附件二：

**仪征市人民医院数据平台、业务系统、互联网医院、OA系统等保测评项目需求**

**一、服务内容：**

**1、项目说明**

为贯彻落实《中华人民共和国网络安全法》（主席令12届第53号）、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）、《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号)等文件要求，做好信息系统信息安全工作，对提升信息系统安全防护能力和水平，维护公共利益和社会秩序，维护公民、法人和组织的合法权益有着重大意义。

**2、项目范围**

本项目等级测评对象为仪征市人民医院数据平台、业务系统、互联网医院、OA系统进行等保测评，预算金额约为20万元。

整个测评包括机房基础设施、主干网；应用系统测评包括业务应用、发布、中间件、数据库软件系统和主机系统。

**3、服务内容**

(1) 对每个信息系统进行等级保护测评。客观的评价重要信息系统在等级保护工作中取得的成绩，按照科学的评估方法，对信息系统的安全现状进行等级保护测评，分析信息系统保护现状和信息安全等级保护基本要求之间的差距，评估目前信信息系统是否符合国家及行业等级保护的相关标准，并出具等级保护测评报告，为开展系统等级保护整改建设奠定基础。

(2)协助建立信息安全等级保护管理体系。根据《信息安全等级保护管理办法》和《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，结合等级保护测评报告提出的安全管理体系与等级保护基本要求之间的差距，在信息安全管理制度、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指导并协助建立健全符合相应等级要求的安全管理制度。

(3)协助进行信息安全等级保护安全技术整改。根据《信息安全等级保护管理办法》和《信息系统安全等级保护基本要求》，结合等级保护测评报告提出的安全防护现状与等级保护基本要求之间的差距，综合重要信息系统的特点，明确安全需求，设计符合相应等级要求的信息系统安全技术建设整改方案，协助开展信息安全等级保护安全技术措施建设，落实相应的物理环境、通信网络、区域边界、计算环境和管理中心等安全保护技术措施。

**二、实施内容范围及项目实施原则**

**1、客观性和公正性原则：**

测评人员应当没有偏见，在最小主观判断情形下，按照评估双方相互认可的评估方案，基于明确定义的测评方式和解释，实施评估活动。

**2、可重复性和可再现性原则：**

依照同样的要求，使用同样的评估方式，对每个评估实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同评估者评估结果的一致性有关，后者与同一评估者评估结果的一致性有关。

**3、连续性原则：**

确保在高速变化的信息安全环境中，在有效的服务期间内，保证采购方风险评估结论的准确性和及时性，对于采购方单位新增设的信息资产和服务，或新建立的信息化项目，进行局部系统的重新评估。从经济上，降低了采购方单位的成本，从信息安全性上，保证信息安全测评的动态稳定性。

**4、扩展性原则：**

在评估过程结束后，信息安全测评过程要保持扩展性，从扩展的属性上进一步加强测评结束后采购方的安全管理有效性和可用性。

**5、保密原则：**

在测评过程中，需严格遵循保密原则，双方签订保密协议，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采购方利益。

**6、互动原则：**

在整个测评过程中，强调采购方的互动参与，每个阶段都能够及时根据采购方的要求和实际情况对测评的内容、方式做出相关调整，进而更好的进行风险评估工作。

**7、最小影响原则：**

测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。

**8、规范性原则：**

信息安全等级保护测评服务的实施必须由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

**9、质量保障原则：**

在整个测评过程中，须特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

**三、实施要求**

本次等级保护测评项目不得转包或者分包，所有驻场测评师必须持证上岗，未经采购方同意，项目组成员不得更改。