

## 附件 3:

# 西双版纳州人民医院 2025 年等保测评服务采购项目需求

## 一、建设依据

项目要求为医院提供等级保护测评及安全服务，该服务须参照以下法律、行政法规、部门规章、国家标准执行：

《中华人民共和国网络安全法》

《中华人民共和国个人信息保护法》

《信息安全等级保护管理办法》

《信息安全技术 网络安全等级保护定级指南》GB/T 22240-2020

《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019

《信息安全技术 网络安全等级保护测评要求》GB/T 28448-2019

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

《关于进一步做好网络安全等级保护有关工作的函》公网安〔2025〕1001 号

《关于对网络安全等级保护有关工作事项进一步说明的函》公网安〔2025〕1846 号

《网络安全等级保护测评高风险判定实施指引(试行)》的通知公网安〔2025〕2391 号

## 二、服务要求

序号	服务名称	服务内容
1	等保测评	按国家及公安机关的法律法规和规章制度的要求，结合医院实际情况，开展西双版纳傣族自治州人民医院互联网医院系统、影像归档和通信系统、智慧医院信息系统平台、集成平台 4 个系统的等级保护测评工作，检测评估被测系统安全等级保护状况是否达到相应等级基本要求，并协助西双版纳州人民医院完成系统备案工作，最终通过三级等保测评。
2	网络安全培训服务	本次服务要求服务方需针对医院内不同层次的安全需求而定制对应的安全培训，全面融合技术和管理要素。借助各项培训课程，提高从一般性的安全意识、到具体的安全攻防操作、再到高级的信息安全管理在内的全方位的安全知识和技能。
3	安全管理体系建设服务	协助医院进行安全管理体系建设，依据等级保护三级要求中管理制度相关要求，根据单位实际情况，建立健全单位内安全管理制度文档，全方位保障单位内各信息系统的的天性。

## 三、采购预算：14.8 万元

## 四、采购项目服务期限和地点

- 1、服务期限：服务期限为一年，自双方正式签订合同之日起计算。
- 2、服务地点：采购人指定地点

## 五、详细服务内容

## 1.等保测评

安全层面	安全控制点	安全层面	安全控制点
1.安全物理环境	物理位置选择	4.安全计算环境	身份鉴别
	物理访问控制		访问控制
	防盗窃和防破坏		安全审计
	防雷击		入侵防范
	防火		恶意代码防范
	防水和防潮		可信验证
	防静电		数据完整性
	温湿度控制		数据保密性
	电力供应		数据备份恢复
	电磁防护		剩余信息保护
2.安全通信网络	网络架构	5.安全管理中心	个人信息保护
	通信传输		系统管理
	可信验证		审计管理
3.安全区域边界	边界防护		安全管理
	访问控制	6.安全管理制度	集中管控
	入侵防范		安全策略
	恶意代码和垃圾邮件防范		管理制度
	安全审计		制定和发布
	可信验证		评审和修订

安全层面	安全控制点		
7.安全管理机构	岗位设置	10.安全运维管理	环境管理
	人员配备		资产管理
	授权和审批		介质管理
	沟通和合作		设备维护管理
	审核和检查		漏洞和风险管理
8.安全管理人员	人员录用		网络和系统安全管理
	人员离岗		恶意代码防范管理
	安全意识教育和培训		配置管理
	外部人员访问管理		密码管理
9.安全建设管理	定级和备案		变更管理
	安全方案设计		备份与恢复管理
	产品采购和使用		安全事件处置
	自行软件开发		应急预案管理
	外包软件开发		外包运维管理
	工程实施		
	测试验收		
	系统交付		
	等级测评		
	服务供应商选择		

### ①系统备案

协助医院填写备案所需资料，并携带备案资料到属地公安机关网安部门完成备案工作。

## ②报告编制

在完成现场检查工作后，经过后期的综合分析与风险判断，确定等级保护测评结论，严格按照《关于进一步做好网络安全等级保护有关工作的函》公网安〔2025〕1001号印发的《附件3：网络安全等级保护[被测对象名称]等级测评报告（2025版）》编写等级保护测评报告。

### 2.网络安全培训服务

为了保证整个系统稳定运行，提高其使用效率和安全性，需要对用户的系统管理人员进行相关技术培训，使他们能掌握各安全产品的配置、故障诊断、设备管理、达到能独立进行日常管理，以保障系统的正常运行。因此，为用户培训出一支有较高水平的技术队伍，来保证整个系统的安全运行，是十分重要的。针对此次项目提供全面的安全培训，其内容涉具体培训内容如下：

等级保护政策标准及内容培训

信息安全意识及终端安全培训

《网络安全法》培训

网络安全加固及运维技术培训

主机安全加固及运维技术培训

其他培训（根据实际需求定制）

### 3.安全管理体系建设服务

对现有安全管理体系、安全管理制度进行梳理、修订、补充，形成建立由安全策略、管理制度、操作规程、执行记录等构成的全面的信息安全管理制度体系，包含：安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理5个层面，最终满足等级保护三级要求。

安全方针和主策略

最高方针，纲领性的安全策略主文档，陈述本策略的目的、适用范围、信息安全管理意图、支持目标以及指导原则，信息安全各个方面所应遵守的原则方法和指导性策略。

#### 安全管理制度和规范

各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法。依据《信息安全技术 信息系统安全等级保护基本要求》，安全管理体系包含：安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理 5 个层面。

#### 安全流程和操作手册

安全流程和操作规程，详细规定主要业务应用和事件处理的流程和步骤，和相关注意事项。作为具体工作时的依照，此部分必须具有可操作性，而且必须得到有效推行和实施。

#### 安全记录单

安全记录单，落实安全流程和操作规程的具体表单，根据不同等级信息系统的要求可以通过不同方式的安全记录单落实并在日常工作中具体执行。主要包括日常操作的记录、工作记录、流转记录以及审批记录等。