口腔医院三级信息测评参数

**一、本项目不接受超过4.99万元（采购项目预算金额）的报价。**（报价包含产品价、税金、配送、安装等全部费用，采购人不再支付报价以外的任何费用。）

**二、项目内容：**口腔医院三级信息评测。

**三、服务要求：**

### 测评依据

（1）政策依据

《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)

《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)

《信息安全等级保护管理办法》(公通字[2007]43号)

关于开展信息安全等级保护安全建设整改工作的指导意见(公信安[2009]1429号)

《信息安全技术 信息系统安全等级保护实施指南》(GB/T 25058-2019)

《计算机信息系统安全保护等级划分准则》(GB 17859-1999 )

《信息安全技术 网络安全等级保护定级指南》(GB/T 22240—2020)

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）

《中华人民共和国网络安全法》

（2）技术标准

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》

GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》

GB/T 25058-2019《信息安全技术 信息系统安全等级保护实施指南》

### 测评方法

安全测评的主要方法有：访谈、核查和测试及综合评估。

* 访谈

本次测评采取访谈方式涉及对象为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面内容。其中安全物理环境、安全管理中心重点采取访谈方式。在访谈的广度上，访谈覆盖不同类型的系统运维管理人员，包括系统负责人、机房管理员、系统管理员、网络管理员、开发人员、应用业务人员、文档管理员等。对测评对象采取抽样的形式确定测评数量；在访谈的深度上，访谈包含通用和高级的问题以及一些有难度和探索性的问题。测评人员访谈技术负责人、系统管理员、业务开发人员等系统技术架构的实现及配置；访谈系统负责人系统的整体运行状况、安全管理中心的执行成效。

* 核查，包括文档核查及配置核查

本次测评采取核查方式主要涉及对象为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面的内容。除安全物理环境、安全管理中心主要采取文档核查方式外，其它方面主要采取系统配置核查方式。在核查的广度上，数量上采取抽样的形式，基本覆盖系统包含的网络设备、安全设备、主机设备、应用软件、管理制度文档等不同类型对象；在核查的深度上，详细分析、观察和研究除了功能级上的文档、机制和活动外，还包括总体/概要和一些详细设计以及实现上的相关信息。

* 测试，包括案例验证测试、漏洞扫描测试、渗透性测试。

本次测评采取测试方式主要涉及对象为安全通信网络、安全区域边界、安全计算环境等方面的内容。其中，验证测试主要通过测试工具或案例验证安全通信网络、安全区域边界、安全计算环境，安全管理中心的安全功能是否有效。漏洞扫描测试主要分析网络设备、操作系统、数据库等安全漏洞。在核查的广度上，基本覆盖不同类型的机制，在数量、范围上采取抽样方式；在测试的深度上，功能测试涉及机制的功能规范、高级设计和操作规程等文档及深度验证系统的安全机制是否实现，包括冗余机制、备份恢复机制的实现。基于本系统存在来自上级安全域和下级安全域可能的攻击威胁，故本次测评采取渗透测试方式，试图模拟非授权进入信息系统。

* 风险分析方法

本项目依据安全事件可能性和安全事件后果对信息系统面临的风险进行分析，分析过程包括：

1）判断信息系统安全保护能力缺失（等级测评结果中的部分符合项和不符合项）被威胁利用导致安全事件发生的可能性；

2）判断安全事件对信息系统业务信息安全和系统服务安全造成的影响程度；

3）综合1）和2）的结果对信息系统面临的风险进行汇总和分等级；

4）结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。