**采购需求**

1. 项目概况

依据《中华人民共和国网络安全法》《信息安全等级保护管理办法》的相关要求，对我院重要信息系统进行等级测评，包括：安全技术测评、安全管理测评等，形成差距分析报告，编制系统安全整改方案，编制和完善安全管理制度等。

1. 技术、服务要求
2. 标准和规范

《中华人民共和国网络安全法》

《信息系统安全等级保护管理办法》（公通字〔2007〕43号）

《GB/T22240-2020信息安全技术 网络安全等级保护定级指南》

《GB/T22239-2019信息安全技术 网络安全等级保护基本要求》

《GB/T25058-2019信息安全技术 网络安全等级保护实施指南》

《GB/T28448-2019信息安全技术 网络安全等级保护测评要求》

《GB/T28449-2018信息安全技术 网络安全等级保护测评过程指南》

《关于信息系统安全等级保护工作的实施意见》（公通字〔2004〕66号）、

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861 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）

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071号）

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]967号）等文件精神，

《医疗署办公厅关于地方医疗机关信息系统安全等级保护工作有关问题的通知》（审办计发[2012]105号）

结合业主单位工作实际，现拟对业主单位重要信息系统实施等级保护测评，以进一步完善信息系统安全管理体系和技术防护体系，切实提高系统信息安全防护能力，为医疗信息化建设的健康有序发展提供可靠保障。

1. 测评范围

|  |  |  |
| --- | --- | --- |
| 系统名称 | 安全保护等级 | 测评地点 |
| 医院信息系统 | 二级 | 寿县县医院院内 |

1. 测评内容

（1）安全技术测评。包括物理安全、网络安全、主机系统安全、应用安全和数据安全等五个方面的安全测评。

（2）安全管理测评。包括安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

（3）形成差距分析报告。依据测评结果和《信息系统安全等级保护基本要求》（GB /T 22239），对各信息系统进行安全现状分析，形成相应的差距分析报告。

（4）编制系统安全整改方案。依据《信息系统安全等级保护基本要求》和《信息系统等级保护安全设计技术要求》，结合差距分析结果，编制针对各信息系统的安全整改建设方案。

（5）编制和完善安全管理制度。依据《信息系统安全等级保护基本要求》和《信息系统等级保护安全设计技术要求》，协助业主单位制订和完善各项信息安全管理制度，规范信息安全日常管理工作，提高信息安全基础管理水平。

完成上述测评工作和实施整改后，出具符合公安机关要求的（年度）信息系统安全保护等级测评报告。

1. 实施要求
2. 实施原则

保密性原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购人网络的行为，否则采购人有权追究责任。

规范性原则：成交供应商工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制；

可控性原则：测评的工具、方法和过程需在双方认可的范围之内并符合进度表的安排，保证采购人对服务工作的可控性；

整体性原则：测评和分析的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患；

最小影响原则：测评工作应尽可能小的影响系统和网络的正常运行，不能对现网的运行和业务的正常提供产生显著影响(包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况应在应答书上详细描述)；

标准性原则：测评及评估方案的设计与实施应依据国家的相关标准进行。

1. 实施要求

应详细描述信息系统安全等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、时间安排、阶段性文档提交和验收标准等。应详细描述测评及评估人员的组成、资质及各自职责的划分。应配置经验丰富的测评及评估人员进行信息系统安全等级保护测评工作。

1. 测评及测评方法
2. 访谈

访谈是指测评人员通过与被测系统有关人员（个人/群体）进行交流、询问等活动，获取证据以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，访谈方法主要应用于安全管理机构测评、人员安全管理测评、系统建设管理测评和系统运维管理测评等安全管理类测评任务中。

在安全管理类测评任务中，测评人员依据定制的测评指导书（访谈问题列表）对相关人员进行访谈，获取与安全管理有关的测评证据用于判断特定的安全管理措施是否符合国家相关标准以及委托方的实际需求。

在安全功能检查任务中，测评人员依据定制的测评指导书（访谈问题列表）对相关人员进行访谈，为后续的检查和测试收集必要的系统基本信息并提供参考数据。

1. 检查

检查是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，检查方法的应用范围覆盖了物理安全测评、主机安全测评、网络安全测评、应用安全测评和数据安全及备份恢复等技术类测评任务，以及安全管理类测评任务。

在物理安全测评任务中，测评人员采用文档查阅与分析和现场观测等检查方法来获取测评证据（如机房的温湿度情况），用于判断目标系统在机房安全方面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。

在主机安全测评、网络安全测评、应用安全测评和数据安全及备份恢复等测评任务中，测评人员综合采用文档查阅与分析、安全配置核查和网络监听与分析等检查方法来获取测评证据（如相关措施的部署和配置情况，特定设备的端口开放情况等），用于判断目标系统在主机、网络和应用层面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。

在安全管理类测评任务中，测评人员主要采用文档查阅与分析的检查方法来获取测评证据（如制度文件的编制情况），用于判断特定的安全管理措施是否符合国家、行业相关标准的要求以及委托方的实际需求。

1. 测试

测试是指测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看、分析这些行为的结果，获取证据以证明信息系统安全保护措施是否有效的一类方法。在本次测评过程中，测试方法主要应用在手工验证、漏洞扫描等测评任务中。

在网络安全、主机安全和应用安全等测评任务中，测评人员将综合采用手工验证和工具测试方法对特定安全技术措施的有效性进行测试，测试结果用于判断目标系统在网络、主机或应用层面采用的特定技术措施是否符合国家相关标准以及委托方的实际需求，并进一步应用于对目标系统进行安全性整体分析。

1. 人员要求

1、供应商拟派的安全服务团队不得少于4人。

2、投标人为本项目配备的质量经理具有等级测评师证书（高级）；

3、投标人为本项目配备的项目经理具有等级测评师证书（高级）且同时具备注册信息安全专业人员（CISP）证书、信息安全保障人员认证（CISAW）类证书（中级）、高级信息系统监理证书；

4、除项目经理、质量经理外，投标人为本项目配备的项目测评人员具有信息安全等级测评师证书（中级及以上）；

5、除项目经理、质量经理外，投标人为本项目配备的安全服务人员具有注册信息安全工程师（CISP）证书、高级大数据技术工程师证书、软件测评师、全国工业和信息化应用人才测评证书。

注：响应材料须提供证书扫描件或影印件并加盖供应商公章。

1. 其他
2. 时间要求：测评工作应在45个工作日内完成。
3. 中标人协助采购人进行备案工作。
4. 验收标准：按等保要求，完成规定工作内容，并提供相关过程文档和系统测评报告，经采购人确认后视为验收完成。