附件1：

**用户需求书**

**一、项目概况**

1、项目名称：中山市中医院网络安全等级保护评测服务项目

2、项目内容：医院拟委托一家具备相关资质的服务公司，对我院的重要信息系统（中山市中医院HIS系统、EMR系统、LIS系统、PACS系统、OA系统、信息集成平台、门户网站、微信小程序）依法进行网络安全等级保护测评工作，保障我院信息化健康发展，切实保护人民群众的合法权益。

3、服务期限：合同签订后6个月（完成所有测评对象的测评工作，并出具相关的评估报告）

4、拟测评等级：三级

5、项目预算：45万元

**二、项目服务内容**

1、信息系统定级、协助备案服务

服务商按照《信息安全技术网络安全等级保护定级指南》（GB/T 22240—2020）要求，指导并协助采购人进行材料填写，协助完成在本地公安机关的备案工作。

2、网络安全等级测评服务

服务商依据国家相关网络安全标准和规范，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，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，测评工作包括技术测评和管理测评两部分，分别为：

（1）技术测评

2.1.1安全物理环境：物理位置的选择、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。

2.1.2安全通信网络：主要涉及对象为信息系统的网络拓扑结构、路由器、交换机、无线接入设备和防火墙等提供网络通信功能的设备或相关组件，具体的测评内容如下所示：网络架构、通信传输、可信验证。

2.1.3安全区域边界：通过访谈、检查和测试的方式，主要涉及对象为网闸、防火墙、路由器、交换机和无线接入网关设备等提供访问控制功能的设备或相关组件。具体测评内容包括：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、可信验证、安全审计。

2.1.4安全计算环境：通过访谈、检查和测试的方式，主要涉及的对象为终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、业务应用系统、数据库管理系统、中间件等，具体测评内容包括：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、个人信息保护。

2.1.5安全管理中心：通过访谈和检查的方式，测评主要涉及的对象为提供集中系统管理功能的系统。具体测评内容包括：系统管理、审计管理、安全管理、集中管控。

（2）管理测评

2.2.1安全管理制度：安全管理制度测评通过访谈和检查的形式评估安全管理制度的制定、发布、评审和修订等情况。主要涉及的对象为安全主管人员、安全管理人员、其他人员、管理制度、操作规程文件等，具体测评内容包括：安全策略、管理制度、制定和发布、评审和修订。

2.2.2安全管理机构：安全管理机构测评通过访谈和检查的形式评估安全管理机构的组成情况和机构工作组织情况。主要涉及的对象为安全主管人员、安全管理人员、相关的文件资料和工作记录等，具体测评内容包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

2.2.3安全管理人员：人员安全管理测评通过访谈和检查的形式评估机构人员安全控制方面的情况。主要涉及对象为安全主管人员、人事管理人员、相关管理制度、相关工作记录等，具体测评内容包括：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。

2.2.4安全建设管理：系统建设管理测评通过访谈和检查的形式评估系统建设管理过程中的安全控制情况。主要涉及对象为安全主管人员、系统建设负责人、管理制度、操作规程文件、执行过程记录等，具体测评内容包括：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、服务供应商选择。

2.2.5安全运维管理：通过访谈和检查的形式测评系统运维管理过程中的安全控制情况。主要涉及人员有安全主管人员、安全管理人员、运维人员，涉及内容有运维管理制度、运维服务团队的管理制度、操作规程文件、执行过程记录等。具体测评内容包括：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、应急预案管理、外包运维管理。

**三、项目服务要求**

1、服务商按照等级保护要求对此次项目中每个信息系统进行初次测评，并出具《问题清单及安全加固整改建议书》，制订详细的安全整改实施计划，对必须新增安全软硬件产品才能解决相关安全问题，提出详细的风险规避措施和实施建议。

2、服务商应积极配合采购人完成整改，并进行测评直至符合等级保护要求。

3、测评通过后，服务商应根据项目服务内容10个层面的现场测评结果，对每个信息系统出具《网络安全等级测评报告》，并到当地公安完成备案。

4、保密要求

（1）服务商须与采购人签署保密协议，未经采购人同意不得向第三方泄露此项目相关情况。服务中产生的所有资料、技术文档要妥善保管，不得遗失、转借、复印，严禁通过互联网等公共信息网络、普通邮政进行传递。

（2）相关工作人员须由采购人进行资格审查和保密教育，对知悉的事项及信息予以保密，自觉遵守国家保密法律法规及招标人纪律和规章制度，不做任何窃取或泄露国家秘密、警务秘密的行为，签署《保密承诺书》并报采购人备案。

（3）服务商若违反保密协议、未履行相关职责或教育、监督措施落实不到位，发生参与本项目人员窃取或泄露国家秘密、警务秘密的事件，将按照《中华人民共和国保守国家秘密法》等有关法律法规追究其相应的责任。

**四、结算方式**

服务商出具《网络安全等级测评报告》，并完成公安部门备案后，采购人在收到发票后60天内一次性支付合同款项。