项目需求说明

|  |  |
| --- | --- |
| 项目名称 | 南宁市第二人民医院2025年商用密码应用安全性评估项目 |
| 用途及主要功能 | 根据《中华人民共和国密码法》、《商用密码管理条例》以及《商用密码应用安全性评估管理办法》的要求，医院作为关键信息基础设施运营单位，必须对已备案的两个等保三级信息系统（南宁市第二人民医院信息集成平台、南宁市第二人民医院数字化管理系统）每年至少开展一次商用密码应用安全性评估。不开展密评将导致违反国家法规要求，可能面临行政处罚及遭受安全风险。  本项目旨在提升我院信息系统的安全性，确保使用商用密码技术、产品和服务的网络和信息系统的安全性，保障医院重要信息和其他敏感数据的安全。通过对两个三级系统分别开展“应用安全性评估+应用方案编制+应用方案评审”三项服务，确保医院密码应用符合国家强制标准并顺利通过监管审核，及时发现系统脆弱性，识别变化的风险，了解系统安全状况以及存在的安全隐患，为后续的安全建设和整改工作提供依据；同时满足国家政策要求，提升医院信息系统的整体安全性。 |
| 建设内容及功能技术要求 | **建设内容：**  我院需对已备案的两个三级信息系统（南宁市第二人民医院信息集成平台、医院数字化管理系统）开展商用密码应用安全性评估、编制商用密码应用方案和商用密码应用方案评审。  **技术要求：**  **一、商用密码应用安全性评估**  （一）、项目要求  依据《中华人民共和国密码法》要求和系统自身的安全需求分析，对我院信息系统（三级）进行商用密码应用安全性评估，并出具商用密码应用安全性评估报告。  被评估对象的商用密码应用安全性评估服务内容详见下表内容。  （二）、技术标准  GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》  GM/T 0115—2021《信息系统密码应用测评要求》  GM/T 0116—2021《信息系统密码应用测评过程指南》  GB/T 43207—2023《信息安全技术 信息系统密码应用设计指南》  《商用密码应用安全性评估测评作业指导书（试行）》  《信息系统密码应用高风险判定指引》  《商用密码应用安全性评估量化评估规则》  （三）、实施方式  1、通用要求测评  核查信息系统中使用的密码算法、密码技术、密码产品和密码服务是否满足国家密码管理的相关标准或规范要求。  2、密码技术应用要求测评  具体包括物理和环境安全测评、网络和通信安全测评、设备和计算安全测评、应用和数据安全测评，验证不同安全等级信息系统的密码应用是否达到相应安全等级的安全保护能力、是否满足相应安全等级的保护要求。  3、安全管理测评  从制度、人员、实施和应急四个方面进行安全管理测评，验证信息系统安全管理机制是否完善，是否能够确保密码技术被合规、正确、有效地实施。  4、整体测评与风险评估  对系统进行整体安全测评，并依据《商用密码应用安全性评估量化评估规则》，对信息系统的密码应用情况给出定量评估结果。依据《信息系统密码应用高风险判定指引》判断系统是否存在高风险并分析相关风险可能对信息系统安全造成的影响，提交整体测评与风险评估结果。  5、评估成果  测评完成后，基于测评结果，对我院两个三级系统出具符合国家密码管理局要求的《商用密码应用安全性评估报告》，并协助我院向广西壮族自治区密码管理局提交密评备案材料。  **二、商用密码应用方案编制服务**  对我院信息系统现状进行调研分析，梳理系统存在的安全漏洞及对应安全需求，结合实际情况和《信息系统密码应用基本要求》中的各项条款，为我院已两个三级信息系统分别编写《商用密码应用方案》。方案需满足国家密码管理局发布的相关编制要求，最终出具《商用密码应用方案》。  **三、商用密码应用方案评审服务**  对最终形成的《商用密码应用方案》进行评审，依据《信息系统密码应用基本要求》和《密码应用方案评估报告模板》，对方案的可行性、科学性、完备性、合理性进行评估，最终出具符合国家密码管理局要求的《商用密码应用方案评审报告》。 |
| 安全性与权限控制要求 | 建设方在项目进场前需与院方签订数据保密协议。 |
| 实施及后续运维服务要求 | （一）实施要求  1.测评周期：  （1）商用密码应用安全性评估：  ①签订合同后，自接到我院通知进场之日起60个工作日内，完成待测系统的商用密码应用安全性评估工作，若被测系统的评估结论为“符合”或“基本符合”，供应商现场评估结束后30个工作日内，提供该系统的商用密码应用安全性评估报告，供应商不提供复测服务，项目完结；  ②若被测系统的初次评估结论为“不符合”，供应商在现场评估结束后30个工作日内提供该系统的整改建议或提供该系统的商用密码应用安全性评估报告（初测报告），经过我院整改完成后与供应商确认复测日期；整改应在出具整改建议或初测报告之日起6个月内完成，若逾期未能完成整改的，供应商不再提供复测服务，项目完结；若如期完成整改，自我院出具项目复测通知书之日起 15个工作日完成该项目现场复测，复测完成后30个工作日内提供该项目的最终商用密码应用安全性评估报告，项目完结。   1. 密码应用方案编制：   签订合同后，供应商在接到我院通知进场后60个工作日内完成方案编制。   1. 密码应用方案评估：   出具密码应用方案后，方案通过供应商评审合格后30个工作日内，供应商出具《密码应用方案评估报告》。  （二）保密要求：供应商和我院签署保密协议，严格遵循保密原则，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害我院利益。  （三）人员要求：供应商应提供不少于5名商用密码应用安全性评估人员，其中包含1名项目经理。  （四）售后响应：①为我院提供免费维保和技术咨询服务及提供技术支持和升级服务；平均故障修复时间少于2小时。紧急情况应于2小时内到达现场。  ②测评完成之后，承诺协助我院完成信息系统备案和整改咨询服务，承诺提供科学、合理、有效的整改建议，并及时跟进。在整改过程中，如需现场服务，安排技术人员将赶到现场协助处理。并定期对我院进行电话回访服务，如有疑难或故障，随即启动远程或上门检修服务。   1. 其他费用：供应商报价中应包含人工费、保险费、税费、技术支持与评估服务费等所有相关费用。 |