**玉溪市人民医院**

**信息系统网络安全等级保护测评服务技术要求**

1. **采购标的需实现的功能或者目标**

本项目要求供应商依据国家有关信息系统等级保护的政策与技术标准，提供如下服务：

1. **项目服务范围**

|  |  |  |
| --- | --- | --- |
| **信息系统名称** | **等保定级** | **服务期（2025-2027年）** |
| **互联网医院管理信息系统** | **三级** | **三年** |
| **医院信息系统（HIS、电子病历、集成平台）** | **三级** | **三年** |

服务供应商应根据国家最新网络安全等级保护相关要求，结合玉溪市人民医院的实际情况，发现安全存在问题，并提出合理化建议，协助医院逐年完成网络安全等保测评工作。

**2、信息系统等保测评服务**

服务供应商依据网络安全等级保护相关标准，应包含但不限于从安全物理环境、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、安全运维管理十个层面开展测评工作，输出网络安全等级保护测评差距分析报告。

**3、信息安全等级保护整改建议和指导服务**

服务供应商根据医院信息系统等级保护测评情况，对系统发现的网络安全问题，向采购单位提供整改、加固建议，协助、指导采购单位做好整改工作。服务供应商根据系统往年的测评问题情况，向采购单位提出系统针对性的整改、加固建议，切实帮助采购单位对系统安全问题进行治理，直到达到国家三级等保要求为止。

1. **采购标的执行的标准规范**

按照如下国家发布的法律及等级保护相关标准文件要求开展信息系统测评工作：

《中华人民共和国网络安全法》 中华人民共和国主席令 第三十五号

《计算机信息系统 安全保护等级划分准则》GB 17859-1999

《信息安全技术 网络安全等级保护基本要求》GBT 22239-2019

《信息安全技术 网络安全等级保护安全设计技术要求》GBT 25070-2019

《信息安全技术 网络安全等级保护测评要求》GBT 28448-2019

《信息安全技术 网络安全等级保护测评过程指南》GBT 28449-2018

《信息安全技术 网络安全等级保护定级指南》GBT 22240-2020

《信息安全技术 网络安全等级保护测试评估技术指南》GBT 36627-2018

《信息安全技术 网络安全等级保护安全管理中心技术要求》GB∕T 36958-2018

《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》GBT 36959-2018

《信息安全技术 网络安全等级保护实施指南》GB/T 25058-20190

1. **采购标的需满足的服务标准、期限、效率等要求。**

**（一）网络安全等级保护测评技术要求**

根据网络安全相关要求，应逐年对玉溪市人民医院在当地监管部门进行备案的信息系统进行网络安全等级保护测评。

1. **服务周期和地点要求**

在本项目约定的服务要求基础上，根据实际情况与用户方，在服务周期和服务地点等方面进行再约定。

1. **测评服务标准规范要求**

等级保护测评要求：按照GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》、GB/T28448-2019《信息安全技术 网络安全等级保护测评要求》和GB/T28449-2018《信息安全技术 网络安全等级保护测评过程指南》文件要求开展信息系统测评工作。

1. **测评能力要求**
2. **测评服务要求**

提供 7×24 小时响应，提供完善现场保障服务，完成定级备案，提供完整的实施和现场保障方案。方案应包含：在项目实施过程中需对测评的信息系统提供数据保密协议，对系统的数据不外泄，不影响信息系统的正常使用。对信息系统的使用与测评实行规范化、流程化，提高工作效率。在项目全过程中，每周和每月需提交周报、月报，有需要定期举行项目例会，确保相关方能及时了解项目进展情况和相关信息。

1. **测评人员要求**

供应商参与业务方项目组的成员至少5人，参与项目的人员必须具备网络安全等级保护测评师资质（提供资质证书复印件），并提供现场服务。

供应商必须成立等级保护测评项目组，由项目负责人统一负责，项目负责人须具有一定的技术管理知识和经验，能够容易地与客户沟通，能够很好地执行并完成测评服务工作，并能根据一些特殊的情况可以适当增加服务人员，接受采购人的统一管理。

供应商派驻的测评项目负责人和测评服务人员必须固定，如有变更，必须经采购人同意并签字确认。供应商必须提供人员管理及配备方案，并确保其人员的稳定性。

1. **测评内容要求**
2. **安全技术测评**

主要包括：物理安全技术测评、网络安全技术测评、主机安全技术测评、应用安全技术测评、数据安全与备份恢复技术测评等五个层面上的测评。

**1）物理安全**

物理安全主要涉及的方面包括环境安全（防火、防水、防雷击等），设备和介质的防盗窃防破坏等方面。须测评以下十个控制点：

控制点一：物理位置的选择；

控制点二：物理访问控制；

控制点三：防盗窃和防破坏；

控制点四：防雷击；

控制点五：防火；

控制点六：防水和防潮；

控制点七：防静电；

控制点八：温湿度控制；

控制点九：电力供应；

控制点十：电磁防护；

**2）网络安全**

网络安全主要涉及网络结构、网络边界以及网络设备自身安全等。须测评以下七个控制点：

控制点一：结构安全；

控制点二：访问控制；

控制点三：安全审计；

控制点四：边界完整性检查；

控制点五：入侵防范；

控制点六：恶意代码防范；

控制点七：网络设备防护；

**3）主机（数据库）安全**

主机系统安全须测评以下九个控制点：

控制点一：身份鉴别；

控制点二：安全标记；

控制点三：访问控制；

控制点四：可信路径；

控制点五：安全审计；

控制点六：入侵防范；

控制点七：恶意代码防范；

控制点八：资源控制；

**4）应用安全**

应用安全须测评以下十一个控制点：

身份鉴别；

安全标记；

访问控制；

可信路径；

安全审计；

剩余信息保护；

通信完整性；

通信保密性；

抗抵赖；

软件容错；

资源控制；

**5）数据安全及备份恢复**

保证数据安全和备份恢复测评以下三个控制点：

数据完整性；

数据保密性；

备份和恢复；

1. **安全管理测评**

主要包括：安全管理制度测评、安全管理机构测评、人员安全管理测评、系统建设管理测评、系统运维管理测评等五个层面上的测评；

安全管理制度

安全管理制度测评以下三个控制点：

管理制度；

制定和发布；

评审和修订；

安全管理机构

安全管理机构测评以下五个控制点：

岗位设置；

人员配备；

授权和审批；

沟通和合作；

审核和检查；

人员安全管理

对人员安全的管理，主要涉及两方面：对内部人员的安全管理和对外部员的安全管理。测评以下五个控制点：

人员录用；

人员离岗；

人员考核；

安全意识教育和培训；

外部人员访问管理；

系统建设管理

系统建设管理测评以下十一个控制点：

系统定级；

安全方案设计；

产品采购；

自行软件开发；

外包软件开发；

工程实施；

测试验收；

系统交付；

系统备案；

等级测评；

安全服务商选择；

系统运维管理

系统运维管理测评以下十三个控制点：

环境管理；

资产管理；

介质管理；

设备管理；

监控管理和安全管理中心；

网络安全管理；

系统安全管理；

恶意代码防范管理；

密码管理；

1. **系统整体测评**

主要包括：

1. 安全控制间安全测评；
2. 层面间安全测评；
3. 区域间安全测评；
4. 系统结构安全测评；

实施人员应根据特定信息系统的具体情况，结合相关国家标准和要求，确定系统整体检查的具体内容，在安全控制符合性检查的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，检查安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。检查完毕，必须向用户方提交测评报告及整改方案。

1. **测评流程要求**
2. **安全技术差距测评**

针对单位信息系统的物理安全、网络安全、主机安全、应用安全、数据安全和备份恢复5个技术层面进行现场测评和差距分析，记录相关的测评结果。

1. **安全管理差距测评**

针对单位信息系统的安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理这5个管理层面进行现场测评和差距分析，记录相关的测评结果。

1. **差距测评记录撰写、评审、定稿**

依照《等级保护现场测评记录》中所记录的针对单位信息系统的技术和管理测评结果，结合系统整体差距测评结果，按照标准测评报告模板撰写测评记录，完成初稿后交由单位进行评审，并最终定稿作为整改加固工作的依据。

1. **等级保护测评**

针对医院定级系统在《等级保护差距测评记录》的基础上进行全面的网络安全等级保护测评。

1. **形成等级测评结论及测评报告备案提交**

针对医院定级系统测评在数据汇总分析的基础上，分析系统存在的问题，给出系统等级测评结论，编制《等级保护测评报告》提交公安机关网安部门备案。

1. **安全整改要求**

依照《等级保护差距测评记录》中的测评结论和整改建议，结合针对单位信息定级系统的实际情况，配合用户方设计系统整改方案。

**（二）安全管理制度体系建设技术要求**

建立医院统一的信息安全管理体系，落实各项管理制度。从安全管理制度、安全管理机构、人员安全管理、系统建设及运维管理等方面进行系统规划设计，建立统一的信息安全管理系统，落实各项管理制度，让用户的安全管理体系，有宏观的设计、有清晰的责任权限、有合理的制度要求。同时应用包括安全可视化、统一运维管理等创新的技术手段，简化安全运维管理，减轻安全运维负担，提升安全运维管理的效率，最终做到整体防御、分区隔离；积极防护、内外兼防；自身防御、主动免疫；纵深防御、技管并重。

1. **安全管理策略和制度**

根据医院信息安全管理工作的特点，制定信息安全工作的总体方针和安全策略，明确安全管理工作的总体目标、范围、原则和安全框架等。根据安全管理活动中的各类管理内容建立安全管理制度；并由管理人员或操作人员执行的日常管理操作建立操作规程，形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系，从而指导并有效地规范各级部门的信息安全管理工作。通过制定严格的制度规定与发布流程、方式、范围等，定期对安全管理制度进行评审和修订。安全的管理制度可以在很大程度上防止由于人为因素导致的安全性问题，同时，对一个信息网络系统来说，管理制度需要结合系统的特点以及系统所处环境的特殊性进行考虑。

1. **安全管理机构和人员**

建立符合医院部门机构设置和人员分工特点的信息安全管理组织体系，成立信息安全管理小组等信息安全管理机构，明确信息安全管理机构的组织形式和运作方式，建立高效的安全管理机构, 设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。并从人员配备、授权和审批、沟通和合作、审核和检查、人员录用、人员离岗及安全意识教育和培训各方面进行管理落地。

1. **安全建设管理**

以信息安全管理工作为出发点，充实完善信息系统工程建设管理制度中有关信息安全的内容。涉及信息系统等级保护的定级、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、服务供应商管理等方面。从工程实施的前中后的初始定级设计到验收测评的整个工程周期中融入信息安全管理的策略和内容。以及强化对信息系统软件的开发过程和软件交付的安全指导和检测。

1. **安全运维管理**

根据医院信息安全管理制度体系框架中有关信息系统安全运维的有关制度规定，利用物理环境、网络系统、信息安全防护等运行维护管理和监测审计的系统和功能，以及统一安全监控管理中心等，不断完善系统运维安全管理的措施和手段，强化运维安全管理的科学规范，具体包括：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、网络与系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理及外包运维管理等内容，确保系统安全稳定的运行。

重点要进一步建立完善网络系统安全漏洞的日常扫描、检测评估和加固，系统安全配置变更，恶意代码病的监测防护，网络系统运行的日志审计记录和分析，数据的备份和恢复，安全事件的监测通报和应急响应等机制，并注重对安全策略和机制有效性的评估和验证。

**（三）测评检查工具要求**

针对本次测评工作，服务供应商应根据测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据；汇总统计分析单项测评结果，给出测评对象的整体测评结果。分析被测系统整体安全状况及对单项测评结果的修订情况，分析被测系统存在的风险情况，提出安全建设整改建议，得出等级测评结论，输出测评报告。为保障采购单位信息系统，服务供应商开展测评工作时，应采用专用检查工具开展信息系统测评工作。

**安全稽核工具**需具备以下功能：

仪表盘：查看资产、策略统计信息

资产管理：管理资产信息，根据IP段搜索资产并添加到资产管理中

策略管理：管理系统基础策略信息、管理系统高级策略信息、管理基线库信息

扫描管理：管理基础扫描信息、管理高级

扫描信息

离线任务：离线状态下实现信息安全扫描报表管理：用于下载各种报表

系统设置：用户管理、角色管理、机构管理、区域管理、菜单管理

须提供安全稽核工具原厂《计算机软件著作权登记证书》（加盖原厂公章）。

1. **采购标的的数量、采购项目交付或实施的时间和地点**

采购标的：根据相关要求，结合玉溪市人民医院在当地网安部门备案的系统逐年开展测评工作。

采购项目交付时间：合同签订后60天内。

采购项目实施地址：甲方指定地点。

1. **采购标的的验收标准**

验收时测评服务商提交成果要求：

供应商完成等级保护测评工作应按要求提供相应系统的测评报告、整改建议书及测评实施计划书等，包括但不限于：

1. 《信息系统等级保护测评方案》（纸版和电子版）
2. 《等级保护测评过程记录文件》（纸版和电子版）
3. 《信息系统等级保护测评报告》（纸版和电子版）
4. 《安全整改建议书》（纸版和电子版）
5. 在公安备案系统里可查。
6. **采购标的的其他技术、服务等要求。**

其他要求：

* 1. 应按网络安全等级保护测评要求制定测评服务过程中产生的文档，做科学、规范、详尽、统一等方面的要求。
	2. 保密要求：成交供应商不得在任何场合向任何无关单位或个人透露被测评信息系统和被测评单位的内部信息，并与用户方签订保密协议。
	3. 成交供应商须在规定时间内配合玉溪市人民医院顺利通过测评；在服务期内有责任提供技术支持，协助单位对照《安全整改建议书》开展整改工作。