# 濮阳医学高等专科学校等级保护测评项目要 求

## 一、项目意义

贯彻国家政策要求，落实网络安全等级保护制度，全面提升信息系统安全保护能力和网络安全管理水平，按照国家相关要求开展网络安全等级保护测评工作。

## 二、项目范围

信息系统包含：一卡通系统、网站系统等。

## 三、项目要求

完成信息系统安全等级保护测评工作，提交信息系统的安全等级保护测评报告，协助完成在当地公安部门的等级保护备案工作，取得备案证明。

## 四、遵循的政策法规和规范

* 《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》（国务院令147号）；
* 《计算机信息系统安全等级保护划分准则》（GB/T17859-1999）；
* 《信息安全等级保护管理办法》（公通字[2007]43号）；
* 《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058-2010）；
* 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）；
* 《信息安全技术 信息系统安全保护等级保护定级指南》（GB/T 22240-2008）；
* 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）；
* 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）。

## 五、项目具体要求

在安全等级测评过程中，每个工作阶段、流程、内容及成果交付严格遵循《信息安全技术 网络安全等级保护测评要求》和《信息安全技术 网络安全等级保护测评过程指南》文件，根据信息系统安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告。

**1、测评过程文档**

项目各阶段的测评过程文档（参照《信息安全技术 网络安全等级保护测评过程指南》）编制。

| **项目阶段** | **交付成果** |
| --- | --- |
| 测评准备活动 | 项目计划书  被测系统基本情况表 |
| 方案编制活动 | 测评指导书  信息系统安全测评方案 |
| 现场测评活动 | 测评结果记录  测评中发现的问题汇总 |
| 分析与报告编制活动 | 单项测评结果汇总分析  整体测评结果汇总分析  等级测评结论  信息系统安全等级测评报告 |

**2、整改建议**

依照《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）的要求，在系统测评工作的基础上，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全建设整改建议方案，方案内容包含但不限于：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全建设整改技术方案设计、安全建设整改管理体系设计、信息系统安全产品选型及技术指标建议、安全建设整改项目实施计划、项目预算、整改后可能存在的其他问题。

**3、具体技术要求**

安全通用要求分为安全技术要求和安全管理要求。

1）安全技术要求：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的安全控制测评。

2）安全管理要求：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面的安全控制测评。

安全物理环境：针对物理机房提出安全控制要求，主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置选择、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、电力供应和电磁防护。

安全通信网络：针对网络架构和通信传输提出安全控制要求。主要对象为广域网、城域网、局域网的通信传输以及网络架构等；涉及的安全控制点包括网络架构、通信传输和可信验证。

安全区域边界：针对网络边界提出安全控制要求，主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计和可信验证。

安全计算环境：对边界内部提出安全控制要求，主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、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、剩余信息保护和个人信息保护。

安全管理中心：针对整个系统提出安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

安全管理制度：针对整个管理制度体系提出安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

安全管理机构：针对整个管理组织架构提出安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

安全管理人员：针对人员管理提出安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

安全建设管理：针对安全建设过程提出安全控制要求，涉及的安全控制点包括定级和备案、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、等级测评和服务供应商管理。

安全运维管理：针对安全运维过程提出安全控制要求，涉及的安全控制点包括环境管理、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、应急预案管和外包运维管理。

## 六、工期要求和交付成果

40个工作日内完成。

成果包含：网络安全等级测评报告、网络安全整改建议方案、等级保护备案证明。