**网络信息安全**

**运维服务项目需求书**

一、项目背景

随着医疗信息化的不断深入发展，医院已全面进入数字化时代。信息化系统不仅提高了医疗服务效率，还改善了患者就医体验。然而，随之而来的是信息安全问题的日益凸显。网络攻击、数据泄露、系统崩溃等事件频发，给医院带来巨大损失，威胁患者信息安全。因此，医院网络信息安全运维服务的需求日益迫切。

二、服务内容

|  |  |  |
| --- | --- | --- |
| 服务名称 | 服务描述 | 数量 |
| 安全驻场服务 | 1、提供专职网络信息安全运维服务人员1名，本科及以上学历，3年以上网络信息安全服务经验，服务期限为1年。  2、提供流动网络信息安全工程师服务人员1名，如重保期间或安全检查特殊期间，提供5\*8小时上门驻场服务。  3、按照医院的作息时间上下班考勤。  4、驻场人员需经过用户单位面试同意，人员确定后，服务期内不随意变更（除甲方要求变更外）。  5、需签订保密协议，在开展网络信息安全运维服务过程中，遵守国家法律法规，中标方及中标方网络信息安全运维服务人员应妥善保管自己的用户权限，如果发生涉密，则承担相应的违约责任甚至法律责任。  6、提供漏洞扫描服务，包含主机扫描、系统应用扫描等服务，并提供针对性的网络信息安全风险处理方案和网络信息安全运维服务记录。  7、根据医院实际需要，提供至少3次以上的应急演练服务，模拟黑客攻击，发起各类攻击事件，防守方检测和发现外部攻击，并对攻击采取相应的防护措施，导演方负责演练导演、监控进程、全程指导、应急处置、演习总结、技术措施与策略优化建议等技术咨询工作。  8、根据医院实际需要，提供至少2次以上的安全培训服务，通过安全专题培训的学习，提升医院信息中心工作人员的安全管理实操能力、提高医院领导对信息安全工作的重视，提升医院信息安全主管部门专业化水平，保障医院业务运行安全、稳定和连续。  9、根据医院实际需要，提供至少3次以上的重要时刻安全保障服务，在重大节假日及检查行动中提供重要时期安全保障服务，进行安全保障工作，节假日前进行安全评估。针对如元旦、春节、两会、七一建党节、国庆等重大节假日时期提供重要的安全保障服务，突发紧急信息安全事件上门服务或协助完成市及区、行业等上级主管部门下发的联合检查其他检查指标及要求。  10、根据医院需要，为医院提供其他相关网络信息安全相关日常运维服务。  11、提供《网络信息安全运维日常报告》、《漏洞扫描服务》、《应急演练文档》与视频相关材料、《网络信息安全培训PPT》、《重要时刻保障服务报告》等等。 | 1项 |
| 渗透服务 | 根据医院实际需要，为医院提供至少15个系统渗透（包含复测），对业务系统模拟黑客攻击进行安全性测试，发现系统存在的安全问题，并对过程中发现的问题及风险提出安全加固建议，推动安全问题整改，并在整改后对应用系统进行复测，提供相对应的《渗透服务报告》及《整改报告》。 | 1项 |
| 机房巡检服务 | 1、提供1个月1次的机房设备巡检服务，并提供相应的巡检报告，设备包含服务器、存储、网络设备等等；  2、协助医院做好IT资产表登记，并记录好变更情况；  3、业务宕机提供2小时以内的上门服务，协助恢复系统应用；  4、协助医院做好重要系统备份。  5、提供《机房巡检服务月底报告》、《IT资产表》。 | 1项 |