附件：

**中国医学科学院肿瘤医院廊坊院区**

**安全驻场运维服务技术需求**

## 1. 项目背景

中国医学科学院肿瘤医院廊坊院区承担重要信息系统的安全保障责任，履行安全保障义务。随着国家对网络安全要求力度的加大，结合国家关键信息基础设施保护以及“网络安全等级保护2.0”的新要求以及信息系统运行情况，中国医学科学院肿瘤医院廊坊院区计划采购安全运维驻场服务项目，加大保障力度，切实维护相关关键基础资源的安全、稳定和高效运行。

## 2.项目服务原则

**（一）安全保密原则**。投标人在提供安全服务的过程中，要严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

**（二）最小影响原则**。投标人开展的安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如不可抗力无法避免，应对风险进行说明。

**（三）规范性原则**。投标人开展的安全服务工作，要由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

**（四）可控性原则**。投标人在开展安全服务工作过程中采用的工具、方法和过程要在双方认可的范围之内，保证用户对于服务过程的可控性。

**（五）质量保障原则**。投标人开展的安全服务工作需特别重视项目质量管理，项目的实施需严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

## 3.具体采购内容

|  |  |  |  |
| --- | --- | --- | --- |
| 服务类别 | 服务项目 | 服务内容 | 最少服务频率 |
| 安全咨询 | 安全规划咨询 | 通过对医院的网络安全现状、漏洞扫描以及攻防演习等情况开展差距评估和行业对标，识别业务活动中的薄弱环节，提供局域可实施性的网络和数据安全规划咨询方案，确定未来1-3年的网络和数据安全建设工作任务和行动路线图，为网络和数据安全提供指导建议。  包含：网络安全架构调整、终端管控问题、物联网医疗设备安全管理问题、脆弱性环节、设备管理、密码管理、数据安全等 | 全年 |
| 医疗信息化和智能化评级对标 | 提供智慧服务、智慧管理、互联互通、电子病历评级条款对标服务，依据医院现状，输出相关评级条款信息安全的符合和不符合情况，并附条款建设要求解读，提供整改方案，达到达标效果 | 全年 |
| 安全评估 | 信息安全风险评估 | 根据医院信息系统的实际情况开展安全风险进行识别与分析，采用传统的风险评估方法，从资产、威胁、脆弱性的角度，进行风险值量化。通过安全管理体系评估评估安全策略、规章制度、程序、表单体系的完整性，及制度是否得到贯彻执行，是否及时更新，是否全面覆盖需进行网络安全风险评估的信息系统。从风险管理的角度，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生时可能造成的危害程度，并提出有针对性的防护对策和整改措施，将风险控制在可接受的水平，最大程度地保障网络安全。 | 1次/年 |
| 系统渗透测试 | 1.根据上级安全监管单位的政策要求，结合医院的实际情况，模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，目的是侵入系统，获取系统控制权并将入侵的过程和细节产生报告给用户，由此证实用户系统所存在的安全威胁和风险，并能及时提醒安全管理员完善安全策略。如存在中高危漏洞则通知相关部门进行漏洞修复，并进行复测，出具漏扫和复测报告。  2.渗透测试包含系统数量：3个系统。 | 1次/年 |
| 新系统上线检测 | 按需对肿瘤医院新上线系统进行基线核查、漏洞扫描等方法进行安全检测，收集需上线系统的web组件，开发框架等信息，检验新上线系统的安全问题，并与开发商在上线的全阶段进行密切沟通，在开发商修复后进行闭环复测，确保漏洞修复到位。针对上线检测服务输出检测情况、修复与加固建议。 | 日常工作 |
| 安全合规 | 完善安全制度 | 根据风险评估、等保测评结果，按照医院要求对安全管理制度和规范流程进行梳理和调整，保障信息安全管理得到有效执行和部分管理风险得到有效控制。 | 日常工作 |
| 信息安全培训 | 1.针对肿瘤医院不同的对象展开不同层面的网络安全培训活动，涵盖模拟钓鱼测试等。  2.网络安全法律法规、相关文件的解读培训。 | 2次/年 |
| 网络安全等级保护合规保障 | 结合等级保护2.0相关标准要求协助医院开展等级保护定级备案、自测评、安全整改以及配合第三方测评的工作，协助医院通过等级保护测评。 | 1次/年 |
| 网络安全联合检查 | 根据当年度上级监管单位的党组责任制、绩效考核、联合检查等考核要求提供本年度的迎检服务工作。通过编写当年的工作计划以及指标解读，拆解指标完成情况并配合单位落地，在检查前准备联合检查材料资料汇编并协助肿瘤医院通过现场检查。 | 日常工作 |
| 日常安全运维 | 驻场运维 | 根据医院网络安全的实际现状提供1位安全服务工程师驻场现场开展安全运维工作：  1.监控管理安全设备的运行、解决各类安全问题。  2.制订巡检制度、操作规范、应急处理方法等。  3.排除安全隐患、处理紧急事件和重大故障等工作。  4.具备安全产品使用经验，如态势感知、防火墙、EDR、WAF、日志审计等常见安全设备运维及排错能力、具备独立的日志分析、安全设备运营维护能力。  5.驻场工程师每日对医院安全设备进行安全日志巡检、包括但不限于服务器EDR杀毒日志、终端杀毒日志分析处理并进行加固。  6.每日根据医院威胁安全事件进行汇总报告。  7.每周备份安全设备配置备份并定期进行密码修改。 | 一年 |
| 基线核查 | 根据《网络安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的标准要求，结合肿瘤医院的实际情况，在不对网络和系统产生影响的情况下采用人工检测、工具核查等方式对医院的主机设备、网络设备、安全设备、数据库、中间件等设备和系统开展例行的安全配置基线核查。 | 1次/年 |
| 漏洞扫描 | 结合医院的实际情况，采用多套自动化的检测工具，针对医院所有相关信息系统使用的主机、终端、数据库系统、网络设备、安全设备、系统应用以及弱口令等进行漏洞扫描，如存在中高危漏洞则通知相关部门进行漏洞修复，并进行复测，出具漏扫和复测报告。 | 日常工作 |
| 资产梳理 | 针对医院所有生产系统及网络设备、安全设备、终端和移动终端，应用系统、存储，利用工具扫描资产，建立台账；颗粒度为IP地址、MAC地址、服务器版本、操作系统版本、中间件版本、网络设备型号、安全设备型号、安全设备规则库版本、数据库版本、系统开发使用的开源架构、打印机版本、个人生产运维终端版本、移动终端型号版本等。 | 日常工作 |
| 漏洞评估 | 对所有的扫描漏洞、公开披露漏洞、紧急发现漏洞等，出具相关评估，划分漏洞整改等级和必要性以及整改对系统和设备的影响。列出计划表，规定整改时限。 | 日常工作 |
| “重保”专项保障 | 在重要节日、重大活动、护网行动等重保时期，加强驻场和人力保障，做好网络与数据安全隐患排查、安全防护、预警监测等安全保障技术支撑服务，必要时增派2-3人。确保肿瘤医院业务系统安全运行，避免敏感事件或影响业务的安全事件发生。 | 日常工作 |
| 安全运营 | 远程运营服务 | 结合医院安全的网络安全工作需求，组织安全运营专业团队，遵循标准化的流程开展日常安全运营工作，利用服务方所提供的安全运营工具，通过暴露面监测、资产管理、7\*24小时的威胁分析、应急响应等服务方式保障医院业务安全，快速响应主机、网络、应用、数据等安全产品的各类安全风险事件，支持通过技术手段进行自动分类和高效处置安全事件，并针对肿瘤医院的业务资产进行持续风险监视和泄露监控等，同时提供应急值守团队进行入侵事件分析及应急保障，提升医院整体网络安全运营效率。服务过程中若发生网络安全事件，服务专家需主动协助医院安全负责人对风险进行管理和控制，通过分析、溯源、处置等操作实现事件应急闭环处置，全方位保障医院业务运行安全。收集监控设备日志，对元数据进行分析，精确研判攻击和风险，加强驻点运维职能。  服务应结合原有平台对威胁分析发现的攻陷(含疑似攻陷)事件、重点攻击事件，提供有效的处置建议，并结合自动编排与响应(SOAR)、一键封堵、策略调优、人工封禁处置等措施协助安全事件闭环处置；（提供产品界面截图并加盖原厂公章）  服务应结合原有平台，编写自动化编排脚本，实现云地协同响应，提升威胁事件检测与处置效率；（提供产品界面截图并加盖原厂公章） | 一年 |
| 安全通告服务 | 利用最新漏洞研究，通过多种方式（电话、邮件、短信等）及时对互联网爆发的新型漏洞进行预警，对重大安全事件进行通告，协助肿瘤医院及时了解最新外部安全环境和最新的漏洞信息，及时规避新安全漏洞带来的风险。 | 一年 |
| 应急演练 | 根据实际情况，为医院提供应急预案编写，结合应急预案，制定详细的年度综合性网络与网络安全应急演练方案，并协助开展应急演练，应急演练前，组织全体参演人员学习演练脚本并解说注意事项，通过应急演练加强安全应急预案的可执行性。 | 1次/年 |
| 应急响应 | 根据医院实际情况，提供信息安全应急响应工作，包括应急预案、事件处置及问题修复、报告输出。提供为期一年的365×7×24小时重大安全事件的应急响应工作，半小时以内响应，通过电话、电子邮件、或通过远程控制等方式提供非现场技术支持服务。重大安全事件4小时内到现场，应急响应主要针对突发的网站安全故障、网络安全事件、应用系统安全事件、主机安全事件、黑客攻击事件等进行诊断、分析并协助解决。在网络或安全设备发生故障之后，评估网络环境、配置、状况、备份等因素，判断是否可以进行修复。在做好数据的备份、现场的记录之后，对配置进行紧急修复，尽可能的减少故障时间。 | 一年 |
| 其他 | 其他 | 协助完成其他现场支持类工作。 | 全年 |

## 4.资质要求

1. 投标人应具有有效的中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书(信息系统安全运维)一级资质；

2. 投标人应具有有效的中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书(信息安全应急处理)一级资质；

3. 投标人应具有中国信息安全测评中心颁发的信息安全服务资质证书（数据安全类）一级资质；

4. 有近两年内安全驻场运维服务经验；

5. 为保证远程运营服务可以顺利对接医院现有的安全运营平台，投标人应获得安全运营平台原厂承诺函；

## 5.项目实施服务需求

投标人需根据项目的采购、技术规格要求，采用满足要求的服务进行投标，服务必须满足项目采购主要技术规格要求，并保证能对选用服务进行很好的实施，如遇所选服务不能满足项目建设要求或项目中存在缺漏项情况，投标人应承担相应损失，投标总报价不做调整。

投标人需要具有丰富的安全实施团队保证整体项目实施的完整性、安全性、可靠性，保质保量的按时完成。

投标人须服从中国医学科学院肿瘤医院廊坊院区的统一协调，与本工程的相关单位进行积极主动的合作，在系统规划、方案设计、实施方案设计、系统集成、技术支持、运行维护等方面相互配合。