#  惠州市第二人民医院信息系统网络安全等级保护测评项目用户需求书

**一、项目背景**

本项目为我院信息系统网络安全等级保护测评服务项目，主要用于建立健全的医院网络安全等级保护管理体系。为落实《中华人民共和国网络安全法》、《国家信息化领导小组关于加强信息安全保障工作的意见》、《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》等法律法规和有关规定，按照省、市发来的《广东省卫生健康系统网络信息与数据安全管理办法（试行）》、《惠州市关于加快推进我市信息系统安全等级保护工作的通知》等文件工作要求：各单位要及时开展网络安全等级保护工作，新建信息系统需完成网络安全等级保护测评工作，三级信息系统每年完成一次等保测评工作，二级信息系统每两年完成一次等保测评工作。现结合我院网络安全等级保护工作部署，需开展信息系统网络安全等级保护测评工作，保障我院主要信息系统安全稳定运行。

**二、总体要求**

根据《中华人民共和国网络安全法》及《网络安全等级保护条例》，实施符合国家标准的网络安全等级保护体系建设，对医院信息系统的安全等级划分，重点确保医院核心信息系统的安全性，消除网络安全隐患，确保医院网站和信息系统网络安全稳定。实现如下总体安全目标：

（1）通过对信息系统所承载业务及业务流程的分析，分析信息系统内信息资产和信息系统所提供服务的重要性，判断信息系统中业务信息和所提供的服务机密性、完整性或可用性等安全属性遭到破坏后，对国家安全利益、经济建设、公共利益或单位利益所造成的影响程度。提出等级建议，协助我院进行系统定级。

（2）以等级保护标准要求为依据，对我院信息系统在安全物理环境、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、安全建设管理和安全运维管理方面的测评，发现安全保护现状，并为确立安全策略、制定安全规划、开展安全建设提供决策建议，完成网络安全等级保护测评工作。

**三、项目内容**

需测评系统一栏表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **测评系统名称** | **系统级别** | **测评时间要求** |
| 1 | HIS系统 | 三级 | 2025年 |
| 2 | EMR系统 | 三级 | 2025年 |
| 3 | 集成平台与数据中心 | 三级 | 2025年 |
| 4 | 互联网医院系统 | 三级 | 2025年 |
| 5 | AI病历质控系统 | 二级 | 2025年 |

**四、商务要求**

1、投标人应具备《中华人民共和国政府采购法》第二十二条规定的条件，提供下列材料：

1）具有独立承担民事责任的能力：投标人需提供以下相关证照的扫描件之一：1.企业法人提供企业法人营业执照；2.事业法人提供事业法人登记证；3.其他组织提供其他组织的营业执照或执业许可证；4.自然人提供居民身份证等。分支机构投标的，还须提供分支机构的营业执照（执业许可证）扫描件及总公司（总所）出具给分支机构的授权书。

2）有依法缴纳税收和社会保障资金的良好记录，提供近半年内任意一个月的缴纳税收和社保证明。

3）具有良好的商业信誉和健全的财务会计制度，提供财务审计报告或者银行资信证明

4）履行合同所必需的设备和专业技术能力，依据《投标人资格声明函》及其附件。

5）参加采购活动前3年内，在经营活动中没有重大违法记录，依据《投标人资格声明函》及其附件。

6）本项目不接受联合体投标，依据《投标人资格声明函》及其附件。

**五、项目要求**

1、定级备案服务

根据《信息安全技术信息系统安全等级保护定级指南》等标准要求，协助配合按公安机关最新等保备案要求完善本单位信息系统定级测评和备案工作。

2、网络安全等级保护风险梳理服务

2.1针对本单位定级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、安全管理制度等进行现场测评和差距分析，记录相关的测评结果,输出现场测评记录结果。

2.2依照《等级保护现场测评记录》中所记录的针对本单位定级系统的技术和管理测评结果，结合系统整体差距测评结果，按照公安部标准测评报告模板撰写测评记录，完成提交《整改问题清单》或《风险梳理报告》。

3、信息安全等级保护测评服务

3.1在信息系统完成差距测评后，本单位整改实施完成，测评方对信息系统的安全技术和安全管理各个层面的安全控制进行整体性验证，针对本单位定级系统进行全面的信息安全等级保护测评。

3.2等级保护测评包括，安全技术及安全管理测评两个方面。根据现场访谈、配置核查的基础上通过先进的安全测试工具进行安全漏洞、应用系统代码漏洞的扫描及人工核查,在现场测评的结果和本单位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》提交公安部门备案，协助用户完成等级保护测评工作。

4.测评工具要求

4.1 本项目在实施过程测评方需提供能够满足《信息系统等级保护安全设计技术要求》（GB/T25070-2019）、《信息安全等级保护实施指南》（GB/T25058-2019）、《信息系统安全等级保护测评准则》（GB/T28448-2019）等规范中相关测评技术要求的专业安全服务工具，且服务工具由测评方免费提供，测评方应保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由测评方负完全责任。

4.2 测评工具软件运行所需要的硬件平台（如计算机、打印机等）均由测评方自行准备，本单位有权按照相关的要求对设备进行必要的处理。测评方在测评期间未经本单位许可，不得将设备带离本单位指定的场所，也不得使用任何未经本单位确认的存储设备对测评数据进行复制。未经本单位许可，测评方不得向任何第三方泄露医院网络信息相关数据及资料，违者付相应法律责任。

4.3 测评方须在文件中列出专业安全服务工具清单。相关工具指标要求：安全脆弱性扫描技术参数在等级保护测评过程中，采用询问、检查、测试、工具扫描等多种手段组合的方式。工具扫描应至少包括使用安全评估系统(即安全脆弱性扫描)工具对重要服务器、网络设备等进行漏洞扫描。

5、服务质量要求

5.1测评方应通过自身在等保测评工作中积累的经验，结合自身的技术优势，充分考虑到信息系统实际情况，提供一份具体细致的、操作性强的等级保护实施计划，并指导我单位完成对安全管理制度的补充完善和整理工作，协助完成信息系统等级保护的相关工作。

5.2测评方应依据《信息安全等级保护管理办法》、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评准则》、《信息系统安全等级保护实施指南》和《信息安全风险评估规范》等有关要求，按照严格程序对信息系统的安全防护能力进行科学公正的综合测评活动，完成对信息系统的等级保护落实情况与等级保护相关标准要求之间的符合程度的测试判定。

5.3 测评过程中，测评方需提供整改指导服务，就本项目成果中的具体内容提供解释，提供信息系统等级保护相关工作的技术支持和指导服务，以帮助我单位完成信息系统整改及提高安全防护能力。

5.4测评方应通过在安全技术和安全管理上选用与安全等级相适应的安全控制来实现信息系统安全等级。做到不同安全等级的信息系统应具有不同的安全保护能力，并使信息系统安全等级保护达到公安部门信息系统安全等级保护工作的各项要求，并且须协助我单位取得公安部门等级保护备案证。

5.5测评方须服从我单位业务信息系统的统一协调，且必须在项目实施期间由测评方派驻有丰富实施经验的测评师为项目实施团队，全程参与项目实施，现场检测工时必须符合国家相关标准。

5.6测评方须与我单位签订项目合同、保密协议和现场评测授权书，核实驻场测评师资质与投标时对本项目配备的测评师是否一致。确因工作调配需更换测评师，需提前10个工作日向本单位书面报备，并提供更换测评师资质证明。

▲6、服务资质要求

6.1服务机构资质要求：

1）网络安全服务认证证书等级保护测评服务认证；

2）具有省级电子政务服务能力水平等级证书；

3）信息安全服务资质证书（风险评估一级）；

4）具有质量管理体系认证证书、信息安全管理体系认证证书、环境管理体系认证证书、职业健康安全管理体系认证证书；

5）中国合格评定国家认可委员会颁发的CNAS检验机构认可证书；

6）具有省级检验检测机构资质认定政数证书（CMA证书）；

 7）具有计算机软件著作权登记证书的网络安全等级保护测评管理系统；

6.2 服务人员资质要求

1）项目经理资质：高级工程师、信息系统监理师、高级网络信息安全工程师、ITIL v3认证、ISMS审核员；

2）项目实施人员资质：高级信息安全等级测评师、信息安全专业人员证书（即 CISP 证书）、注册渗透测试工程师资质证书（CISP-PTE）、工业互联网安全评估工程师；

7、测评成果要求

测评方须完成本项目五个信息系统的等级保护测评工作，并协助完成信息系统的定级备案；须交付完整的《整改问题清单》或《风险梳理报告》、《网络安全等级保护测评报告》等测评备案过程中所要求的输出文件资料。

**六、项目依据遵循的政策法规及行业规范**

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

《中华人民共和国网络安全法》

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息安全技术 网络安全等级保护基本要求》（GB/T22239—2019）

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

《信息系统等级保护安全设计技术要求》（GB/T25070-2019）

《信息安全等级保护实施指南》（GB/T 25058-2019）

《信息系统安全等级保护测评准则》（GB/T 28448-2019）

《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）

《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）

《信息安全技术 操作系统安全技术要求》（GB/T20272-2019）

《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2019）

《信息安全技术 服务器技术要求》（GB/T21028-2007）

《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）

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

**七、项目工期要求及地点**

（1）完工时间：自合同签订之日起 20 日内完成测评工作，整改完成后 20 日内提交测评报告。

（2）完工地点：采购人指定地点。

**八、付款方式**

1、合同签订后支付合同金额50%款项；

2、完成网络安全等级保护测评工作，并经采购人审核确认后，支付合同金额的50%款。

**九、合同期限及售后服务**

1、合同期限：一年

2、中标人须在合同期内，提供相关系统整改指导服务。