**阿勒泰地区人民医院等保测评、风险评估项目**

1. **项目背景**

为深入贯彻国家关于网络安全和信息化工作决策部署，全面落实总体国家安全观和网络强国战略，确保关键技术自主可控，根据《中华人民共和国网络安全法》、《国家政务信息化项目建设管理办法》等法律法规要求，依据《信息安全技术网络安全等级保护测评基本要求》等规范以及系统自身安全性需求，对被评估系统进行网络安全等级保护测评、风险评估工作。为阿勒泰地区人民医院重要网络和信息系统的等保安全提供科学评价，规范网络安全应用和管理行为，推动信息系统安全防护水平的提升。同时，指导信息系统信息安全保障体系建设，增强安全防 护意识，促进安全管理水平的提高。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 预算金额（元） | 简要规格描述 | 备注 |
| 1 | 阿勒泰地区人民医院等保测评、风险评估项目 | 120000.00 | 电子病历信息系统、LIS 系统、HIS 系统3个信息系统开展等保测评、风险评估 | 详见文件内容 |

**二、总体要求**

2.1 测评原则

保密性原则：测评机构应与招标人签订安全评估协议、保密协议，对测评服务的过程 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，不得利用此数据侵害采购人的权益，否则采购人有权追究响应人的责任。

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。

规范性原则：测评机构工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

可控性原则：测评服务的进度应符合进度安排，保证招标人对测评工作的可控性。

整体性原则：测评的范围和内容应系统、全面、规范，满足国家安全评估、等级保护相关基本要求。

最小影响原则：技术测评工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评应在招标方许可的条件下进行。

2.2 实施要求

测评机构应详细描述等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、时间安排、阶段性文档提交和验收标准等。测评机构应详细描述测评人员的组成、资质及各自职责的划分。测评机构应配置经验丰富的测评人员进行等保测评工作。

2.3 测评方法

测评方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地察看等多种方法。

如需在等级保护测评实施过程中采用在线测评工具的，各种工具软件由测评机构推荐，经招标人确认后由测评机构提供并在测评中使用。应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对 系统造成的风险等。等级保护测评应有详细的实施方案和严格的操作步骤，采取的措施应 是经过测试、稳定可靠的。

 2.4 风险控制 测评工作本身也会引入安全风险，必须加强测评过程中的风险控制。测评实施前，双方应充分讨论并明确测评对系统可能带来的风险和隐患，确定测评对象、测评方法和工具，并制定应急恢复措施。

（1）操作的申请和监护

测评操作必须遵守现场运行规章制度，确保系统安全稳定运行。如需在线测试，按照相关工作规程，事前申请，并在专责人员的指导和监护下进行。

1. 人员与数据管理

重视测评保密工作，加强测评过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

1. 测评对象选择

优先选择备用设备（系统）或临时搭建的模拟环境进行测评，避免影响在线系统运行。

1. 制定应急预案

根据被测评系统情况，在测评实施前制定应急预案，加强系统在线应急处置能力。

1. **测评对象**

本次评估对象为阿勒泰地区人民医院电子病历信息系统、LIS 系统、HIS 系统3个信息系统，根据被评估对象的实际情况、所属行业及系统情况，开展网络安全等级保护测评、信息安全风险评估。

1. **项目实施依据和执行标准**

《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）

《信息安全技术 计算机信息系统安全保护等级划分准则》GB 17859-1999

《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）

《新疆维吾尔自治区政务信息化项目建设管理办法》（新政办发〔2021〕14 号）

《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2020

《信息安全技术 网络安全等级保护测评要求》GB/T 28448-2020

《信息安全技术 网络安全等级保护测评过程指南》GB/T 28449-2018 《信息安全技术 信息安全风险评估模型》GB/T 20984-2007

《信息安全技术 网络基础安全技术要求》（GB/T 20270-2006）

《信息安全技术 信息系统安全通用技术要求》（GB/T 20271-2006） 《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）

《信息安全技术 信息系统安全工程管理要求》（GB/T 20282-2006） **五、服务内容**

 5.1 协助采购单位组织完成所有被测系统的定级、备案工作

协助采购单位组织完成被测系统中所有信息系统的定级备案工作，包含但不限于完成信息系统定级备案材料、通过信息系统定级专家评审、提交信息系统定级备案材料至网安部门。协助采购单位取得《信息系统备案证明》。

5.2 网络安全等级保护测评

通过等级测评及时发现信息系统中存在的安全隐患和安全威胁，分析安全风险的大小及对信息系统的影响，指导开展信息系统安全建设的目标和思路，最终使信息系统的安全防护水平达到等级保护的基本要求。

被测信息系统的范围包括：物理机房、网络基础架构、网络设备、信息系统应用服务器、应用系统软件、数据库、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面。

5.3 信息安全风险评估服务

根据国家《信息安全风险评估规范》（GB/T 20984-2007）并结合国家《信息安全技术网 络安全等级保护基本要求》（GB/T 22239-2019）、信息安全管理体系（ISO/ETC 27001：2005）对信息系统及其网络环境进行评估，识别出系统中的资产、威胁和脆弱性，并通过风险计算的方法对系统面临的安全风险进行分类，最后根据安全风险的风险等级提出适合实际环境的风险处置建议。

5.4 渗透测试和漏洞扫描服务

提供一年2次（每半年一次）的渗透测试和漏洞扫描服务，提供渗透测试报告、漏洞扫描报告和安全加固建议，并跟踪核查加固结果。

5.5 安全培训

培训目的：使采购人熟悉国家对网络安全等级保护相应法律法规的内容、测评内容及方法。

培训内容：网络安全等级保护法律法规、测评内容及方法，当前网络安全形势及网络安全加固基础知识。

培训对象：采购人信息安全管理人员。

培训教师：培训教师须具备相应认证资质与丰富经验。

5.6 应急响应服务

在国家法定节假日、国家或自治区重要会议、安全事件大规模爆发等重要时刻，提供7x24小时现场应急支撑服务。

**六、项目要求**

6.1 管理要求

中标单位需提供详细的项目管理方案，应配备1个独立的项目管理小组，提供项目团队人员安排、项目进度安排、项目关键点控制计划与方案、项目安全控制计划与方案等，以确保项目顺利实施。

 6.2 人员要求

项目实施团队：供应商为本项目须建立一支具有一定服务能力的管理团队，小组成员不少于4人，其中中级测评师2名，初级测评师 2 名，提供测评师证书，以及6个月社保证明。并合理调配各岗位人员，保障服务工作相关岗位人员需要。

6.3 质量要求

对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力。

6.4 服务要求

应急响应：提供 7×24 服务响应（7×24 小时测评师电话支撑），需要现场支撑时，供应商需在3小时内安排至少1名具有服务能力的测评师到达现场处理。

6.5 保密要求

中标人须与招标人签署保密协议，未经招标人同意不得向第三方泄露此项目相关情况。服务中产生的所有资料、技术文档要妥善保管，不得遗失、转借、复印，严禁通过互联网等公共信息网络、普通邮政进行传递。相关工作人员须由中标人进行资格审查和保密教育，对知悉的事项及信息予以保密，自觉遵守国家保密法律法规及招标人工作纪律和规章制度，不做任何窃取或泄露国家秘密、警务秘密的行为，签署《保密承诺书》并报招标人备案。中标人若违反保密协议、未履行相关职责或教育、监督措施落实不到位，发生参与本项目人员窃取或泄露国家 秘密、警务秘密的事件，将按照《中华人民共和国保守国家秘密法》等有关法律法规承担相应的责任。

6.6 成果文件交付要求

中标方应提交的书面材料中应包括但不限于以下内容：

1. **网络安全等保测评报告**

在完成测评工作后，按照等级保护要求对此次项目中每个信息系统出具《网络安全等级保护测评报告》并完成备案工作。

1. **信息安全风险评估报告**

在完成测评工作后，按照信息安全风险评估要求对此次项目中每个信息系统出具《信息安全风险评估报告》并完成备案工作。

3、服务期：自合同签订之日起 1 年

交付期：自合同签订之日起 60 个工作日内出具测评报告

服务地点：阿勒泰地区人民医院院内

付款方式：合同签订并提交测评报告完成验收后支付 100%货款。