**潍坊市人民医院等级保护测评和网络安全运维服务项目征集公告**

潍坊市人民医院根据《中华人民共和国政府采购法》等有关规定，对等级保护测评和网络安全运维服务项目进行市场价格等调查征集，欢迎广大符合条件的供应商积极参与。

一、联系人：潍坊市人民医院物资采购办公室

二、联系电话：0536-8192593

三、内容：

|  |  |  |
| --- | --- | --- |
| 序号 | 设备名称 | 数量 |
| 一 | 等级保护测评 | 1 |
| 二 | 网络安全运维服务 | 1 |

四、供应商资质要求：1.中国境内注册，具有独立法人资格；2.投标人必须提供营业执照、组织结构代码证、税务登记证复印件加盖公章（三证合一的投标人只需要提供营业执照复印件加盖公章）；3.具有公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》，需提供复印件加盖公章。

五、参考要求详见附件。

六、征集方式：供应商将填写无误的附件报名表格（同时提交可编辑电子版一份），连同有效期内营业执照副本、法定代表人资格证明或法定代表人的授权委托书扫描后以邮件附件形式发送到潍坊市人民医院物资采购办公室邮箱wfrmgyszj@163.com,邮件主题为：项目名称+公司名称。

七、征集时间：2022年10月26日上午9点至11月1日下午3点（休息日除外）。

八、符合要求的供应商，邀请函免费发至预留的邮箱，如未收到，请务必自行电话联系物资采购办公室核实。

**备注：本次征集仅作为该项目市场价格****等需求调查，不属于采购公开招标，望各供应商知悉。如有疑问，请拨打联系电话咨询。**

潍坊市人民医院物资采购办公室

2022年10月25日

**附件：参考参数**

**第一部分 等级保护测评**

参考要求

1、项目概述

为了保障信息系统安全稳定运行，在全面了解相关国家政策和自身信息系统的基础上对信息系统实施网络安全等级保护测评工作。

根据公安部《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安［2010］303号）《中华人民共和国网络安全法》的相关要求，主管部门的整改建议，对潍坊市人民医院相关信息系统开展信息系统等级保护测评工作，在技术和管理两个方面的的内容进行逐一的检查和测试，夯实单位信息系统安全基础，提高信息安全管理水平，消除安全隐患，确保信息网络的安全运行。测评对象及对应网络安全等级保护级别如下表所示：

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 网络安全等级保护级别 |
| 1 | 以电子病历为核心的医院信息系统 | 三级 |
| 2 | 网络系统 | 三级 |
| 3 | 面向患者服务系统 | 三级 |
| 4 | 医院集成平台数据中心 | 三级 |

### 2、项目目标

（1）按照国家等级保护相关标准和要求，开展网络安全等级保护测评工作，提交对应等级的测评报告。

（2）需根据招标方要求，对内部人员开展数据安全治理培训。

### 3、项目实施参照标准及依据

主要依据标准

* 《中华人民共和国网络安全法》
* 公安部、国家保密局、国际密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）；
* 公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》（公通字 [2007]43号）；
* 《关于加快推进国家电子政务外网安全等级保护工作的通知》（政务外网［2011］15 号）；
* 《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 网络安全等级保护实施指南》；
* 《信息安全技术 网络安全等级保护测评要求》；
* 《信息安全技术 网络安全等级保护测评过程指南》；
* 《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27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 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/T 20270-2006）；
* 《信息安全技术 操作系统安全技术要求》（GB/T 20272-2006）；
* 《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）；
* 《信息安全技术 服务器技术要求》（GB/T 21028-2007）；
* 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T 671-2006）；
* 《信息安全技术 信息系统安全管理要求》（GB/T20269-2006）；
* 《信息安全技术 信息系统安全工程管理要求》（GB/T20282-2006）；

### 4、内容说明

4.1网络安全等级保护测评服务

系统安全等级测评的内容包括但不限于以下内容：

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、安全计算环境和安全管理中心等五个方面的安全测评；

安全管理测评：安全管理制度、安全管理机构、安全人员管理、安全建设管理和安全运维管理等五个方面的安全测评。

（1）安全物理环境

根据信息系统机房和现场安全测评记录，针对机房和现场在“物理位置选择”、“物理访问控制”、“防盗窃和防破坏”、“防雷击”、“防火”、“防水和防潮”、“防静电”、“温湿度控制”、“电力供应”和“电磁防护”等安全物理环境方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

（2）安全通信网络

根据信息系统安全通信网络测评记录，针对网络方面在“网络架构”、“通信传输”、“可信认证”等安全通信网络方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

（3）安全区域边界

根据信息系统安全区域边界测评记录，针对网络方面在“边界防护”、“访问控制”、“入侵防范”、“恶意代码和垃圾邮件防范”、“安全审计”、“可信验证”、“资源控制”。等安全区域边界方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

（4）安全计算环境

根据信息系统安全计算环境测评记录，针对网络方面在“身份鉴别”、“访问控制”、“安全审计”、“入侵防范”、“恶意代码防范”、“可信验证”、“数据完整性”、“数据保密性”、“数据备份恢复”、“剩余信息保护”、“剩余信息保护”等安全计算环境方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

（5）安全管理中心

信息系统安全管理中心现场测评包括“系统管理”、“审计管理”、“安全管理”、“集中管控”等安全计算环境方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

（6）安全管理制度

根据现场安全测评记录，针对信息系统在安全管理制度方面的“安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

（7）安全管理机构

根据现场安全测评记录，针对信息系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

（8）人员安全管理

根据现场安全测评记录，针对信息系统在人员安全管理方面的“人员录用”、“人员离岗”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

（9）安全建设管理

根据现场安全测评记录，针对信息系统在系统建设管理方面的“定级和备案”、“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”、“等级测评”以及“安全服务商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

（10）系统运维管理

根据现场安全测评记录，针对信息系统在系统运维管理方面的“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”、“网络和系统安全管理”、“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”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。

4.2网络安全培训

需依据国家相关标准和要求，对甲方运营维护人员开展数据安全治理方面的培训，培训内容及培训大纲需依据注册信息安全治理人员（CISP-DSG）的要求开展，包括且不限于：

（1）网络安全技术

此内容包括：信息安全保障、信息安全评估、网络安全监管、信息安全支撑技术等

（2）数据安全基础知识

此内容包括：数据安全基础知识、机构化数据应用、非结构化数据应用、大数据应用、数据安全基础等

（3）数据安全技术

此内容包括：数据防泄漏技术、数据库安全技术、数据可用性保障、大数据安全防护

（4）数据安全治理及保障体系

此内容包括：治理与保障框架、数据安全管理、数据安全评估、数据安全策略、数据安全运营、合规评测

5、成果交付

该项目提交的文档至少包括以下几类文件：

1. 《信息系统网络安全等级保护测评方案》
2. 《信息系统网络安全等级保护测评报告》
3. 《测评报告电子版文档》

6、其他相关服务

（1）漏洞扫描服务

利用专业的漏洞扫描工具，对系统与应用每半年进行一次脆弱性扫描，通过漏洞扫描找到各个层面上的脆弱性漏洞，分析各脆弱性的利用可能性和危害程度，并提供漏洞统计、漏洞分类、漏洞详情等信息，为信息安全加固、整改提供支持信息。

（2）安全意识培训

提供不少于1天的安全培训，培训体系针对不同受训角色提供相应的培训内容，涵盖从领导层、技术管理层到一般技术人员等各层次人员所需了解或掌握的网络安全知识和技术。制定详细的培训计划和方案，包括：信息系统安全等级保护培训、安全意识培训等。

（3）渗透测试服务

对系统每半年进行一次渗透测试服务一次，将遵循保密性原则、标准性原则、规范性原则、可控性原则、整体性原则、最小影响原则。

（4）应急支援

在服务期内提供信息安全应急支援服务及重大节假日应急响应，包括远程应急支援和现场应急支援。现场应急响应时间不超过6小时，正常情况6小时到达用户现场。

（5）安全咨询服务

基于用户的信息安全需求，依据国家政策和国家信息安全标准，提供信息安全技术和信息安全管理方面的信息安全咨询。

# 第二部分 网络安全运维服务

|  |  |  |
| --- | --- | --- |
| 序号 | 服务名称 | 参考需求 |
| 1 | 安全运维服务 | 1、每周定期提供安全巡检，对安全设备的可用性进行检查。  2、结合现有安全手段和服务单位的安全检测手段对用户安全状态进行监控，实现对内外网安全风险的监控，及时发现网络中的安全风险；包括但不限于高级可持续威胁攻击监测、失陷主机监测、攻击监测、僵木蠕监测、DDoS监测、恶意程序监测、WEB安全监测、元数据提取、流量分析等。  3、对安全告警进行研判分析；每周出具相关分析报告；  4、根据告警情况提供安全优化建议，对安全策略进行优化调整。 |
| 2 | 应急演练服务 | 1、服务期内每年进行应急演练，服务单位需根据用户实际情况，创建演练场景，每次不少于3个不同类型场景，包含不限于暴力破解场景，终端病毒场景、数据泄露场景、数据损坏场景、软件后门事件、高危漏洞场景等演练内容。  2、服务单位提供响应技术支持；配合客户做技术支持模拟发生网络与信息安全事件，并依照应急预案的规定开展事件处置工作。 |
| 3 | 应急响应保障服务 | 1、提供安全事件应急响应服务，针对突发的危害程序事件，网络攻击事件，信息破坏事件，设备实施故障和灾害性事件等安全事件开展应急响应处置工作，对安全事件进行快速抑制及消除，减少安全事件造成的损失。  2、服务单位要求提供专业的安全应急支撑队伍，对安全事件进行分析和取证，对安全事件进行分析、处置和响应的过程进行复盘；对安全隐患进行排查。  3、要求服务单位以现场、远程等多种服务方式提供7×24小时的应急响应服务。  4、应急涉及安全设备的由服务单位免费借用方式提供。 |
| 4 | 新上线业务系统检测 | 1、为满足合规要求，认真履行落实《网络安全法》、《关键信息基础设施安全保护条例》等法律法规针对应用系统运营单位的责任与义务，需对入网系统开展上线运行前的安全检查，全面发现信息系统存在的安全隐患，加强应用系统上线后的安全稳定运行，降低发生网络安全事件与违反政策法规的风险。  2、入网系统上线前，服务单位需对系统进行上线安全检查工作；包括漏洞扫描、配置核查、渗透测试、安全措施策略等；提前发现信息系统潜在的恶意代码、安全漏洞、配置错误等安全风险，并提供安全风险处置建议修补风险项。  3、每年提供2次新系统上线检测服务，并提供响应检测报告。 |
| 5 | 渗透测试服务 | 服务期间对两个指定业务系统进行渗透测试，挖掘安全漏洞；并提出整改意见。 |
| 6 | 安全培训服务 | 1、安全意识培训  服务期内提供1次网络安全意识培训；提供网络安全意识视频、易拉宝等意识宣传物资。  每年网络安全宣传周期期间，开展网络安全意识宣贯服务，供应商需组织安全意识宣贯，提供网络安全意识视频、易拉宝等宣传物资。组织专家开展意识培训主要介绍网络安全形势，普及网络安全意识，使本单位工作人员能够充分了解和感知网络安全风险，增强工作人员网络安全防范意识。  2、安全知识培训  服务期内可根据用户需要，提供安全知识培训，包括数据安全知识培训，网络安全知识培训、安全产品培训以及操作培训等。 |
| 7 | 重要时期安全保障服务 | 1、在重要时期对单位的重要系统和门户网站提供安全保障服务，解决因人员经验不足、安全技术能力不够和人员配置不全等方面的问题。  2、在事前、事中、事后对重要信息系统和门户网站进行全程的安全保障，从而使信息系统在重要时期能安全稳定地运行。包括保障前的风险排除和加固，保障中的安全监测、预警、分析处置，保障后的分析总结，重要保障期间提供连续服务。 |
| 8 | 安全建设规划服务 | 依据客户网络安全现状和需求，结合相应法律、法规要求，提供安全风险评估，出具合理化安全建设规划方案及建议。 |

一、服务单位能力参考要求

1、具备专业网络安全服务能力，具备国家级认证的应急支持单位认证，参与过部级攻防演练活动，具备高水平漏洞挖掘能力是国家信息安全漏洞共享平台（CNVD）技术成员单位和国家信息安全漏洞库（ CNNVD ）技术支撑单位，具备中国信息安全测评中心风险评估认证和安全运营认证。

2、为在项目中实现漏洞闭环机制，服务提供商应具备CNVD平台2021年度（原创漏洞发现、漏洞信息报送、漏洞处置）突出贡献单位证书。

3、服务商需在潍坊本地具备专业服务团队，技术人员不少于5人以应对人员变动和重保需求，人员需提供社保查询证明。

4、为应对突发安全应急事件，服务提供商本地需具备应急设备支撑库，服务提供商需提供公司官网查询证明。

二、其它参考要求

1、安全运维人员需具备丰富的项目实施维护经验，渗透攻防能力突出，具备漏洞挖掘能力，参加过省市级攻防比赛，具备行业内相关资格认证。安全运维人员需经过我院面试，面试合格后入场，服务期间发现人员能力不足不能胜任我院工作的，我院有权提出更换，服务单位要在接到更换通知后10个工作日内进行更换。

2、除我院现有设备外，服务单位在服务期间开展的安全检测、风险评估、暴露面检测、安全监测、安全应急等服务时涉及的安全设备由服务单位自行提供。

3、服务周期以一年为单位进行考核；考核合格后进入下一周期服务；考核不合格我院有权解除合同。

4、服务商必须严格遵守采购人网络安全方面的要求。对于参与项目实施的咨询人员、技术人员均需要签订公司统一的信息保密协议。供应商需对以下信息进行保密，具体包括：

（1）项目信息：如业务流程、技术方案、业务数据（静态数据、动态数据、历史数据）、报表指标、工程设计、技术指标、计算机软件、数据库、操作手册、技术资料、用户防系统漏洞、用户方信息系统架构等。

（2）服务商项目参与人员在履行职责期间，必须遵守采购人规定的任何成文或不成文的保密规章、制度，履行与其工作岗位相应的保密职责。不向不承担相应保密义务的任何第三人披露采购人的商业秘密。采购人的保密规章、制度没有规定或者规定不明确之处，项目组成员亦应本着谨慎、诚实的态度，采取任何必要、合理的措施，维护其于履行职责期间知悉或者持有的任何属于采购人或者虽属于第三方但采购人承诺有保密义务的技术秘密或其他商业秘密信息，以保持其机密性。

（3）除了履行职务的需要之外，项目组成员承诺，未经采购人书面同意，不得以泄露、告知、公布、发布、出版、传授、转让或者以其他任何方式使任何第三方（包括按照保密制度的规定不得知悉该项秘密的采购人其他职员）知悉属于采购人或者虽属于他人但采购人承诺有保密义务的技术秘密或其他商业秘密信息，也不得在履行职务之外使用这些秘密信息。