雷山县人民医院网络安全等级保护系统测评

服务项目服务内容及要求

一、适用范围

1.本技术规范提出的是最低限度的技术要求。凡本技术规范中未规定，但在相关国家标准中有规定的规范条文，应按相应标准的条文进行服务供应说明。

2.如果没有以书面形式对本技术规范的条文提出异议，则认为提供的服务完全符合本技术规范。

3.本技术规范所建议使用的标准如与所执行的标准不一致，应按更严格标准的条文执行或按双方商定的标准执行。

二、标准和规范

下列文件中的条款通过本规范的引用而成为本规范的条款，除本技术规范书特别规定外，所提供的测评标准均应遵循公安部相关文件要求，所用的标准必须是其最新版本；如果这些标准内容矛盾时，应按最高标准的条款执行或按双方商定的标准执行。1.《中华人民共和国网络安全法》；2.《信息安全等级保护管理办法》（公通字〔2007〕43号）；3.《GB/T22239-2019信息安全技术 网络安全等级保护基本要求》；4.《GB/T22240-2019信息安全技术 网络安全等级保护定级指南》；5.《GB/T25058-2010信息安全技术 信息系统安全等级保护实施指南》；6.《GB/T28448-2019信息安全技术 网络安全等级保护测评要求》；7.《GB/T28449-2018信息安全技术 网络安全等级保护测评过程指南》。

三、测评范围

|  |  |  |  |
| --- | --- | --- | --- |
| **系统名称** | **安全保护等级** | **测评地点** | **备注** |
| 核心业务系统 | 二级 | 雷山县人民医院 | 包含医院信息系统（HIS）、电子病历系统（EMR）、影像系统（PACS） |

四、技术要求

**（一）测评及评估原则**

1.保密性原则：成交供应商应与采购人签订保密协议，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，不得利用此数据侵害的权益，否则有权追究责任。

2.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。

3.规范性原则：成交供应商工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

4.可控性原则：项目的进度应符合进度安排，保证对测评工作的可控性。

5.整体性原则：测评及评估的范围和内容应系统、全面、规范，满足等级保护的相关基本要求。

6.最小影响原则：技术测评及评估工作应尽可能小地影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评及评估应在许可的条件下进行。

**（二）测评及评估方法**

1.测评及评估方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地查看等多种方法。

2.如需对系统安全等级保护测评实施过程中采用在线测评工具，各种工具软件由成交供应商推荐，经确认后由成交供应商提供并在工作中使用。

3.安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由成交供应商推荐，经确认后由成交供应商提供并在测评中使用。

**（三）等级保护测评内容**

根据国家等级保护相关标准，本次项目的安全等级保护测评应包括以下内容：

**1.安全技术测评：**包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评；

**2.安全管理测评：**包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。

（1）安全物理环境。安全物理环境针对物理机房提出了安全控制要求，主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置选择、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）安全通信网络。安全通信网络针对网络架构和通信传输提出了安全控制要求。主要对象为广域网、城域网、局域网的通信传输以及网络架构等；涉及的安全控制点包括网络架构、通信传输和可信验证。

（3）安全区域边界。安全区域边界针对网络边界提出了安全控制要求，主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计和可信验证。

（4）安全计算环境。安全计算环境针对边界内部提出了安全控制要求，主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、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、剩余信息保护和个人信息保护。

（5）安全管理中心。安全管理中心针对整个系统提出了安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

（6）安全管理制度。安全管理制度测评是对信息系统的安全管理制度体系和制度内容、制定和发布流程、评审和修订机制等情况进行测评涉及的控制点包括：安全策略、管理制度、制定和发布、评审和修订。

（7）安全管理机构。安全管理机构测评是对信息系统的安全管理组织和岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

（8）安全管理人员。人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗、安全意识教育和培训，以及外部人员访问管理等情况进行测评。

（9）安全建设管理。系统建设管理测评是对信息系统建设过程中的定级和备案、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、服务供应商选择进行测评。

（10）安全运维管理。系统运维管理测评是对信息系统运行维护过程中的环境管理、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、备份和恢复管理、安全事件处置、应急预案管理、外包运维管理进行测评。

**（四）交付文档**

| 序号 | 项目阶段 | 输出成果 |
| --- | --- | --- |
| 1 | 测评准备阶段 | 《测评计划书 》《调研结果报告》《工具清单》《信息安全等级保护测评方案》《测评指导书》 |
| 2 | 现场测评阶段 | 《网络安全等级保护测评过程文档》 |
| 3 | 现场结果分析 | 《网络等级安全保护测评加固建议方案》 |
| 4 | 报告编制 | 《网络安全等级保护测评报告》 |
| 5 | 备案 | 《等保定级报告》《备案表》 |
| 6 | 安全服务 | 《安全培训方案和相关文档》《漏洞扫描报告》《渗透测试报告》 |