**附件3：互联网安全检测服务技术要求**

一、服务要求

| **序号** | **名称** | **内容** |
| --- | --- | --- |
| 1 | 互联网资产梳理 | **服务内容：**对所有网络资产及IT资产进行梳理盘点，按照资产类别形成资产台账，包括服务器、网络设备、安全设备、虚拟机、中间件、数据库、应用系统等。**服务频次：**签订合同后一个月内完成IT资产梳理，按照客户要求形成资产清单，每年最少2次全面资产梳理工作，对新增、变更和删减的资产进行更新。 |
| 2 | 风险评估 | **服务内容：**对信息系统系统进行风险评估，评估内容包括物理安全评估、网络安全评估、主机安全评估、应用系统评估、数据安全评估、病毒木马检查等。**服务频次：**1. 每年开展不低于2次全面风险评估，每次评估后，出具相应的风险评估报告和改进措施报告。
2. 甲方信息系统上线或升级后，根据甲方要求开展渗透测试及漏洞扫描，并出具书面的测试报告，作为甲方系统上线依据，根据甲方要求随时进行。
 |
| 3 | 漏洞扫描 | **服务内容：**对信息系统重要资产（服务器、数据库、网络设备、安全设备、应用系统等），服务提供商需提供利用检测工具进行漏洞扫描检测服务。**服务频次：**每年开展不低于4次全面漏洞扫描报告，每次服务后，提供情况评估和改进措施报告。 |
| 4 | 安全加固服务 | **服务内容：**包括对信息系统加固、网络加固、服务器操作系统加固等。1、加固服务，包括但不限于：①系统配置整改；②系统补丁协助修复；③与各外联单位（包括银行专线、政务外网专线、天网专线等）对接的接口安全加固；④根据甲方需求提供网络安全设备的离线升级服务。2、服务器操作系统加固服务，包括但不限于：①系统配置整改；②官方补丁修复；③系统账户口令、协议安全、认证权限、日志审计。**服务频次：**每年不低于1次，根据甲方需求按需开展。每次服务后，提供具有针对性的安全评估和改进措施报告。 |
| 5 | 安全应急响应服务 | **服务内容：**发生安全事件时，应急响应人员及时采取行动限制事件扩散，为医院提供安全事件应急响应服务；在限制潜在的损失与破坏服务基础上，实施人员协助客户检查所有受影响的系统；在准确判断安全事件原因的基础上，提出基于安全事件整体安全解决方案，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。**服务项：**现场技术支持，包括现场安全事件排查、现场协助日志分析、现场协助故障排除、现场协助系统恢复等**服务频次：**根据甲方需求按需开展，每次服务后，提供具有针对性的应急响应报告和安全整改建议书。 |
| 6 | 安全应急演练服务 | **服务内容：**开展信息安全应急演练，不断提高甲方开展应急工作的水平和效率，发现预案不足，进一步完善应急预案。安全应急演练场景包括DDoS攻击、蠕虫木马攻击、网页防篡改等。**服务频次：**每年不低于1次，根据甲方需求按需开展。整个应急演练过程需提供应急演练场景模板、应急演练签到文件、应急演练脚本文件、应急演练记录文件、应急演练总结报告。 |
| 7 | 关键时期安全保障服务 | **服务内容：**在重大活动、攻防演练、迎检、重要时期等期间，提供现场驻守、远程值守、监控、现场应急、处置、事后总结等方式保障医院网络安全。**服务项：安全驻守、**安全巡检、安全保障。**服务频次：**根据关键时期的时间节点和响应上级部门的要求来开展，提供关键时期安全巡检报告、总结报告及改进措施报告等。 |
| 8 | 安全培训服务 | **服务内容：**举行网络安全培训，提供定制化的信息安全意识和安全实操培训服务。包括安全意识培训、安全管理与理念培训、网络及安全设备安全运维培训、操作系统及数据库安全运维培训、应用系统安全开发与运维培训等。1、安全意识培训、安全管理与理念培训面向相关人员开展，须由经验丰富的安服人员进行现场讲授。以现实中发生的真实案例为出发点，为提供生动、真实的安全意识培训，以提高员工在生活及工作信息安全防范意识。2、网络及安全设备安全运维培训、操作系统及数据库安全运维培训、应用系统安全开发与运维培训主要面向信息科工作人员开展。**服务频次：**每年不低于1次，时长不少于半天，根据甲方需求按需开展。 |
| 9 | 安全通报服务 | **服务内容：**包括内部安全通报、外部安全通报和信息安全通报溯源服务。1、内部安全通报 根据安全评估及安全巡检所发现的安全威胁，定期汇总成安全通报，发送相关安全预警信息及通报文件。2、外部安全通报 通过相关即时通讯工具发送业内或非业内最新的安全动向及安全漏洞通告。3、如接到主管部门信息安全通报，须根据通报内容提供信息安全溯源服务。**服务频次：**内部安全通报根据需求随时开展，外部安全通报根据实时预警第一时间发送至相关技术人员，信息安全通报溯源服务在接到信息安全通报后进行。 |
| 10 | 安全体系建设 | **服务内容：**根据等级保护三级2.0标准为甲方提供详细的制度梳理、制度修订服务，并协甲方对已修订制度进行管理等工作。**制度内容包括但不限于：**1、机房安全管理制度2、网络安全管理制度3、系统运行维护管理制度4、数据安全管理制度5、固定资产管理制度6、设备管理制度7、便携式计算机及移动存储介质管理制度8、用户登记管理制度9、口令、密码管理制度10、安全责任制度11、信息审查、登记、保存、清除、备份制度12、操作权限管理制度13、安全教育培训制度14、信息系统安全应急处置预案15、信息安全组织机构16、数据备份与恢复制度17、网络安全漏洞检测和系统升级制度18、网络安全审计制度**服务频次：**安全体系建设根据甲方需求按需开展。 |

二、其他要求

1. 投标方须在本地设有服务机构，在本地有10人以上网络安全服务团队，提供团队人员社保证明和人员资质复印件并加盖投标人公章。
2. 投标方须提供不少于一个市级以上网信办或公安等网络安全主管部门应急支撑单位证书。提供证书复印件并加盖投标人公章。
3. 投标方需提供2年内护网或重保服务合同或网络安全运维服务合同2个以上。
4. 在重保或攻防演练期间，须在我院部署网络安全流量监测分析设备,、漏洞扫描设备用于重点防护，提供产品的技术参数并加盖投标人公章。
5. 信息安全应急响应服务，要求技术人员到达现场时间不超过1小时。