**等保测评及服务项目**

1.网络安全等级保护测评服务

1.1测评范围

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 定级情况 |
| 1 | 辅助生殖病历系统 | 三级 |
| 2 | 互联网诊疗系统 | 三级 |
| 3 | 医患服务平台 | 三级 |
| 4 | 全预约系统 | 三级 |
| 5 | 门户网站系统 | 二级 |
| 6 | OA办公系统 | 二级 |

1.2协助定级备案

1.2.1供应商应按照《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）的要求，遵循规范的流程，协助山东大学附属生殖医院整理信息系统备案材料，组织专家评审，并在属地公安局进行备案工作，直至取得信息系统正式备案证明；

1.3差距分析测评

1.3.1供应商应按照信息系统等级保护基本要求及测评流程，进行信息系统安全现状分析，明确信息系统目前采取的安全保护措施与网络安全等级保护相关国家标准和行业标准之间的差距，排查信息系统安全隐患和薄弱环节，查找信息系统安全建设整改需要解决的问题，确定安全需求，编制《差距分析报告》；

1.4协助安全建设整改

1.4.1供应商应协助山东大学附属生殖医院进行安全建设整改工作。确保安全建设整改工作安全、科学、有效的进行，并达到国家相关标准的技术要求，切实、高效的提升信息系统安全防护水平；

1.5安全测评

1.5.1供应商应按照《信息安全技术 网络安全保护等级基本要求》（GB/T 22239-2019）的要求，对山东大学附属生殖医院信息系统进行网络安全等级保护现状测评。依据信息系统安全等级保护测评相关标准，运用各种管理和技术手段对信息系统安全等级进行等级测评，测评过程中须完全按照国家相关标准和规范要求实施测评工作并在最终交付的等级保护测评报告中加盖认证专用章；

1.5.2测评的内容包括但不限于以下内容：

1.5.3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、安全管理中心等方面安全测评；

1.5.4安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面安全测评；

2.信息安全风险评估服务

2.1供应商应按照《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）等国家信息安全相关标准的技术要求，从风险管理角度，综合利用相关评估技术、评估方法、评估工具，对系统进行风险识别、风险分析、风险评价，对物理安全、主机安全、应用安全、网络安全、数据安全、管理安全等多方面进行评估，对所面临的威胁和脆弱性进行分析，提出有针对性的抵御风险的防护对策和整改措施，全面的识别系统中存在的及潜在的安全风险，出具信息安全风险评估报告；

2.2服务频次要求：1次/年，根据山东大学附属生殖医院安排对等保测评范围内系统提供信息安全风险评估服务；

3.网站安全监测服务

3.1供应商需通过对网站的实时信息采集和分析，对山东大学附属生殖医院门户网站系统进行远程监测。监测内容主要包括：远程网页木马监测、网页敏感内容监测、网页篡改监测和网站平稳度检测等四个部分，每季度一次出具安全监测报告；

3.2服务频次要求：在服务期内对山东大学附属生殖医院门户网站系统开展7\*24小时的实时安全监测；

4.驻场网络安全运维服务

4.1供应商需安排1名网络安全运维工程师，提供驻场网络安全运维服务；

4.2服务期间应依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）等国家信息安全相关标准的技术要求，针对信息系统的安全状况进行巡查和分析。巡检范围包括相关的服务器、网络设备和安全设备，对服务器、网络设备和安全设备等的相关日志进行分析，发现存在异常情况，提前掌握网络的安全运行情况，并对发现的问题提出整改建议，协助进行处置，出具安全巡检报告；

4.3对安全设备进行策略制定和配置等工作，主要包括安全需求收集、安全配置信息收集、安全需求分析、制定安全设备配置策略、检查安全设备有效性、持续改进安全配置策略等方面；

4.4提供专业、科学、有效的安全咨询服务，为解决网络安全问题提供解决方案；

4.5完成甲方安排的其他工作；

4.6服务频次要求：服务期内提供1名驻场服务工程师5\*8小时现场安全驻场运维。1次/季度，根据山东大学附属生殖医院安排提供每季度的安全巡检服务；

5.漏洞扫描服务

5.1供应商需采用主流专业的漏洞扫描工具（漏洞扫描采用产品必须为商业化产品）对山东大学附属生殖医院系统开展全面的漏洞扫描工作，并针对漏洞扫描结果进行汇总和分析，生成漏洞扫描报告；

5.2服务频次要求：1次/季度，根据山东大学附属生殖医院安排提供每季度的漏洞扫描服务；

6.渗透测试服务

6.1供应商需对医院门户网站等互联网系统进行渗透测试服务。模拟攻击者对指定目标业务系统进行安全性渗透测试，测试的内容包含但不限于以下内容：配置管理测试、业务逻辑测试、认证测试、授权测试、会话管理测试、数据验证测试、拒绝服务测试、Web服务测试、Ajax测试等。通过及时发现存在的web漏洞，给出整改建议，并提交渗透测试报告；

6.2服务频次要求：1次/季度，根据山东大学附属生殖医院安排提供每季度的渗透测试服务；

7.信息安全整改加固

7.1供应商需根据前期开展的各项安全检查、安全监测结果和外部检查发现的安全问题提出合理化的解决方案，并协助进行安全整改加固；

7.2服务频次要求：1次/年；

8.信息安全管理体系建设

8.1供应商应按照网络安全等级保护的相关要求，结合山东大学附属生殖医院业务系统实际情况，梳理和修订信息安全管理制度，不断完善信息安全管理体系和技术保障体系等；

8.2服务频次要求：服务期内根据山东大学附属生殖医院需求修订信息安全管理制度，开展信息安全管理体系建设。