**信息系统维保服务项目需求清单**

1. **运维信息系统模块清单**

|  |  |
| --- | --- |
| **服务类别** | **服务内容描述** |
| 安全运维服务 | （1）针对安全设备网络设备，进行策略的合理性和有效性设置与检查，并对日志进行审计分析，记录保存检查和审计结果并配合用户处理调整相关策略；（2）针对客户平时业务网络调试或是改动要求，协助配合用户处理相关技术问题；（3）对策略的管理，包括：新业务上线时，梳理出符合业务要求的安全策略；业务运行期间，由于策略的不断变更，对安全策略的持续分析优化以及变更监控等。包括：策略之间冗余、冲突、可合并、策略次序不合理、策略变得宽松（不严格）等问题，导致策略管理风险增加，处理性能下降等。提供防火墙等安全策略分析优化功能，帮助用户快速发现这些问题，并支持问题原因所在，指导用户消除这些问题;(4)信息安全加固，根据等保测评问题清单，完成对应安全产品问题的加固工作； |
| 安全规划服务 | 从信息安全技术与管理出发，针对的业务与资产状况和属性，为医院设计以业务和资产为基石，在网络层面、系统层面和应用层面等不同层面的安全机制，机制中融合身份认证、访问控制、加密、恶意代码防护、审计、加固、监控、跟踪备份恢复和安全管理等安全措施进行框架性设计,提出整体解决方案。 |
| 安全培训服务 | 定期进行信息安全意识、安全技能、政策法规、产品实操等安全培训，每年两次； |
| 风险评估 | 对全网的核心资产每年进行一次风险评估，资产覆盖网络设备（交换机、路由器）、安全设备（防火墙、WEB应用防护系统、日志审计、入侵检测系统等）、服务器（Windows系统、Linux系统）和应用系统（数据库、中间件、WEB系统）等，检查系统补丁是否更新、帐号弱口令、数据库补丁是否更新、应用软件补丁是否更新等，并出具风险评估安全报告。避免由配置更改、资源过载和新出漏洞引发的安全问题，有助于实现整个信息系统的安全防护能力提高。 |