**重钢总医院**

**安全运维服务项目市场征询函**

重钢总医院本着“公平、公开、公正”的原则，特向服务商单位发出重钢总医院安全运维服务项目的征询函，望积极参与响应。

1. 项目信息
2. 项目名称：安全运维服务项目
3. 项目类型：服务采购
4. 项目目标

重钢总医院安全运维服务项目建设目标是以等级保护标准为基础，参考ISO27001标准以及相关安全规范和标准，建立符合医院信息化系统实际安全需求的安全管理体系，提高安全管控水平。

1. 形成体系化的安全管理与技术机制

制定整体安全规划和建设路线图，有计划的建成一个可扩展的、相互协同和制约的完整信息安全体系，减少单效独建的补救方法，逐步形成完整安全体系。

1. 满足当前及未来信息安全合规性要求

以《网络安全法》为纲，以等级保护标准为基础，建设全面的信息安全合规能力，充分满足信息安全联合检查等合规性检查的要求。

1. 技管结合，安全管理在日常工作中落地

构建完善的安全管理体系和安全基线，管理为主、技术为辅，使安全管理工作的落实成为日常工作的一部分。

1. 信息化资产

|  |  |  |
| --- | --- | --- |
| 序号 | 设备名称/型号 | 数量 |
| 1 | 信息系统 | ≤60 |
| 2 | 服务器 | ≤60 |
| 3 | 虚拟化平台 | ≤2 |
| 4 | 网络安全设备 | ≤17 |
| 5 | 终端 | ≤900 |

1. 征询内容

根据《信息系统安全等级保护基本要求》（GB/T22239-2008）、重庆市卫生健康信息化主管部门关于信息安全工作的要求，安全服务商为我院至少提供以下两个服务包工作，并按服务包报价。如安全服务商根据我院现状可提供更多服务，建议增加服务内容，可在服务包三中描述并单项报价：

服务包一：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务项 | 描述 | 数量 | 一年期总价 | 三年期总价 |
| 1 | 安全评估服务 | 根据《ISO/IEC 27005信息技术–安全技术–信息安全风险管理》、《GB/T 20984-2007信息安全技术信息安全风险评估规范》等相关规范要求，由信息安全人员开展全面的风险评估，综合发现的安全问题分析网络存在的安全隐患，及危害程度，提出整改建议并及时整改。主要内容如下：1. 信息收集：根据指定主机系统收集系统的信息和业务并且进行整理和登记并提交相应内容。
2. 安全扫描：通过评估工具以远程扫描的方式对系统和网络进行安全扫描，查找网络结构、网络设备、服务器主机、中间件、数据库系统、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。出具扫描报告和作出相应整改。
3. 安全加固：针对定期安全扫描中发现的各种安全隐患，通过打补丁、修补漏洞、安全配置增强、系统架构和安全策略调整等方式及时进行加固和安全优化。安全加固须根据扫描结果来进行加固，加固前应制定详细的安全加固方案，并且经过严格的评估后方可进行。
4. 配置核查：对全网核心网络单元、业务系统和安全设备进行安全基线检查，查找主机设备、网络设备、重要应用、数据库存在的安全配置隐患，汇总基线报告，提出整改加固方案，并协助加固设备。
5. 漏洞审计：根据安全扫描情况，进行加固和修复后，重新进行一次漏洞修复情况的验证，并得出检测结果。
6. 对机房环境如（温度、湿度、用电、防水、防火、防盗等）安全评估检查并提出整改建议。
 | 2次/年 |  |  |
| 2 | 渗透测试服务 | 对关键系统进行模拟攻击，对系统和网络进行非破坏性质的攻击性测试。渗透测试内容包括针对系统进行信息泄露测试、溢出攻击测试、跨站脚本攻击测试、SQL注入测试、Cookie欺骗测试、特定错误页面检测，并识别脆弱性识别的重要手段，能够帮助客户发现设备和系统中存在的严重漏洞，帮助客户了解技术措施是否有效执行，并通过及时修补完善，避免对信息系统造成严重影响。对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层面的全面扫描与分析，扫描设备检测规则库及知识库应涵盖CVE、CNCVE、CNVD、CNNVD等标准。扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提出准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案并进行解决。 | 2次/年 |
| 3 | 安全管理制度 | 根据《中华人民共和国网络安全法》相关要求，拟定相适应的安全管理制度，并对管理人员或操作人员执行的日常管理操作建立操作规程。对安全管理制度体系的合理性和适用性进行审定、颁布、执行和检查等。需满足等级保护相应要求，达到相应标准。拟定制度加以培训和严格执行 | 1次/年 |
| 4 | 安全培训服务 | 1、信息安全意识培训：对单位非技术类员工，供应商需提供信息安全意识培训，强化员工安全意识，理解安全问题的重要性，掌握工作中的基本安全知识和安全技能。2、信息安全技术培训：对单位信息安全技术类员工，供应商需提供信息安全技术培训，帮助员工掌握信息安全技术在网络、系统、应用的理论，了解常见的网络攻击技术原理，掌握常见的攻击防护方法。 | 2次/年 |
| 5 | 应急响应与安全值守 | 对突发的网络安全事件或公共事件做出第一时间响应并处理。处理包括：现场或通过电话或网络方式远程支持解决的一般故障，在故障等级情况确定后应尽快解决故障，对重大、紧急安全响应请求后的30分钟内，工程技术人员立即到达现场解决问题或启动应急预案。 | 按需执行 |
| 6 | 应急演练 | 模拟业务系统出现各种故障情况，制定应急演练方案，完成应急演练报告。 | 2次/年 |
| 7 | 安全预警及通告服务 | 提供全年驻场服务，对最新安全威胁信息及安全事件及时以电子邮件通告方式和电话通告方式进行预警通告通告。提供及时的、针对性的各类安全信息，帮助采购人及时了解最新安全动态，并协助进行补丁更新，做好安全调整，完善安全保护措施。主要预警通告包括：系统漏洞安全通告（Windows、AIX、Linux、Solaris等），应用漏洞安全通告（Oracle、SQL Server、Sybase、Weblogic、Apache等) ，产品漏洞安全通告（Cisco、华为、防火墙、入侵检测等) ，行业安全事件通告（医疗卫生健康行业发生的热点安全事件通告与分析）。 | 按需执行，不少于12次/年 |
| 8 | 综合运维巡检服务 | 对网络设备、服务器、存储设备、安全设备、UPS、精密空调等进行全面巡检：包括但不限于：硬件状态检查：包括设备电源状态、网络接口状态、设备所在物理环境状态；性能负载检查：包括CPU、内存的占用率、日志存储空间的占用率等；为用户提供相关设备的升级服务咨询；提供整体安全巡检报告。对维护设备提供性能调优、系统漏洞发现和补救方案制定，并有确切的效果。 | 12次/年 |
| 9 | 驻场服务 | 为确保相关设备完好，运转正常，指派专人驻场运维。包括但不限于对网络系统、服务器，网络设备，机房等相关所有维护设备提供定期巡检；确定是否正常运行状态，并形成检查报告，提出现有问题及解决方案；如对机房供配电、空调、温湿度控制等设施进行检查，机房人员的出入、服务器的开机或关机等工作进行记录；新应用的设备需求，及时提交设备配置现状，以便该应用能及时运维服务；掌握设备的运行情况，就保修期、存储空间等及时进行提醒，对网络运行日志、服务器运行日志的报警信息分析和处理工作，并对监测和报警记录进行分析、评审，发现可疑行为，采取必要的应对措施等。按公安部门或其他安全部门要求完成安全检查、自查等信息安全相关工作。 | 持续执行 |

服务包二：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务项 | 描述 | 数量 | 一年期总价 | 三年期总价 |
| 1 | 信息安全规划服务 | 协助医院完成网络安全规划编制，并对网络安全规划进行跟踪验证。针对医院的安全建设，遵循 “三同步”原则——同步规划、同步建设、同步运行。提供信息安全咨询服务，基于医院信息化顶层设计和新兴技术发展方向，识别信息安全建设任务，制定未来1~3年的信息安全规划，并进行跟踪、评价、修订。输出《年度信息安全规划》 | 1次/年 |  |  |
| 2 | 安全策略优化 | 1、根据《国家信息安全等级保护管理办法》制订针对性的《信息中心网络配置规范》，即安全基线系统。 2、根据《信息系统安全等级保护基本要求》对信息中心对全网核心网元、业务系统和安全设备进行安全基线检查，查找主机设备、网络设备存在的安全配置隐患，对其进行安全策略优化。 | 2次/年 |
| 3 | 安全加固 | 1、针对服务过程中发现的系统安全隐患，通过打补丁、修补漏洞、安全配置增强、系统架构和安全策略调整等方式及时进行加固和安全优化。 2、提高系统的安全性和抗攻击能力，以期将系统的安全状况维持在较高的水平，降低安全事件发生的可能性。3、对于现有运行系统或第三方软件著作权人产品，需著作权人进行代码级修复或更改的，服务商需出具问题说明函和修复方式给与业主方，以方便业主方协调安排软件著作权人进行整改。对于正处于开发阶段系统的，需在正式上线前，对试运行系统进行安全渗透和加固服务，代码级修复的，需出具安全加固方案，由业主方协调软件著作权人进行整改加固。4、对于因系统架构或者应用软件、中间件、数据库等软件问题，可能会引起系统稳定性或者使用性的情况，需出具书面报告，详细描述因加固可能出现的后果，报甲方审核再确定是否可以加固。 | 2次/年 |
| 4 | 业务上线评估 | 提供系统上线安全评估服务。针对医院新增的业务系统，检查是否存在平台系统、应用、数据库、业务逻辑和程序代码漏洞，并提供详细的上线安全评估报告。如发现存在安全漏洞，提供详细的漏洞利用操作步骤、方法及加固建议，提出加固方案。评估内容包括但不限于以下内容访问控制限制、主机漏洞扫描、安全基线配置检查、账号弱口令检查、WEB 应用漏洞扫描等; | 按需执行 |
| 5 | 物联网运维 | 1、如有物联网相关节点设备，定期巡视物联网节点设备的部署环境，对可能影响物联网节点设备正常工作的环境异常进行记录和维护，记录维护人、维护设备、故障原因、维护结果等方面内容。2、对物联网节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。 | 2次/年 |

服务包三（增加服务内容）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务项 | 描述 | 数量 | 一年期总价 | 三年期总价 |
| 1 |  |  |  |  |  |

1. 征询时间及方式

提交解决方案及报价邮件文件截止时间：2023年3月07日北京时间17:30，该询价为初步询价，不作为最终招投标报价，可先将盖章电子档文件扫描件回复至邮箱514578628@qq.com，逾期不予受理。纸质资料(盖鲜章)请送至重钢总医院信息科(地址：重庆市重钢总医院)。

联系人：黄老师

联系电话：023-81915049

日期：2023年3月03日