技术参数要求

1. 项目概况

依据《中华人民共和国计算机信息系统安全保护条例》（国务院令 147 号），我国先后颁布了《信息安全等级保护管理办法》（公通字[2007]43 号）、《信息安全技术 信息系统安全等级保护测评过程指南》、《信息安全技术 信息系统安全等级保护测评要求》、《网络安全法》等一系列信息化安全防御体系建设有关的法律法规和技术标准，信息化建设都需要落实网络安全等级测评制度，以提高本单位的信息化安全防御能力和水平。

因此，为贯彻落实我国信息安全等级评测的有关要求，西平县人民医院需要对涉及的信息系统进行安全等级测评，以进一步提高自身信息系统安全保护能力。

2. 需遵循的政策法规及行业规范

2.1 需遵循的政策法规

（1）《中华人民共和国网络安全法》

（2）《中华人民共和国保守国家秘密法》

（3）《中华人民共和国保守国家秘密法实施办法》

（4）《中华人民共和国国家安全法》

（5）《中华人民共和国计算机信息系统安全保护条例》

（6）《计算机信息系统保密管理暂行规定》

（7）《计算机信息系统国际联网保密管理规定》

（8）《中华人民共和国计算机信息网络国际联网管理暂行规定》

（9）《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》

（10）《计算机病毒防治管理办法》

（11）《计算机信息网络国际联网安全保护管理办法》

（12）《计算机信息系统安全专用产品分类原则》

（13）《互联网电子公告服务管理规定》

（14）《计算机信息系统安全等级保护划分准则》

（15）《计算机信息系统安全等级保护网络技术要求》

（16）《计算机信息系统安全等级保护操作系统技术要求》

（17）《计算机信息系统安全等级保护数据库管理系统技术要求》

（18）《计算机信息系统安全保护等级划分准则》

（19）《计算机信息系统安全等级保护通用技术要求》

（20）《计算机信息系统安全等级保护管理要求》

（21）《计算机机房场地安全要求》需遵循的行业规范

其他政策法规；

（1）《中华人民共和国计算机信息系统安全保护条例》

（2）《信息安全等级保护管理办法》

（3）《国家电子政务工程建设项目管理暂行办法》

（4）《信息安全等级保护安全建设整改工作指导意见》

（5）《信息安全技术 网络安全保护等级保护测评要求》

（6）《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》

（7）《信息安全技术 网络安全等级保护定级指南》

（8）《信息安全技术 网络安全等级保护基本要求》

（9）《信息系统安全等级保护实施指南》

（10）《信息安全等级保护安全建设整改工作指南》

3. 项目范围

根据西平县人民医院已规划的业务信息系统，参照《信息系统安全等级划分准则》、《信息安全技术信息系统安全等级保护定级指南》文件要求，对业务系统拟定安全保护等级并开展相应级别的等级保护测评工作。

序号	系统范围	级别
1	HIS 信息系统	二级
2	LIS 信息系统	二级
3	PACS 信息系统	二级
4	EMR 信息系统	二级

4. 具体要求

项目总体管理和技术要求：总体要求与《信息安全等级保护管理办法》、《信息系统安全等级保护实施指南》和《信息安全等级保护安全建设整改工作指导意见》等网络安全等级保护系列文件要

求保持一致，开展网络安全等级测评工作。具体网络安全技术标准以文件相应部分提及的为准。

4.1 等级测评要求

（1）项目内容

本项目**按照网络安全等级保护 2.0** 测评标准进行安全等级测评。具体项目测评内容如下：

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。

安全管理测评：安全管理机构、安全管理制度、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控制测评。

（2）具体要求

在安全等级测评过程中，每个工作阶段、流程、内容、及成果交付严格遵循《信息安全技术 网络安全等级保护测评要求》和《信息安全技术 网络安全等级保护测评过程指南》文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告，测评报告需得到项目单位的确认，并报送网安部门审核、批复。测评报告编制的内容及格式严格遵照《网络安全等级保护测评报告模版（现行版）》进行。

测评技术团队符合《网络安全等级保护测评机构管理办法》对测评机构和测评人员管理的要求，项目负责人由公安部培训考核认证通过的信息安全高级等级测评师承担，通过注册信息安全专业认证、具备良好的教育背景、受过专业的技术培训、拥有丰富的行业

安全服务工作经验，对用户在信息系统安全等级测评过程中可能会面临的各类技术问题提供及时解决方案。

（3）项目交付成果

项目阶段各阶段的测评过程文档（参照《信息安全技术 网络安全等级保护测评过程指南》）编制。相见下表（包括但不限于）

项目阶段	交付成果
测评准备活动	项目计划书 被测系统基本情况分析报告
方案编制活动	测评指导书 信息系统安全测评方案
现场测评活动	测评结果记录 测评中发现的问题汇总
分析与报告编制活动	单项测评结果汇总分析 整体测评结果汇总分析 风险分析和评估 等级测评结论 信息系统安全等级测评报告

整改建议要求

（1）具体要求

依照《信息安全等级保护安全建设整改工作指导意见》，严格遵循《信息安全等级保护安全建设整改工作指南》各项要求，在系统测评工作的基础上，对信息系统总体信息安全管理和技术方面现

状进行全面的分析，制订信息安全等级保护安全建设整改方案，方案内容包含但不限于：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全建设整改技术方案设计、安全建设整改管理体系设计、信息系统安全产品选型及技术指标建议、安全建设整改项目实施计划、项目预算，整改后可能存在的其他问题。

（2）工作过程文件及项目交付成果（包括但不限于）

安全等级测评整改技术方案，方案可根据整改和规划内容的重要性和复杂程度采用分册方式编写。

（3）提交要求

需包含如下内容：

方案分项	详细内容及要求
等级化安全保障建议方案	内容应包括但不限于以下方面： 1、安全区域和等级划分； 2、安全体系框架设计； 3、等级化安全指标体系报告。
安全体系建设建议方案	内容应包括但不限于以下方面： 1、网络面临风险分析； 2、针对性措施建议。
相关网络安全 管理制度	内容应包括但不限于以下方面： 1、机房安全管理制度； 2、网络故障应急预案及应急方案流程制

	度； 3、客户端管理制度； 4、数据备份及恢复制度； 5、灾难恢复策略及制度。

4.2 应急响应要求

为西平县人民医院建立安全应急预案，遇到重大安全事件如网络入侵、大规模病毒爆发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决时，需供应商安排专业技术人员以 7*24 小时远程、电话、邮件及现场等方式提供应急响应支持，快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响，查明安全事件原因，确定安全事件的威胁和破坏的严重程度，并根据对事件的分析及原因提供相应的解决方案。

服务要求

在发现安全事件时，须及时判断安全事件的级别。针对严重的安全事件，对安全事件进行紧急分析处理、灾难恢复和和入侵追踪和取证，并出具应急响应报告（含加固建议）。

建立长期稳定的本地专业安全服务团队，并通过专业认证，在发生重大安全事件时，在半小时内提供现场应急响应；在发生一般安全事件时，一小时内提供现场应急响应。

4.3 安全咨询要求

安全服务机构建立专业团队对网络安全现状进行调研、梳理，按照国家等级保护相应等级要求、公安部的网络安全要求及信息安

全规划，以 ISO27000、ITIL 系列标准以及国际、国内最佳实践为指导，提供信息安全等级保护等相关安全咨询服务，保证本项目建设期内持续性、连续性安全需求。咨询服务内容包括：安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和运维等信息安全服务咨询；系统定级、备案、测评、建设整改等咨询； 信息技术服务管理体系（ISO/IEC 20000-1:2011）、信息安全管理体系认证（ISO/IEC 27001:2013）等合规咨询。

服务要求

安全管理体系建设规划要求能够落地，明确信息安全管理的方针、目标和对象。在信息安全管理标准框架下，通过制订各项信息安全管理制度，规范信息安全日常管理工作，切实提高信息安全基础管理水平，实现制度化、流程化、体系化的管理思想。

5. 项目工期

45 个工作日（整改时间除外）

6. 项目成果

（1）《网络安全等级测评报告》

（2）《网络安全等级测评整改建议》

7. 项目验收

7.1 验收条件

（1）完成各个信息系统的等级测评工作并提交等级测评报告；

（2）提交测评各个阶段的文档；

(3)协助我院取得网监部门颁发的等保备案证明.