大竹县人民医院2025年度三级等保测评服务院内自主采购项目

采购需求

**一、采购标的**

采购包1：

采购包预算金额（元）:120000.00

采购包最高限价（元）:120000.00

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目类型 | 项目名称 | 数量 | 单位 | 委托代理服务范围 |
| 1 | 服务类 | 大竹县人民医院2025年度三级等保测评服务院内自主采购项目 | 1 | 项 | 包括： PACS系统、EMR系统、数据交换平台系统及与完成采购人等级保护测评、备案工作相关的所有事项。 |

本项目采购人大竹县人民医院是集医疗、教学、科研、预防保健为一体的国家三级甲等综合医院。

（一）本项目是由采购人支付服务费，招一家信息安全服务公司。采购人委托该公司代其办理所拥有的PACS系统、EMR系统、数据交换平台系统的安全等级保护测评以及网络信息安全在公安部门备案的全部工作，并在合同履行期间提供信息技术安全咨询服务。

（二）采购人招的安全服务咨询公司为本项目的供应商，采购人授权该供应商委托办理采购标的内容如下:

1.要求该供应商全面梳理及汇总代理采购人采购标的的全部工作需求并形成需求文档和实施计划。

2.经采购人授权后，供应商应代采购人完成PACS系统、EMR系统、数据交换平台系统的等级保护测评工作，出具测评报告，并在达州市网络安全支队完成以上系统的备案以及在四川省公安厅系统完成报备工作。工作内容包括但不限于了解采购人需求，编制采购人的等级保护测评方案、确定实施进度、对接采购人上级主管部门、行政机关、第三方测评机构，组织行业专家进行定级评审、组织有资质单位进行安全等级保护测评、向公安行政部门（或等保测评备案有关的行政主管部门）办理安全等级保护备案手续等。

3.供应商应负责采购人院内以及与测评工作相关部门的所有协调工作，不得将部分环节工作转嫁给采购人的职能人员，占用采购人职能人员时间，最终应代采购人在2025年12月31日前完成采购人的PACS系统、EMR系统、数据交换平台系统的测评工作，取得以上系统的有效的安全等级保护测评报告及完成公安部门的备案工作。

（三）供应商的报价是完成本项目的全部内容的价格体现。应包括供应商为完成本项目的全部工作须支付或发生的一切所需费用（包括但不限于管理费、服务费、人工费、税费等以及拟获得的利润。）供应商报价应充分考虑合同履行期内各种费用、市场风险、价格波动、承担义务和付款条件等，本项目无成本分担和风险补偿。

**二、技术、服务要求**

（一）供应商应代采购人完成PACS系统、EMR系统、数据交换平台系统的等级保护测评工作，出具每个系统有效的测评报告，上述所有测评成果资料必须具有法律效力，且所有测评成果资料必须能够在达州市网络安全支队完成备案及在四川省公安厅系统完成报备。

（二）供应商成立工作小组并指定项目负责人，项目负责人应具有良好的职业道德、业务素质和责任意识。供应商在本项目合同履约期间，应提供不少于3人的服务团队，该服务团队在采购人处驻场服务，主要负责办理本项目的安全等级保护测评、数据渗透、漏洞扫描、安全咨询等服务。本项目常驻服务人员不得随意更换，如出现不可抗力原因需更换的，必须在更换事由发生之日起三日内向采购人提交书面申请，并详细说明更换的原因、提供替代人员的简历等，经采购人同意后，方可更换。若上述人员不能满足采购人采购文件要求的内容，由供应商自行补充人员，采购人不再额外支付费用。

（三）采购人与供应商仅为签订采购合同的合作关系，供应商所提供服务的工作人员与采购人之间没有任何劳动用工关系和雇佣关系。供应商自行为本项目工作人员办理劳动手续并支付一切费用。供应商必须认真执行中华人民共和国《中华人民共和国劳动法》《中华人民共和国民法典》等相关规定，必须与员工建立合法的用工关系，必须与工作人员签订劳动合同，必须认真履行各项义务，确保员工的合法权益。供应商为本项目员工发放劳动报酬、福利待遇和缴存社会保险，其具体金额由供应商与员工协商确定，供应商为本项目员工发放的劳动报酬、社会保险、福利待遇等不得低于国家和四川省达州市的相关法律、法规和部门规章规定的最低标准。如遇劳动薪酬、福利待遇、社会保险等纠纷问题一概由供应商自行解决。供应商员工发生的工伤及劳动合同纠纷均由供应商自行负责处理。供应商与员工之间的任何争议纠纷与采购人无关。

（四）按照达州市网络安全支队要求，本项目需在2025年12月31日前完成测评系统的《安全等级保护测评报告》并完成备案。**采购人在本采购文件中委托供应商代理完成该事项，供应商应在2025年12月31日前出具有效的安全等级保护测评成果资料并取得达州市公安局网安支队部门有效备案证明。**

（五）供应商提供的委托代理服务，必须符合以下标准：

1. 《中华人民共和国网络安全法》
2. 《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
3. 《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》
4. 《GB/T 25058-2019 信息安全技术 信息系统安全等级保护实施指南》
5. 《GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》
6. 《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》
7. 《GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》
8. 《GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南》
9. 《GB/T 36627-2018 信息安全技术 网络安全等级保护测试评估技术指南》
10. 与本项目相关国家最新标准、行业标准及三级甲等医院运行管理要求。

（六）供应商参与本项目的所有人员，对工作中所涉的数据、资料及文件等负有保密义务，未经采购人同意，不得向第三方泄露，不得利用任何数据进行任何侵害采购人的行为，否则采购人有权追究供应商的责任。

（七）供应商须遵守采购人规定的院内各项制度和要求，并在指定的区域内进行作业，供应商做好各项安全保障工作和预案，做好员工安全教育工作，确保安全，严格执行国家相关法律法规、安全规章制度，采取有效的安全措施，合同履行过程中由供应商及员工原因造成的一切安全事故、人身伤亡、经济损失均由供应商自行承担，其责任与采购人无关。若供应商造成采购人损失的，包括但不限于采购人本身的财产损失或人身伤害或由此而导致的采购人对任何第三方的法律责任等，供应商对此均应承担全部的赔偿责任和法律责任。

（八）供应商合同履约期间不服从采购人的监督管理，或造成安全事故，或受到行政机关处罚未及时整改，或服务质量不符合国家标准及三级甲等医院要求，或给采购人带来严重负面影响的视为供应商违约，采购人将立即解除合同，供应商给采购人造成其他损失的，还要向采购人进行全额赔偿。

（九）若供应商原因导致采购人受到行政机关处罚，所产生的罚款费用和法律责任由供应商全部承担，供应商要立刻整改，并对造成的损失进行赔偿。

（十）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。供应商如欲在项目实施过程中采用自有知识成果，需在响应文件中声明，并提供相关知识产权证明文件。使用该知识成果后，供应商需提供开发接口和开发手册等技术文档，并承诺提供无限期技术支持，采购人享有永久使用权。供应商未拥有的知识产权，则在响应报价中必须包括合法获取该知识产权的相关费用。

（十一）三级等保测评技术要求：

1.测评内容包括技术和管理测评：

（1）技术安全性测评至少包括：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。

（2）管理安全测评至少包括：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。

1.安全物理环境

（1）物理位置选择：至少通过访谈、检查机房的信息系统物理场所在位置上是否具有多方面（至少包含防雷、防风和防雨）的安全防范能力。

（2）物理访问控制：至少通过访谈、检查主机房出入口、机房分区域情况，测评信息系统在物理访问控制方面的安全防范能力。

（3）防盗窃和防破坏：至少通过访谈、检查机房的主要设备、介质和防盗报警系统，测评信息系统是否采取必要的措施预防设备、介质的丢失和被破坏。

（4）防雷击：通过访谈、检查机房的设计/验收文档，测评信息系统是否采取相应的措施预防雷击。

（5）防火：至少通过访谈、检查机房的设计/验收文档和机房防火设备，测评信息系统是否采取必要的措施防止火灾的发生。

（6）防水和防潮：至少通过访谈、检查机房的除潮设备，测评信息系统是否采取必要措施来防止水灾和机房潮湿。

（7）防静电：通过访谈、检查机房是否采取必要措施防止静电的产生。

（8）温湿度控制：通过访谈、检查机房温、湿度情况，判断是否采取必要措施对机房内的温湿度进行控制。

（9）电力供应：至少通过访谈、检查机房供电线路、设备，判断其是否具备提供电力供应的能力。

（10）电磁防护：通过访谈、检查，判断是否具备电磁防护能力。

2.安全通信网络

（1）网络架构：至少通过访谈、检查、测试网络拓扑情况、抽查核心交换机、接入交换机和接入路由器，测试系统访问路径和网络宽带分配情况的过程，测评分析网络架构与网段划分、隔离情况的合理性和有效性，以及通信线路、关键设备硬件冗余，系统可用性保证情况。

（2）通信传输：通过访谈、检查、测试通信传输过程的数据完整性和保密性保护情况。

（3）可信验证：至少通过访谈、检查通信设备的系统引导、系统程序、重要配置参数和通信应用程序进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。

3.安全区域边界

（1）边界防护：通过访谈、检查、测试边界完整性检查设备，测评分析跨域边界的访问控制和数据流通过边界设备的控制措施，非法内联、外联、无线准入控制的监测、阻断的能力。

（2）访问控制：至少通过访谈、检查、测试网络访问控制设备策略部署，测试系统对外暴露安全漏洞情况的过程，测评分析对进出网络的数据流量控制以及基于应用协议和应用内容的访问控制能力。

（3）入侵防范：通过访谈、检查、测试网络边界处、关键网络节点检测、防止或限制从内部和外部发起网络攻击行为的防护能力，以及网络行为分析、监测、报警能力，特别是新型网络攻击行为的分析，对攻击行为的检测是否涉及防范能力（至少包括：攻击源、攻击类型、攻击目标、攻击事件、入侵报警方面）。

（4）恶意代码和防垃圾邮件：通过访谈、检查、测试关键网络节点处对恶意代码、垃圾邮件进行检测、防护和清除、恶意代码防护机制的升级和更新维护的情况。

（5）安全审计：至少通过访谈、检查网络边界、重要网络节点安全审计情况，测评分析信息系统审计配置和审计记录保护，审计内容的情况。

（6）可信验证：至少通过访谈、检查边界设备的系统引导、系统程序、重要配置参数和边界防护应用程序进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。

4.安全计算环境

（1）身份鉴别：通过访谈、检查、测试对登录的用户进行身份标识和鉴别，是否具有不易被冒用的特点，口令应有复杂度要求并定期更换，以及远程管理安全、双因素鉴别的内容。

（2）访问控制：通过访谈、检查、测试是否启用访问控制功能，依据安全策略控制用户对资源的访问；是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的至少最小权限内容。

（3）安全审计：通过访谈、检查安全审计范围及内容。

（4）入侵防范：通过访谈、检查、测试是否能够检测到对重要节点进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警，是否遵循最小化安全安装原则、系统服务、默认共享和高危端口、终端接入限制、数据有效性检验、已知漏洞防护的内容。

（5）恶意代码防范：通过访谈、检查、测试是否具有防恶意代码攻击的技术措施或主动免疫可信验证机制，能否及时识别入侵和病毒行为并将其有效阻断等内容。

（6）可信验证：通过访谈、通过访谈安全员，检查计算设备（至少包含系统引导、系统程序、重要配置参数和应用程序）进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。

（7）数据完整性：通过访谈、检查、测试重要数据在传输和存储过程中的完整性保护情况，至少包括鉴别数据、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。

（8）数据保密性：通过访谈、检查、测试重要数据在传输和存储过程中的保密性保护情况，至少包括鉴别数据、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。

（9）数据备份恢复：通过访谈、检查、测试重要数据本地备份与恢复功能，异地实时备份功能，以及重要数据处理系统的热冗余和高可用性保证。

（10）剩余信息保护：通过访谈、检查、测试边界信息在存储空间被释放或重新分配前是否有效清除，存有敏感数据的存储空间被释放或重新分配前是否有效清除。

（11）个人信息保护：通过访谈、检查、测试是否仅采集和保存业务必需的用户个人信息，对用户个人信息的访问和使用。

5.安全管理中心

（1）系统管理：通过访谈、检查、测试对系统管理员身份鉴别、命令或操作管理、操作审计，以及是否通过系统管理对系统资源和运行进行配置、控制和管理。

（2）审计管理：通过访谈、检查、测试对审计管理员身份鉴别、命令或操作管理、操作审计，以及是否通过审计管理员对审计策略、审计记录进行分析、处理。

（3）安全管理：通过访谈、检查、测试对安全管理员身份鉴别、命令或操作管理、操作审计，以及是否通过安全管理员对安全策略、参数进行配置。

（4）集中管控：通过访谈、检查、测试是否具有特定的管理区域，对分布在网络中的安全设备或安全组件进行集中管控，对网络链路、安全设备、网络设备和服务的运行进行集中监测，对分散在各设备上的审计数据进行收集汇总和集中分析，并确保记录留存符合法律法规要求，对安全策略、恶意代码、升级补丁等安全相关事项进行集中管理，对网络中发生的各类安全事件进行识别、报警和分析。

6.安全管理制度

（1）安全策略：通过访谈、检查网络安全工作的总体方针及安全策略是否全面、完善。

（2）管理制度：通过访谈、检查管理制度的制定和发布过程是否遵循流程。

（3）制度和发布：通过访谈、检查管理制度定期评审和修订情况。

（4）评审和修订：通过访谈、检查管理制度在内容覆盖上是否全面、完善。

7.安全管理机构

（1）岗位设置：通过访谈、检查安全主管部门设置情况以及各岗位设置和岗位职责情况。

（2）人员配备：通过访谈、检查各个岗位人员配备情况。

（3）授权和审批：通过访谈、检查对关键活动的授权和审批情况。

（4）沟通和合作：通过访谈、检查内部部门间、与外部单位间的沟通与合作情况。

（5）审核和检查：通过访谈、检查安全工作的审核和检查情况。

8.安全管理人员

（1）人员录用：通过访谈、检查录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。

（2）人员离岗：通过访谈、检查人员离岗时是否按照手续办理。

（3）安全意识教育和培训：通过访谈、检查是否对人员进行安全方面的教育和培训。

（4）外部人员访问管理：通过访谈、检查对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

9.安全建设管理

（1）定级和备案：通过访谈、检查是否按照一定要求确定系统的安全等级。

（2）安全方案设计：通过访谈、检查整体的安全规划设计是否按照一定流程进行。

（3）产品采购和使用：通过访谈、检查是否按照要求进行系统的产品采购。

（4）自行软件开发：通过访谈、检查自行开发的软件是否采取必要的措施保证开发过程的安全性。

（5）外包软件开发：通过访谈、检查外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。

（6）工程实施：通过访谈、检查建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。

（7）测试验收：通过访谈、检查系统运行前是否对其进行测试验收工作。

（8）系统交付：通过访谈、检查是否采取必要的措施对系统交付过程进行有效控制。

（9）等级测评：通过访谈、检查等级测评、整改情况。

（10）服务商选择：通过访谈、检查是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

10.安全运维管理

（1）环境管理：通过访谈、检查是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。

（2）资产管理：通过访谈、检查是否采取必要的措施对系统的资产进行分类标识管理。

（3）介质管理：通过访谈、检查是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。

（4）设备维护管理：通过访谈、检查是否采取必要的措施确保设备在使用、维护和销毁等过程安全。

（5）漏洞和风险管理：通过访谈、检查安全漏洞和隐患识别、处理情况，以及是否定期开展安全测评以及安全问题的应对措施。

（6）网络和系统安全管理：通过访谈、检查是否采取必要的措施对系统的安全配置、系统账户、漏洞扫描和审计日志进行有效地管理。是否采取必要的措施对网络的安全配置、网络用户权限和审计日志进行有效地管理，确保网络安全运行。

（7）恶意代码防范管理：通过访谈、检查是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。

（8）配置管理：通过访谈、检查基本配置信息管理情况。

（9）密码管理：通过访谈、检查是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。

（10）变更管理：通过访谈、检查是否采取必要的措施对系统发生的变更进行有效管理。

（11）备份与恢复管理：通过访谈、检查是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。

（12）安全事件处置：通过访谈、检查是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效地管理。

（13）应急预案管理：通过访谈、检查是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查。

（14）外包运维管理：通过访谈、检查外包运维服务商选择是否符合国家要求，外包运维保密、服务内容管理。

11.安全扩展要求

按照所测评系统的具体情况选用云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求。

12.验证测试相关要求

按照等级保护测评要求，测评过程中应配备必要的工具、仪器/设备对信息系统进行验证测试，采用的测评工具的生产商应为正规厂商，具有研发和服务能力，能够对产品进行持续更新并提供质量和安全保障。

验证测试内容至少包括以下内容：

12.1渗透测试

验证安全策略正确性；保证用户登录窗体身份验证的安全性；非授权用户不能浏览到未授权内容；不存在跨站点脚本攻击漏洞；脚本不存在SQL、Cookie注入漏洞；安全的处理异常，没有出错页面泄露系统信息；应用和系统漏洞及其他，并提出整改建议。验证内容包括（但不限于）以下几个方面：

|  |  |
| --- | --- |
| 注入 | 失效的身份认证 |
| 敏感信息泄露 | XML外部实体（XXE） |
| 失效的访问控制 | 安全配置错误 |
| 跨站脚本（XSS） | 不安全的反序列化 |
| 使用含有已知漏洞的组件 | 不足的日志记录和监控 |

12.2性能测试

通过模拟手段对网络（包括丢包、时延、带宽等）、软件系统（包括负载、响应）、负载下硬件占用（包含CPU、内存）等进行全面的测评评估验证系统的可靠性、可用性，通过对测试结果的分析，给出相应的整改建议。

12.3漏洞扫描

据相关标准、规范要求对重要信息系统的安全漏洞进行测评。分析总结系统中存在的主要安全漏洞，指出系统中可能被利用的安全漏洞、系统配置错误缺陷以及相应的安全加固意见、建议。

**三、商务要求**

（一）标的交付时间

双方签订采购合同生效后，供应商必须在2025年12月31日前，向采购人交付：

1.有效的PACS系统、EMR系统、数据交换平台系统等级保护测评成果资料；

2.达州市网络安全支队的有效备案证书；

3.四川省公安厅系统报备证明。

（二）项目履行地点：大竹县人民医院院内指定地点。

（三）项目付款方式

1、采购人付款采用银行转账支付方式，采购人付款前，供应商必须出具有效的足额发票，否则采购人有权拒绝付款。供应商为一般纳税人的，应当提供增值税专用发票。

2、采购人与供应商双方签订合同生效后，供应商完成本项目全部服务内容，并向采购人交付合格、有效的成果后（包括不限于PACS系统、EMR系统、数据交换平台系统及其子系统有效的安全等级保护测评成果资料，达州市网络安全支队有效的备案证明，四川省公安厅系统报备证明），项目经采购人履约验收合格后，采购人在收到供应商有效发票后60日内，一次性转账支付供应商项目成交总金额。