**北京胸科医院信息系统安全等级保护服务项目需求说明**

为了保障医院核心业务系统持续、稳定的运行，确保信息系统安全满足国家相关标准、规范要求，需要按照《北京市卫生局关于进一步加强北京卫生行业信息安全等级保护工作的通知》京卫办[2012]26号文件和等级保护的基本要求，对客户指定的数据统一应用平台系统、PACS系统、LIS系统、门户网站系统开展等级保护服务工作。

通过技术手段持续完善总体网络安全保障体系，开展方案编制、现场初测、结果分析、现场复测、报告编制等测评工作，以科学制定信息系统安全保障与持续策略，落实《卫生行业信息安全等级保护工作的指导意见》（卫办发【2011】85号）和《关于进一步加强北京市卫生行业信息安全等级保护工作的通知》（京卫办字[2012]26号）文件要求，建成一个覆盖推进高效、有序、可持续发展并满足等级保护二级防护要求的信息安全保障体系，全面保障应用平台安全稳定、持续运行。

具体工作内容:

1. **方案编制**

**服务内容：**

依据基本信息收集结果，确定测评范围，编制实施方案（内容包括信息系统基本情况，测评依据和目的、测评内容、测评工具和方法、测评对象选择方法、项目实施计划等内容初测现场记录表与复测现场记录表制作。

1. **现场初测**

**服务内容：**

通过人工黑盒的测试方式，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议；

利用扫描器检查等保定级涉及的重要服务主机操作系统、数据库系统及关联的重要网络设备、重要安全设备的漏洞情况包括初测和复测）；

依据信息系统安全等级组合定级结果，与GB/T 22239-2019信息安全技术网络安全等级保护基本要求内容实施安全测评，对测评结果进行记录。

1. **结果分析**

**服务内容：**

依据测评结果，将被测对象不合规与部分合规的系统名称进行分类，列出测评对象所面临的安全问题列表，并提出安全整改建议清单。

**交付成果：**《等级保护安全问题清单》、《信息系统安全漏洞扫描报告》、《信息系统安全渗透测试报告》

1. **现场复测**

**服务内容：**

依据初测时的测评结果，对不合规项与部分合规项展开复测，并对测评结果进行记录。

1. **报告编制**

**服务内容：**

针对测评结果进行报告编制（报告内容涵盖被测资产范围、不适用项声明、总体安全测评单元符合情况、综合问题分析、安全威胁评估分析、安全层面间得分、仍面临的安全风险问题列表、本次测评结果、测评结论与评价）。

**交付成果：**《信息安全等级保护测评报告》