附件2

**广元市妇幼保健院**

**三级等保采购项目市场询价清单**

**项目清单及技术参数要求**

## 一、测评对象

|  |  |
| --- | --- |
| 系统名称 | 安全等级 |
| 医院核心业务系统 | 三级 |

二、测评要求

根据项目需求，为保障信息安全现场测评过程安全可控，明确测评人员职责分配、规范测评人员操作，保障测评结果有效，至少包括以下几个流程：

| 序号 | 关键实施阶段 | 工作要求 |
| --- | --- | --- |
| 1 | 确定测评范围 | 明确本次被测评信息系统的范围，包括每个信息系统的范围、信息系统的边界等。 |
| 2 | 获得信息系统的信息 | 通过调查或查阅资料的方式，了解被测评信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等。 |
| 3 | 确定具体的测评对象 | 初步确定每个信息系统的被测评对象，包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。 |
| 4 | 确定测评工作的方法 | 根据信息系统安全等级情况、系统规模大小等，明确本次测评的方法。 |
| 5 | 制定测评工作计划 | 制定测评工作计划或方案，说明测评范围、测评对象、工作方法、人员组成、角色职责、时间计划等。 |
| 6 | 实施等级保护测评 | 实施测评，包括人工检查、工具扫描等方式。 |
| 7 | 项目总结 | 对测评结果进行总结、汇报 |

三、测评内容

1、按照信息系统等级保护测评依据开展测评工作（包括不限于以下项目）

（1）安全物理环境测评：物理安全检测应当包含：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、电磁防护等十个单元。

（2）安全通信网络测评：安全通信网络测评应当包含：网络架构、通信传输、可信验证等。

（3）安全区域边界主机安全测评：安全区域边界测评应当包含：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等。

（4）安全计算环境测评：安全计算环境测评应当包含：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。

（5）安全管理中心测评：系统管理、审计管理、安全管理、集中管控。

2、信息系统管理安全测评

（1）安全管理制度测评：安全管理制度测评应当包含：安全策略、管理制度、制定与发布、审批和修订。

（2）安全管理机构测评：安全管理机构测评应当包含：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

（3）安全管理人员测评：安全管理人员测评应当包含：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。

（4）安全建设管理测评：安全建设管理测评应当包含：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。

（5）安全运维管理测评：安全运维管理测评应当包含：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。

四、项目管理

投标供应商必须提供完整的项目管理方案，投标供应商需要针对以下项目管理要求进行项目管理服务要求进行承诺，未提供项目管理服务承诺为无效投标人。

（1）投标供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任；

（2）应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力；

（3）投标供应商在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留；

（4）投标供应商的岗位配置要至少配置测评师、项目经理、渗透工程师、质量主管等并明确各个岗位的相关职责。

（5）测评工具要求

①采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件；

②采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品；

③采用的测评工具的生产商应为正规厂商，能够对产品进行持续更新并提供质量和安全保障；

④测评机构所使用的测评工具不会对单位系统产生破坏或负面影响以及不影响医院业务正常开展。

五、交付产物

包括但不仅限于以下资料：

|  |  |
| --- | --- |
| 1 | 信息系统安全等级测评报告（包含整改建议） |
| 2 | 其他未列入的应交资料 |

六、此次依据的标准包括但不限于以下内容：

（1）《信息安全等级保护管理办法》（公通字[2007]43号）

（2）《信息安全技术网络安全等级保护基本要求》GB/T22239-2019

（3）《信息安全技术信息系统安全等级保护定级指南》GB/T22240-2008

（4）《信息安全技术信息系统安全等级保护实施指南》GB/T25058-2010

（5）《信息安全技术信息安全风险评估规范》GB/T20984-2007

（6）《信息安全技术信息系统安全等级保护测评要求》GB/T28448-2012

（7）《信息安全技术信息系统安全等级保护测评过程指南》GB/T8449-2012

（8）《中华人民共和国网络安全法》