**供应商须知**

**一、供应商须提供证明材料**

1、营业执照、基本开户证明、等级测评证书（复印件加盖公章）；

2、法定代表人授权委托书及授权代表身份证复印件；

3、报价表

**按以上要求提供证相关证件及资料各一份、不可缺项，按顺序装订。**

**二、供应商须满足以下要求**

1、付款方式：签订合同、出具检测报告后付合同款95%，剩余5%一年后一次性结清。

2、报价包括：检测费、报告编写费、专家评审费等。

3、工期：2个月

　服务期：一年

4、项目说明

为落实信息系统安全等级保护要求，进一步增强信息系统安全防护能力，确保信息系统安全稳定运行，依据《信息系统安全等级保护基本要求》（GB/T22239-2019）和《关于进一步加强全省卫生计生行业网络安全等级保护工作的通知》（鲁卫规划字[2017]10号）等文件要求，按照《医疗卫生机构网络安全管理办法》要求开展此次网络安全等级保护测评工作。

一、基本要求

1.保密要求。★项目实施过程中所收集、产生的所有与本项目相关文档、资料，包括文字、图片、表格、数字等各种形式所属权均归属采购人，成交供应商有义务对所涉及到的内容保密，并在签定合同时签署保密协议。

2.项目团队要求。项目团队人员不少于3人，项目经理为等级保护高级测评师。团队成员具有安全管控审计的能力，具有安全、网络、主机等专业方向上的能力；所有成员必须全程全职参与本次项目。项目成员不得随意变动，确需变动必须提前征得采购人同意.

二、项目需求和技术方案要求

1.总体要求

(1) 按照网络安全等级保护定级标准和工作要求，开展信息系统安全等级保护系统梳理和定级工作，协助完成系统的定级报告，并协助完成到公安机关的备案工作。

(2)按照国家等级保护2.0相关标准和要求，对上述系统按照对应级别标准开展信息系统安全等级保护测评工作，找出系统现状与相关标准要求之间的差距，遵循适度原则，提出切实可行的整改建议，最终完成等级保护测评报告。

(3)针对测评中发现的信息安全管理漏洞和薄弱环节，并深入分析下一步信息系统建设和管理的实际安全需求，协助开展相关的安全整改工作，确保重要信息系统的安全防护水平满足当前和未来建设发展的安全要求。

(4)对系统进行全面风险评估，识别系统脆弱性，出具系统安全风险评估报告。

2.测评依据

(1)《信息安全技术-信息系统安全等级保护基本要求》（GB/T 22239-2019）

(2)《信息安全技术-网络安全等级保护定级指南》（GA/T 1389-2017）

(3)《信息安全技术-网络安全等级保护实施指南》（GB/T 25058-2019）

(4)《信息安全技术-网络安全等级保护测评要求》（GB/T 28448-2019）

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

(6)《信息安全技术-办公信息系统安全管理要求》（GBT 37094-2018）

(7)《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

(8)《信息安全技术-信息系统通用安全技术要求》（GB/T 20271-2006）

(9)《信息安全技术-网络基础安全技术要求》（GB/T 20270-2006）

(10)《信息安全技术-操作系统安全技术要求》（GB/T 20272-2006）

(11)《信息安全技术-数据库管理系统安全技术要求》（GB/T 20273-2006）

(12)《信息安全技术-服务器技术要求》（GB/T 21028-2007）

(13)《信息安全技术-终端计算机系统安全等级技术要求》（GA/T 671-

(14)《信息安全技术-信息系统安全管理要求》（GB/T20269-2006）

(15)《信息安全技术-信息系统安全工程管理要求》（GB/T 20282-2006）

(16)《信息技术 安全技术 信息技术 安全性评估准则》（GB/T 18336-2001）

(17) 项目涉及的其它相关国际、国内标准或规范

3.服务内容

按照公安部网络安全等级保护工作要求，对上述系统按照对应级别标准开展信息系统安全等级保护定级备案工作。要求完成系统的定级报告，并协助到公安机关完成备案。系统情况包含但不限于下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | 建议等级 | 备注 |
| 1 | 以电子病历为核心的医院管理信息系统 | 三级 | 已备案 |
| 2 | 医院官方网站 | 二级 | 未备案 |

　　三、网络安全等级保护测评

1.测评要求

按照网络安全等级保护2.0标准和相关要求，对上述系统按照对应级别标准开展网络安全等级保护测评工作，找出系统现状与国家相关标准要求之间的差距，进行逐项分析、整体分析，提交差距分析报告和整改建议方案，并协助整改。待整改完毕后，进行结果确认，最终出具网络安全等级保护测评报告，并将测评报告报当地公安机关备案。

2.测评内容

等级保护测评的内容包括但不限于以下内容，所有技术要求参照上述“测评依据”。

(1)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、安全管理中心等五个方面的安全测评。

(2)安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

　　四、信息系统安全风险评估

1.评估要求

依据《信息安全技术 信息安全风险评估规范》等国家信息安全相关标准的技术要求，从风险管理角度，综合利用相关评估技术、评估方法、评估工具，分析与信息安全有关的资产，对资产进行识别，评价所面临的信息安全威胁、存在的薄弱点及其对信息安全的影响，确认已有的信息安全控制措施，判断安全事件发生的概率以及可能造成的损失，对物理环境安全、网络架构安全、主机设备安全、应用系统安全、数据安全、管理安全等多方面进行风险评估。根据分析结果提供有针对性的整改加固方案，并协助用户进行整改加固，将风险控制在可接受范围内，最终出具信息安全风险评估报告。

2.评估内容

(1)物理环境安全性评估

(2)网络架构安全性评估

(3)主机系统设备安全性评估

(4)应用系统安全性评估

(5)信息安全管理组织架构和理性评估

(6)信息安全管理制度及安全性评估

(7)人员安全管理状况评估

(8)安全产品和技术应用状况有效性及合理性评

(9)对应重大紧急安全事件的处理能力评估

　　五、网络安全加固服务

针对本次等保测评的2个系统，根据网络安全等保测、风险评估及软件测试发现的问题进行重点加固，遵循适度安全原则，综合考量成本与效益因素，提出信息系统安全等级保护整改建议，形成加固列表。按照等级保护基本要求进行保护整改，出具具备可操作性的整改方案。根据测评报告、专项检查结果形成整改方案系统地进行安全整改，整改工作是对信息系统完善的过程，通过建立整改方案和有效的整改工作，使系统能够进一步完善，达到等级保护的要求。安全加固服务包括以下内容：

1. 协助采购人完善、编制网络安全管理制度包括但不限于《网络安全管理制度》、《人员安全管理制度》、《机房安全管理制度》、《设备管理制度》、《防病毒管理制度》、《外部人员安全管理制度》、《资产管理制度》、《用户信息管理制度》等制度内容。

2. 网络架构咨询规划，针对最新的安全防护思路、安全威胁情况提供网络架构的咨询规划，并协助进行架构优化。

3. 提供网络设备策略加固，协助网络设备服务商对医院交换设备、路由器等网络设备进行加固，加固服务的内容包括：访问控制、安全审计、网络设备防护、身份认证、登录管理等安全项加固。

4. 提供安全设备策略加固，根据信息系统的安全情况逐步调整防火墙、IPS、WAF、堡垒机等安全设备的策略，以达到最佳的安全防护效果。安全设备加固服务的内容包括：访问控制、安全审计、网络设备防护、身份认证、登录管理等安全项加固。

5. 提供主机安全加固，协助主机维护商针对使用的操作系统如 windows、Linux、AIX 等进行加固。加固服务的内容包括：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、账号管理等安全项加固。

6. 提供数据库及加固，协助数据库服务商针对不同类型的数据库如Oracle、SQlServer、Mysql 等进行加固，加固服务的内容包括：身份鉴别、访问控制、安全审计、资源控制等安全项加固。

7. 协助进行系统安全漏洞修复，重点针对中高危系统漏洞进行修复指导，制定漏洞修复方案，协助漏洞修复。

8. 为提高全员网络安全普及网络安全知识，使工作人员能够充分了解和感知网络安全风险，熟悉系统网络安全工作要求，掌握基本网络安全技能，最终达到增强工作人员网络安全意识。进行安全教育培训应包括但不限于如下内容：

(1)提供 1 次全员网络安全意识或专题培训。

(2)针对本次安全加固提供 1 次加固网络安全培训，培训内容包括加固方法、加固流程等内容。

9.安全加固方案不能影响各项业务的正常进行，如果加固过程需要暂时中断业务，必须设计具体的解决方案。依据标准《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 信息系统安全管理要求》（GBT20269-2006）和《信息系统安全等级保护基本要求》等，完成安全管理体系的设计，制定等级保护整改方案，指导信息系统安全技术体系和安全管理体系的构建。

10.安全加固工作完成后，对设备和系统运行进行验证并监控，确保安全加固不影响其正常运行。同时，对加固后的设备和系统进行漏洞检测，对加固进行有效证验证，确保安全加固效果到位。

　　六、其他服务要求

1.新上线系统安全评估服务

服务期内提供不低于2次系统安全评估服务，包含但不仅限于：漏洞扫描、渗透测试、基线核查、风险评估、安全功能测试、安全设计建议、移动 APP 安全审核、性能压力测试、评测报告（加盖成交人评测机构公章）。

2.应急响应服务

服务期内指派一名安全事件应急服务人员参与我院应急响应，应急服务人员提供

7\*24 小时电话技术咨询，遇安全突发事件2小时内提供到场技术支持。应急响应服务除了包含发生安全事件后的应急响应活动外，还包括事前协助用户制定或完善应急预案，开展应急演练等活动。修订和完善应急预案将包括现状调研、综合预案完善、专题预案完善、特定系统预案完善等工作内容。根据应急预案规定的流程，协助用户进行相应的模拟演练，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订。使得用户信息系统相关人员了解应急流程和自己的责任，在安全事件发生时，能够有条不紊地开展应急工作，最大程度降低安全事件带来的负面影响和损失，提高用户信息系统业务连续性。

1. 安全培训服务

中标方应提供包含等保 2.0软件测试政策法规、信息安全政策法规、软件测试技术标准、信息安全技术标准、测试项目管理、性能测试技术、代码测试技术、商密测试技术在内的专业安全培训。

　　七、成果交付

1.测评系统提交的文档包括以下文件：

(1)《XXX 系统网络安全等级保护备案证明》

(2)《XXX 系统网络安全等级保护测评方案》

(3)《XXX 系统网络安全等级保护差距分析报告》

(4)《XXX 系统网络安全等级保护整改建议方案》

(5)《XXX 系统网络安全等级保护测评报告》

(6)《XXX 系统信息安全整改加固方案》

(7)《信息系统信息安全风险评估报告》

2.交付形式：电子版和纸介质形式，电子版形式的材料以常规软件可打开的格式提供，加盖测评机构公章的书面材料不少于2份，等级保护测评报告需加盖DJCP 等级测评章。

　　八、售后服务

1、成交人应为招标人提供及时、迅速、优质的服务；

2、在质保期内如出现问题时，成交人应迅速派技术人员及时解决，同时成交人承担备品备件及人员的所有费用，由于成交人原因时间拖延而造成招标人生产损失由成交人赔偿；

3、成交人若能提供其他更优质的服务，可在服务承诺中自行提供。该承诺将做为确定成交的参考依据；

4、对以上技术服务应有明确的时间承诺。

**报价表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测评项目 | | 建议等级 |
| 1 | 以电子病历为核心的医院管理信息系统 | | 三级 |
| 2 | 医院官方网站 | | 二级 |
| 总报价 | | 万元 | |