**中国医学科学院肿瘤医院**

**多系统等保测评和安全加固服务**

**技术需求书**

## 1.项目服务原则

**（一）安全保密原则**。投标人在提供安全服务的过程中，要严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

**（二）最小影响原则**。投标人开展的安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如不可抗力无法避免，应对风险进行说明。

**（三）规范性原则**。投标人开展的安全服务工作，要由专业的安全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，提供完整的服务报告。

**（四）可控性原则**。投标人在开展安全服务工作过程中采用的工具、方法和过程要在双方认可的范围之内，保证用户对于服务过程的可控性。

**（五）质量保障原则**。投标人开展的安全服务工作需特别重视项目质量管理，项目的实施需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。

## 2.具体采购内容

* 对疑难病诊治能力同质化智慧平台、科研随访平台（软硬件环境）2个系统开展信息安全等级保护三级测评工作。主要交付物：《系统等级保护测评报告》、《等保测评工作方案》。
* 渗透测试，服务期内对上述应用系统进行受控的、非破坏性的渗透测试，指定专业安全工程师使用的成熟的测试技术和经过验证的不具备真实破坏性方式，对目标网络、系统、主机应用的安全性深入的探测，发现系统最脆弱环节。每次服务包含初测和若干次复测，并指导系统开发商进行整改，直至无高危漏洞为止。主要交付物：渗透测试报告。数量：1次。
* 安全加固，在安全巡检和渗透测试的基础上提出安全加固方案，在经过相关负责人批准后，由相应的信息系统承建单位实施安全加固操作，系统安全加固实施后由安全工程师审查加固实施情况，进行安全加固补遗工作，保障信息系统的安全运行，排除安全隐患。主要交付物：《信息系统网络安全加固报告》。数量：1次。

## 3.资质要求

1. 具备有效的国家网络安全等级保护工作协调小组办公室颁发的“网络安全等级保护测评机构推荐证书”。
2. 具备有效的公安部三所颁发的“网络安全等级测评与检测评估机构服务认证证书”。
3. 实施团队成员至少有3位拥有在有效期内的CISP证书。
4. 具有国家密码管理局颁发的《商用密码应用安全性评估》证明。

## 4.服务承诺

1. 在项目实施过程中，应充分尊重甲方需求，采取最小影响原则和规范性原则开展工作。
2. 合同期内对发现的各类问题免费进行整改和技术支持。
3. 测评对象选择和具体实施时间以甲方要求为准。