**一、项目名称**

上海交通大学医学院附属新华医院2025年度信息安全技术服务项目

**二、项目参数**

**（一）项目概况**

随着我院网络环境和信息系统的不断扩展、应用服务的不断深入，为了保障我院网络环境和信息系统的安全稳定运行，及时发现并解决各类突发问题成为工作的重中之重。为了进一步优化我院网络环境和信息系统运行维护、网站监控模式、网络安全管理，提高我院网络环境和信息系统运行维护中主动发现问题和应急处置的能力。本项目是为保障我院网络环境和信息系统能够继续在良好稳定的状态下运行，委托具有专业技术的公司对我院网络环境和信息系统进行总体顶层设计及日常运维。

**（二）最高限价**

人民币150.00万

**（三）资格条件**

（1）投标人须具有独立承担民事责任的能力；

（2）投标人须具有良好的商业信誉和健全的财务会计制度；

（3）投标人须具有履行合同所必需的设备和专业技术能力；

（4）投标人须有依法缴纳税收和社会保障资金的良好记录；

（5）投标人参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）投标人在近三年内未被国家财政部指定的“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信名单；

（7）单位负责人为同一人或者存在直接控股、管理关系的不同单位，不得参加同一包件的竞争或者未划分包件的同一采购项目的竞争；

（8）本项目接受联合体投标。

（9）法律、行政法规规定的其他条件。

**（四）功能及技术参数**

**一、项目概况**

随着我院网络环境和信息系统的不断扩展、应用服务的不断深入，为了保障我院网络环境和信息系统的安全稳定运行，及时发现并解决各类突发问题成为工作的重中之重。为了进一步优化我院网络环境和信息系统运行维护、网站监控模式、网络安全管理，提高我院网络环境和信息系统运行维护中主动发现问题和应急处置的能力。本项目是为保障我院网络环境和信息系统能够继续在良好稳定的状态下运行，委托具有专业技术的公司对我院网络环境和信息系统进行总体顶层设计及日常运维。

**二、服务内容**

（一）安全自查

1、安全评估

2、渗透测试

（二）等保咨询服务

（三）SSL证书

（四）网络安全值守

（五）专家服务

1、网络安全公告

2、安全策略

3、安全制度编写

（六）互联网应用安全监控

1、网站安全监测

2、联网终端网络安全监测

3、网络安全预警通报

（七）设备License续费

1. **服务详细技术要求**

**（一）安全自查**

**1.安全评估**

（1）服务内容：IT设备漏洞扫描检测、上线安全评估、勒索病毒安全检查、弱口令安全检查、风险评估

（2）项目目的：清楚、全面的了解自身IT系统的安全风险，明确之后安全改进的方向，并为高层决策提供依据和参考方向。

（3）项目描述：通过工具和人工的方式，及时检测资产的安全漏洞和威胁分析，识别高风险的漏洞；系统上线安全评估；勒索病毒安全检查；弱口令安全检查；风险评估等服务；并提出加固整改建议，帮助弥补安全漏洞。

（4）出具安全自查报告

（5）内容明细：

|  |  |  |
| --- | --- | --- |
| 序号 | 服务项 | 功能描述 |
| 1 | IT设备漏洞扫描检测 | 通过网络扫描工具，对客户IT设备进行漏洞扫描，识别安全风险为安全加固提供依据。 |
| 2 | 上线安全评估 | 参考客户上线检查规范或业界最佳实践进行上线安全评估。 |
| 3 | 勒索病毒安全检查 | 通过漏洞扫描、系统安全防护措施检查、安全日志分析以及安全加固。 |
| 4 | 弱口令安全检查 | 含主机、中间件和数据库的安全检查。 |
| 5 | 风险评估 | 参考ISO27001风险评估规范，给客户提供包括资产识别、威胁识别、漏洞扫描和风险评估等相关服务。 |

**2.渗透测试**

（1）服务内容：渗透测试

（2）项目目的：可直接验证安全防御策略实施状态的有效性；提供当前抗入侵能力证据；为安全运维人员、合作第三方和院方提供信息安全加固方向。

（3）项目描述：主要通过工具扫描及人工评估的方式为客户提供通过模拟攻击的方式，分别从内网和外网对客户的网络信息系统进行抗入侵攻击能力测试，深入发现和检测安全防护措施的有效性，并评估一旦网站系统遭受攻击后可能受到的破坏影响程度。

（4）出具渗透测试报告

（5）内容明细：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务项** | **功能描述** | **客户提供资源** | **备注** |
| 1 | 渗透测试 | 参考OWASP，提供具有CISP资质认证的渗透工程师，模拟黑客攻击行为，对客户的目标系统、设备进行渗透测试，包括身份认证、访问控制、输入输出验证等方面，出具渗透测试报告并提供安全加固建议。 | 提供授权 | 含应用系统、操作系统、数据库、网络设备等的渗透 |

（6）工作范围：

|  |  |
| --- | --- |
| **功能名称** | **功能描述** |
| 主机操作系统渗透 | 对Windows、Solaris、AIX、Linux、SCO、SGI等操作系统本身进行渗透测试。 |
| 数据库系统渗透 | 对MS-SQL、Oracle、MySQL、Informix、Sybase、DB2、Access等[数据库应用系统](http://baike.baidu.com/view/1353688.htm)进行渗透测试。 |
| 应用系统渗透 | 对ASP、CGI、JSP、PHP等组成的B/S、C/S应用进行渗透测试。 |
| 网络设备渗透 | 对各种防火墙、[入侵检测系统](http://baike.baidu.com/view/20936.htm)、[网络设备](http://baike.baidu.com/view/1158081.htm)进行渗透测试。 |

**（二）等保咨询服务**

1.参照《信息安全技术网络安全等级保护基础要求》，依据新华医院当年等保测评情况，提供咨询服务。结合漏洞扫描、渗透测试等技术手段，对信息资产所面临的威胁、存在的漏洞、造成的影响，以及信息系统潜在安全风险的可能性进行全面的评估，并提出针对性解决方案。通过网络架构分析和对系统相关服务器、交换机与安全设备的配置策略检查，查找需要对网络结构实施优化的事项，以等级保护预测评结果为依据，协助等级保护测评机构编写《等级保护差距性分析报告》。根据《等级保护差距性分析报告》并参照《信息安全技术网络安全等级保护基础要求》提出相关等级保护整改建议，落实等级保护整改工作，协助等级保护测评机构编写《等级保护测评报告》。

**（三）SSL证书**

1.用于实现内外网网页访问以HTTPS方式提供服务，签发一年。合同签订后，根据招标人需求进行申请。

**（四）网络安全值守**

**1.日常安全职守**

（1）服务内容：安全值守

（2）内容明细：

1)重要区域安全监测防护

2)核心应用安全检查

3)积极开展应急演练，验证安全防护手段是否到达防护效果。

4)现场值守、应急响应。

5)威胁情报通告，能及时掌握保障期间威胁情报，及时告知。

6)网站安全监控，做好网站可用性,防挂马,防篡改，内容监控等。

**2.重大活动保障**

（1）在重要安全检查、重大活动开展期间，专业服务团队提供技术服务，通过执行现场值守、定期安全检查，应急响应等服务，协助用户开展等级保护、符合性评测以及其他迎检工作，保障满足通过上级单位重大安全检查要求。

（2）重大活动现场值守：在重大活动期间，现场增派经验丰富的专家进行现场安全保障，包括现场安全设备监控，突发安全事件应急响应，安全技术支持等工作。

（3）自重大活动前到重大活动结束，提供增强的安全运维服务，进行7\*24小时现场安全值守保障。

（4）专业服务团队按日和周提供《系统安全运行报告》，前一日和周的系统遭受攻击情况、应急处理情况等进行总结报告。

（5）专业服务团队在活动结束后提供《重大活动保障服务报告》，对重大活动之前的安全检查、期间的安全保障情况等进行总结。

（6）重大活动安全检查：在重大活动前进行系统安全评估及加固指导，提高日常安全作业频率，确保重大活动顺利召开。

**（五）专家服务**

**1.专家特色服务**

（1）服务名称：安全公告、安全技能培训、安全制度编写

（2）服务目的：安全公告提供第一时间的安全预警，能提前部署信息安全防护手段，防患于未然。安全技能培训满足获取安全知识和各种安全技能的需求，最终达到强化安全意识、理解安全理论、掌握安全技术和获得安全实践经验等效果。安全制度编写，帮助建立满足运行要求的安全规范和流程。

（3）专家资质：专家团队中持有工信部、中央网信办等部门颁发的网络信息安全高级职称证书、领队专家拥有相关领域硕士以上学历、团队专家需要提供相关领域3-5年从业经历。专家团队具备与本项目相关的证书，如： CISP等资格证书。

（4）服务描述：安全公告即定期提供结合客户信息系统实际情况，收集并整理相应IT基础设施厂商、安全产品厂商、信息安全组织机构发布的最新安全漏洞信息以及国内外重要信息安全相关新闻及相关补救措施的信息；安全技能培训即通过专业培训，帮助IT人员提高安全技能及处理突发事件的能力。安全制度编写，帮助建立满足运行要求的安全规范和流程。

（5）服务内容描述

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务项 | 功能描述 | 范 围 | 前提 |
| 1 | 安全公告 | 提供一段时期内，各类操作系统，网络安全系统，应用平台，病毒等的安全漏洞及相关补救措施信息。 | * 操作系统
* 网络设备
* 应用服务器
* 病毒信息
 | 无 |
| 2 | 安全技能培训 | 通过专业培训，帮助IT人员提高安全技能及处理突发事件的能力 | * 黑客攻防培训
* 员工安全意识培训
* IT管理员培训
* 可额外定制
 | 无 |
| 3 | 安全制度编写 | 由专业安全顾问帮助客户编写、完善安全管理制度、流程和进行宣贯推广 | * 安全管理制度
* 安全管理流程
* 宣贯推广
 | 客户需提供组织职责分工说明和进行配合、审核 |

**（六）互联网应用安全监控**

**1.网站安全监测**

在公共互联网国际出入口及省级出口上，对新华医院拥有的网站开展网页篡改、网页挂马、网站后门等安全事件的外围性监测和预警通报，协助新华医院及时发现网站的安全事件和存在隐患，并对新华医院处置这类安全事件提供一定的远程技术支持服务。

**2.联网终端网络安全监测**

在网络层面对新华医院接入互联网的计算机所感染木马、蠕虫、僵尸程序等恶意程序事件进行外围性监测和预警通报，协助新华医院及时发现联网终端被恶意程序攻击的情况，并对新华医院处置这类安全事件提供一定的远程技术支持服务。

**3.网络安全预警通报**

定期为新华医院提供公共互联网网络安全态势通报、上海市网络安全月报、重要安全漏洞公告。

**（七）设备License续费**

1.为新华医院以下设备提供License续费服务，续费1年。设备清单由新华医院提供。

**（五）商务要求**

**一、服务时间**

2025年8月20日起一年

**二、服务地点**

上海交通大学医学院附属新华医院

**三、付款方式**

（1）维护服务年度开始至完整服务6个月后，按照医院的付款流程，甲方向乙方支付当年维护服务费的50%。

（2）本项目一年维保期结束后，且运维满意度达到80分以上，甲方在收到乙方开具的有效发票后，根据医院付款流程，向乙方支付本合同项目总金额50%的合同款。当满意度低于80分，甲方有权视情况扣除相应的服务费用(按照服务周期和合同价格扣除未支付比例)，并具有进一步要求赔偿的权利(按照合同约定)。

（3）如项目维护期存续期间，若因特殊原因造成项目维护期提前结束，则本项目涉及的维护期维护费用按照实际发生时长进行结算。

**四、售后服务要求**

★1.提供一年工作日5x8小时的安全值守服务，同时提供电话5分钟之内响应（7\*24小时）。**（以承诺函为准）**

★2.至少3名资深安全工程师（需要投标单位近6个月内由投标人为其缴纳的社保证明）在现场进行值守，以保证安全工作的及时响应和处理。**（提供相关证明资料）**