# 附件一：采购需求

1. 采购需求
   1. 项目依据

《中华人民共和国网络安全法》

《信息安全等级保护管理办法》

《信息安全技术信息系统安全等级保护定级指南》

《信息安全技术信息系统安全等级保护基本要求》

《信息安全技术信息系统通用安全技术要求》

《信息安全技术网络基础安全技术要求》

《信息安全技术操作系统安全技术要求》

《信息安全技术数据库管理系统安全技术要求》

《信息安全技术服务器技术要求》

《信息安全技术终端计算机系统安全等级技术要求》

* 1. 网络安全等级保护测评服务

依据公安部 《关于信息安全等级保护工作实施意见》（公通字[2004]66号）、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）等文件要求，按照等级保护相关标准的要求，需对红河州第三人民医院所涉及的新HIS系统、LIS系统、PACS系统、EMR系统、互联网医院系统开展三级等保测评，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面对系统进行网络安全等级保护测评工作。协助红河州第三人民医院组织召开信息系统定级专家评审会,并在当地公安机关完成定级备案工作，取得备案证书。测评结束后出具《网络安全等级保护测评报告》，并提出相应的安全建设整改建议，提供整改指导服务。为红河州第三人民医院进一步有效、合理地完善信息系统安全等级保护建设提供重要数据分析和安全保障。

* + 1. 技术测评

按照等保2.0要求进行测评，主要包括安全物理环境、安全通信环境、安全区域边界、安全计算环境、安全管理中心等五个层面上的测评。

（1）安全物理环境

安全物理环境测评内容要求包含以下十个控制点：物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护；

（2）安全通信环境

安全通信环境测评内容要求包含以下三个控制点：网络架构、通信传输、可信验证；

（3）安全区域边界

安全区域边界测评内容要求包含以下六个控制点：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证；

（4）安全计算环境

安全计算环境测评内容要求包含以下十一个控制点：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护；

（5）安全管理中心

安全管理中心测评内容要求包含以下四个控制点：系统管理、审计管理、安全管理、集中管控。

* + 1. 安全管理测评

按照等保2.0要求进行测评，主要包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个层面上的测评。

（1）安全管理制度

安全管理制度测评内容要求包含以下三个控制点：管理制度、制定和发布、评审和修订；

（2）安全管理机构

安全管理机构测评内容要求包含以下五个控制点：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查；

（3）安全管理人员

安全管理人员测评内容要求包含以下四个控制点：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理；

（4）安全建设管理

安全建设管理测评内容要求包含以下十个控制点：定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择；

（5）安全运维管理

安全运维管理测评内容要求包含以下十四个控制点：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理。

* + 1. 整体测评

按照等保2.0要求进行测评。从安全控制点、安全控制点间和区域间等方面进行测评和综合安全分析，从而给出等级测评结论。整体测评包括安全控制点测评、安全控制点间测评和区域间测评。

* + 1. 测评报告编制

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

* + 1. 测评服务提交成果要求

完成等保测评工作应按要求提供相应系统的测评报告、整改建议书及测评实施计划书等，包括但不限于以下材料。

（1）《信息系统等级保护测评方案》（纸版和电子版）

（2）《等级保护测评实施计划》（纸版和电子版）

（3）《等级保护测评过程记录文件》（电子版）

（4）《信息系统等级保护测评报告》（纸版和电子版）

（5）《网络与信息系统安全等级保护整改建议书》（纸版和电子版）