知所承诺的事项和作出的报价可能给我方带来的风险和后果。如果我方在招标活动中有弄虚作假等违法违规行为，以及中选后因报价低或不执行承诺条款而不履约,本单位愿承担一切责任（包括赔偿损失、取消招标及中选资格等），我单位报价为：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 报价内容 | 规格 | 数量 | 单价（元） | 备注 |
| 1 |  |  |  |  | 按实际情况可调整表格 |
| 2 | ....... |  |  |  |  |
| 最终报价金额**合计（含税）**： 元  （大写： 仟 佰 拾 万 仟 佰 拾 元 角 分 ） | | | | | |

报价单格式可根据实际自行调整

附件2

法定代表人授权委托书

委托人：

地址：

法定代表人：

委托代理人姓名：

委托代理人职务：

委托代理人身份证号：

委托人现委托上列受委托人为我公司代理人，以本公司的名义参加 投标的相关活动，该受委托人在投标、合同谈判、合同签订、履行过程中所签署的一切文件及处理与之有关的一切事务，本委托人均予以承认，并由本委托人承担全部法律责任。

委托期限：自本授权委托书签署之日起至本授权委托书书面终止日为止。

受委托代理人无转委托权。

特此委托！（附：委托代理人身份证复印件并盖章）

委托人： （盖章）

委托代理人： （签名）

法定代表人： （签名）

年 月 日

附件3

**承诺函**

四川省精神医学中心：

我单位作为本次采购项目的投标人，根据招标文件要求，现郑重承诺如下：

一、具备参加本项目规定的以下条件：

（一）具有独立承担民事责任的能力（提供客观证明材料）；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加采购活动前三年内，在经营活动中没有重大违法记录；

（六）法律、行政法规规定的其他条件；

（七）招标文件中规定的商务要求。（提供客观证明材料）

二、完全接受和满足本项目比选文件中规定的实质性要求，如对招标文件有异议，已经在招标截止时间届满前依法进行维权救济，不存在对招标文件有异议的同时又参加招标以求侥幸中选或者为实现其他非法目的的行为。

三、参加本次招标采购活动，不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的采购活动的行为。

四、参加本次招标采购活动，不存在和其他供应商在同一合同项下的采购项目中，同时委托同一个自然人、同一家庭的人员、同一单位的人员作为代理人的行为。

五、如果有《四川省政府采购当事人诚信管理办法》（川财采[2015]33号）规定的记入诚信档案的失信行为，将在参选文件中全面如实反映。

六、参选文件中提供的能够给予招标人带来优惠、好处的任何材料资料和技术、服务、商务等响应承诺情况都是真实的、有效的、合法的。

七、此次向四川省精神医学中心报价的服务/货物项目为投标人提供同类服务/相同规格型号货物的四川省内最低报价。

本公司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，我公司愿意接受以提供虚假材料谋取中选追究法律责任。

投标人名称：（单位公章）

法定代表（负责人）或授权代表人（签字或加盖个人名章）：

日期：

附件4

**培训方案**

（投标人详细阐述培训方案:）

投标人名称：（盖章）

法定代表人（负责人）或授权代表人（签字或盖章）：

参选日期:

附件5

|  |  |  |  |
| --- | --- | --- | --- |
|  | **评标要素索引表** | | |
| **序号** | **审查** | **评审要素** | **投标文件页码范围** |
| 1 | 资格 | 报价单 |  |
| 2 | 法定代表人委托授权书 |  |
| 3 | 法定代表人委托授权书 |  |
| 4 | 委托人身份证复印件 |  |
| 5 | 公司营业执照 |  |
| 6 | 体现健全的财务制度的证明材料 |  |
| 7 | 依法缴纳税收和社会保障资金的证明材料或承诺函 |  |
|  |  | 参加采购活动前三年内，在经营活动中没有重大违法记录承诺函 |  |
| 8 | 技术 | 技术响应文件 |  |
| 9 | 商务 | 商务响应文件 |  |

附件6：技术参数响应文件

|  |  |  |  |
| --- | --- | --- | --- |
| **技术参数响应文件（格式要求）** | | | |
| **/** | **技术参数** | **投标参数** | **是否响应** |
| / | XX |  |  |
| … | … | … |

备注：如以上标注为响应，但提供相关客观证明材料显示该参数并未响应，则视为虚假响应，不再纳入合作对象范围。

**表格可根据实际情况进行调整。**

**请参考5.1**

附件7：商务响应文件

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 商务要求 | 采购文件要求 | 响应的应答情况 |
| 1 | **▲**服务期及地点 | 1.服务期限：合同签订后一周内进场开始测评工作，本项目须于2023年12月31日前完成。  2.交货地点：采购人指定地点。 |  |
| 2 | **▲**付款方式 | 投标人完成初次测评后，投标人对招标人提供的《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》及过程资料进行验收，验收合格后支付合同金额的100%。 |  |
| 3 | 验收标准 | 按国家有关规定、《财政部关于进一步加强政府采购需求和履行验收管理的指导意见》（财库〔2016〕205号）文件、招标文件要求、投标人的投标文件及有关承诺以及合同约定标准进行验收。本项目主要预期成果为“四川省严重精神障碍综合管理信息系统”通过等级保护测评（三级），在2023年12月31日前取得符合要求的《信息系统安全等级保护备案证明》即可视为验收合格。 |  |
| 4 | 培训要求 | 投标人结合本项目及招标人实际需要，提供技术培训方案。 |  |
| 5 | 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》（公通字[2007]43号、《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/T28448-2019）、《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）、《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）、《信息安全技术信息安全风险评估规范》（GB/T20984-2015）、《中华人民共和国网络安全法》。 |  |
| 6 | 技术原则 | 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。  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。  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.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。  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。  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。  7.测评机构资质及人员要求：（1）从事信息系统检测评估相关工作人员无违法记录；（2）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；（3）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。 |  |