# ****医院网络安全等级保护测评服务****

# ****项目参数及要求****

# ****1.服务要求****

## **1.1.**等保测评服务****

1. **定级备案**

依据《信息安全等级保护定级指南》（GB/T22240-2020）的要求，各信息系统将以系统为单位开展定级工作。定级工作主要是依据业务信息安全和系统服务安全两方面的重要程度来确定安全等级。

**主要定级流程如下：**

1. 确定作为定级对象的信息系统；
2. 确定业务信息和系统服务安全受到破坏时所侵害的客体；
3. 根据不同的受侵害客体，综合评定对客体的侵害程度；
4. 确定业务信息和系统服务两方面安全保护等级；
5. 确定信息系统安全保护等级；
6. 形成各信息系统的《定级报告》；
7. 完成各信息系统的《备案表》；
8. 专家对《定级报告》、《备案表》进行评审；
9. 报送信息安全等级保护工作协调小组，获得《备案证明》。

**2）等级保护测评**

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》（GB/T 28448-2019)和《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）文件，根据系统等级开展相应级别的单项测评和整体测评。测评报告内容及格式严格遵照《网络安全等级保护测评报告模版（2021年版）》。

按照《信息安全等级保护管理办法》、《信息安全技术 网络安全等级保护实施指南》（GB∕T 25058-2019），遵循《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）等技术标准，从每个信息系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等10个层面进行测评，依据信息系统的业务应用和内外部环境，深入调研分析各信息系统资产状况和重要性程度，以及面临网络安全的威胁。

**服务频次及周期：两个等保二级信息系统（医院HIS系统和医院网站），服务周期两年。**

**工作过程文件及项目交付成果（包括但不限于）：《网络安全等级保护测评报告》、《备案证明》**

## **1.2.**风险评估服务****

**1）标准依据**

本次评估所依据的标准规范为《GB/T 20984-2007信息安全技术信息安全风险评估规范》

**2）评估工作过程**

GB/T 20984-2007规定了风险评估的实施流程，根据流程中的各项工作内容，一般将风险评估实施划分为评估准备、风险要素识别、风险分析与风险处置四个阶段。其中，评估准备阶段工作是对评估实施有效性的保证；风险要素识别阶段工作主要是对评估活动中的各类关键要素资产、威胁、脆弱性、安全措施进行识别与赋值；风险分析阶段工作主要是对识别阶段中获得的各类信息进行关联分析，并计算风险值；风险处置建议工作主要针对评估出的风险，提出相应的处置建议，以及按照处置建议实施安全加固后进行残余风险处置等内容。

**3）准备阶段**

风险评估的准备阶段的主要工作内容有：培训与编制计划。

培训一般指评估方根据评估目标，对项目组进行培训。所有培训均采用培训记录方式进行留档备案。风险评估计划由项目组组长与被评估方进行充分沟通，编制出本次风险评估项目计划草案，一般包括工作目标、评估范围、项目实施的团队、评估的依据和方法、本次风险评估工作成果等内容。草案提交整个风险评估小组进行会议审定，项目组组长按照审定意见进行修改，形成风险评估方案

**4）资产识别**

资产识别工作主要参照GB/T 20984-2007《信息安全风险评估规范》及《信息安全风险评估认证实施细则》对资产分类和资产赋值。

**5）威胁识别**

威胁识别工作主要参照GB/T 20984-2007《信息安全风险评估规范》及《信息安全风险评估认证实施细则》对威胁识别和赋值。

结合一系列成熟的调研参考表对威胁进行识别确认。

**6）脆弱性识别**

脆弱性识别是风险评估中最重要的一个环节。脆弱性可从技术和管理两个方面进行识别。技术方面，可从物理环境、网络、主机系统、应用系统、数据等方面识别资产的脆弱性；管理方面，可从安全管理机构、安全管理策略、安全管理制度、人员安全管理、系统运维管理等方面识别其脆弱性。

**7）已有安全措施确认**

在识别脆弱性同时，评估人员应对已采取的安全措施及其有效性进行确认。安全措施的确认应分析其有效性。对有效的安全措施继续保持，以避免不必要的工作和费用；对认为不适当的安全措施应与被评估方共同核实是否需要取消或对其进行修正。

**8）风险分析**

风险评估的结果进行等级化处理，一般分为5级。根据所采用的风险计算方法（明确：风险计算方法），计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。

**9）协助整改**

风险分析工作完成之后生成安全风险清单，基于风险清单确认风险是否可接受，如果不可能接受协助医院整改，按照风险问题的不同提供相应整改支撑工作。

**服务频次及周期：每年一次，服务周期两年。**

**工作过程文件及项目交付成果（包括但不限于）：《风险评估报告》。**

## **1.3.**网络安全培训服务****

根据不同的用户类型安排有针对性地培训内容。

**管理人员主要包括：高层管理、业务专家等。**

培训目标：对管理人员的培训，目的是使他们了解国家相关部门对系统信息安全管理和建设的相关标准，同时建立起一套具有针对性和适用性的安全管理办法。

**技术人员主要包括：操作人员、开发人员、维护人员等。**

培训目标：对技术人员的培训，目的是使他们了解信息系统所面临的严峻安全威胁和挑战，以及如何进行全面有效的安全防护措施。

**全员培训主要包括：安全意识培训等。**

培训目标：全体成员的培训，目的是让大家对信息安全的有初步的认识和逐步增强安全意识，让安全事故可以得到有效地避免。

**服务频次及周期：每年一次，服务周期两年。**

**工作过程文件及项目交付成果（包括但不限于）：《培训课件》。**

## **1.4.**漏洞扫描服务****

对医院系统资产开展例行安全扫描、对扫描出漏洞进行漏洞验证，确认漏洞是否存在。对漏洞整改开展支撑和复测等工作，积极跟踪漏洞的整改状态，提出可落地的整改建议。

采用行业认可、安全合规的漏洞扫描系统，通过定制的扫描规则，形成安全扫描策略文档，对服务器操作系统、网络设备、安全设备及应用层等进行自动化安全扫描，扫描内容包括但不限于空间资产探测、系统漏洞扫描、WEB漏洞扫描、网站安全监测、数据库漏洞扫描、基线配置核查、工控漏洞扫描、大数据漏洞扫描、Docker漏洞扫描、系统渗透测试、网络流量分析、源代码安全审计、离线弱口令扫描、木马病毒扫描、漏洞工单管理、视频监控安全检测、WIFI安全检测、APP漏洞扫描、Windows安全加固等保合规关联等进行全量漏洞扫描。输出安全扫描报告提供修复建议，并协助医院进行漏洞修复。

通过web后门检查工具，针对网站或应用系统服务器所有文件进行安全扫描，发现系统文件中潜在的webshell、网页后门等恶意文件，提供修复建议，并协助医院进行漏洞修复。

**服务频次及周期：每年一次，服务周期两年。**

**工作过程文件及项目交付成果（包括但不限于）：《漏洞扫描报告》。**

## **1.5.**应急演练服务****

## ****1.5.1.应急演练内容****

参考相关标准协助医院建立科学合理的应急演练，在医院的信息系统出现重大突发安全事件时可以通过前期预演达到的效果，最大程度减少信息安全事件造成的损害，保障医院信息系统安全。

### **1.5.2.**应急演练流程

安全应急演练服务为分三个阶段：应急演练准备阶段、应急演练实施阶段、应急演练收尾阶段：

应急演练准备：根据实际情况来进行制定演练的计划、演练方案，在计划、方案中要体现出安全事故的发生、人员的调动、事故的处理等详细的流程，并且在演练前对参与演练的动员人员进行培训、讲解。

应急演练实施：根据制定的演练方案来进行应急演练，安全事故发生、事故处理、业务恢复的一整套流程。

应急演练收尾：演练结束后，对此次演练的全过程进行评估总结。

**服务频次及周期：每年一次，服务周期两年。**

**工作过程文件及项目交付成果（包括但不限于）：《应急演练脚本及总结》。**

## **1.6.**应急响应支撑服务****

针对医院可能发生的主要三大类紧急事件（病毒和蠕虫事件、黑客入侵事件、误操作或设备故障事件）进行快速响应，最大程度上减少因为信息安全事件而带来的直接或间接的经济损失，缩小事件影响范围。

根据以上分类事件进行应急响应，具体到常见安全事件主要为病毒暴发、入侵和DDOS攻击、页面篡改、设备故障等问题，响应流程如下：

1）事件响应

分析小组接到值班人员有关事件的汇报后，首先通过电话指导值班人员对问题进行分析，根据问题分析的情况准备相应工具并立即赶赴现场。

2）调查分析

分析小组到达现场对防火墙、操作系统、审计系统、应用系统的日志进行分析，定位事件的类型，事件产生并保存相应的数据（如日志）。

3）制定方案

根据调查分析的结果，评估事件影响的主机与系统。根据事件的影响选择安全措施，制定响应方案。

4）安全措施

针对不同的安全事件，专业化定制不同的安全措施，主要为遏制影响范围，对系统进行备份、恢复、安全加固以及对攻击的反向追踪。

**服务频次及周期：按需，服务周期两年。**

**工作过程文件及项目交付成果（包括但不限于）：《应急响应支撑报告》。**

# **2.**项目实施要求****

（1）成交供应商必须具备独立完成本项目的能力。

（2）成交供应商提供的资格、资质等证明文件应真实有效。

（3）成交供应商应对了解到的信息保密，并提供保密承诺。

（5）在进行整改过程中提供必要的技术支持。

（6）能按照规定的工作内容及进度安排协助完成风险评估服务。

## **3.**项目管理要求****

（1）兼容性要求

为了保障服务合规验收，要求测评报告所导出文件格式要求兼容国产办公软件，能生成.wps/.et/.dps等文件格式，能与国产办公软件的文字编辑、制作表格、演示文稿软件三个功能模块相互兼容。（投标文件中须提供符合上述要求的证书证明原件扫描件并加盖制造商公章证明，否则投标无效。）

1. 保密要求

保密要求须保证对本项目实施中所获得任何资料和信息严格保密，并签订保密责任书。

## ****4.技术要求****

（1）服务人员要求

要求投标人拟派一名项目经理，为了保障等保2.0 GB/T 22239-2019数据安全完整性和保密性要求，要求该项目经理具备中国信息安全测评中心颁发的注册数据安全治理（CISP-DSG）专业人员证书、全国计算机信息高新技术网络工程师考试合格（国家职业资格三级）证书（能够指导等保测评过程中对于物理环境、通信网络、安全边界、计算环境等方面出现的问题）。（**服务供应商须在服务响应文件中出具符合上述要求的服务承诺函并加盖公章，未提供则视为无效响应。**）（说明：签订合同前拟中标服务供应商须提供上述证书扫描件及开标前三个月投标人为其缴纳的社保证明材料加盖公章，未提供或提供不符合要求视为虚假应标取消中标资格。）

（2）服务工具

根据《GB/T22239-2019》网络安全等级保护通用要求，支持从物理环境、网络通信、安全边界等层面进行资产收集和梳理；同时能够对于近期需测评的等保系统与相应设备的维保状态进行告警提示。（**供应商须提供具有CMA及CNAS标识的第三方检测机构出具的以上功能检测报告原件扫描件及授权函加盖制造商公章，未提供或提供不符合要求视为无效响应。**）（需通过醒目标识标记出对应功能点在报告中的检测情况。）

**5.**其他要求****

1. **交货地点：**医院指定地点。
2. **交付期：**合同签订后30天内交付等保测评服务中《备案证明》、90天内交付《等保测评报告》。
3. **交付成果和服务要求：**

（1）按要求的时间节点，出具技术要求的信息系统《等保测评报告》等相关文档资料。

（2）在评估过程中、评估后提出整改意见和整改措施，配合好系统优化改进、测评等工作。

1. **付款方式：**

阶段性付款，具体付款方式成交后采购人与成交供应商双方协商。