**三级等级保护服务采购需求**

目前云南大学附属医院三级等级保护服务项目主要围绕以下四个方面需求展开：

**（一）建设目标**

1、依据国家相关政策要求，联网医院（含OA办公系统）、体检、HIS（含EMR）、LIS系统四个系统三级等级保护服务总体设计指引以“一个中心、三重防护”为理念，从现有的被动防御的安全体系向事前预防、事中响应、事后审计的动态保障体系转变。从安全技术体系、安全管理体系、安全运营体系三方面来实现信息安全建设。建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系，开展组织管理、机制建设、安全规划、通报预警、应急处置、监督检查、技术检测、队伍建设、安全培训和日常运维保障等工作。

2、构建完整的互联网医院（含OA办公系统）、体检、HIS（含EMR）、LIS系统三级等级保护服务运行质量洞察运维管理体系方案，掌握IT设施的运行趋势，安全趋势、资源运行态势、业务运行态势、提高IT资源、业务应用、数据存储的安全性；预判业务系统整体健康状况和运行趋势，从而有效保障业务应用的连续运行。

3、提供数据中心运行及动态网络空间全域安全持续监测、发现、预警、防护运维服务，及时提出有效应对解决方案并组织医院协同处理可能存在的网络安全威胁；基于基础数据中心全局视角、保障系统健康稳定运行；对业务变更、技术革新、新系统测试、上线、生命周期等全局集成性工作提供30分钟内响应级别的专业支持。

4、按事件、巡检结果、月度等不同颗粒度进行多维度潜在安全性威胁的的分析，并提出相应的有效对策和改进方案。风险分析的工作不仅仅是提出补救措施，还需要定义潜在风险的预防措施。

**（二）服务内容**

| **序号** | **服务项目** | **服务要求** | **数**  **量** |
| --- | --- | --- | --- |
| 1 | 协助制定和完善信息安全管理制度服务 | 协助医院完成信息安全管理制度、知识库、灾备演练及培训等体系建设服务。  1、协助医院建设符合国家法律法规的一系列安全制度，同时制度的执行具有可操作性，并符合医院现阶段的现实情况，并提供必要的执行手段。  2、建立信息安全知识库，按照安全漏洞危害等级、修补方式、时间远近及查询权限等进行覆盖全院的系统快速查询，以提高全院信息安全综合素质。  3、定期开展灾备演练，并提供相应报告。提供安全事故库，切合医院实际情况，对演练环境做到拟真、不走过场，事后报告有详细记录，并有分析总结。  交付成果：《医院安全管理制度》、《医院信息安全知识库》、《灾备演练报告》。 | 1项 |
| 2 | 安全咨询服务 | 全周期对医院新建信息化项目从业务需求分析、系统设计、部署实施、测试运行、竣工验收等环节，提供网络安全技术咨询支持。咨询方式包括：邮件咨询、电话咨询、电话会议、现场会议等，咨询时间及方式由招标人根据实际情况指定。  交付成果：不定期提交《安全服务工作服务记录单》 | 1项 |
| 3 | 安全策略梳理优化服务 | 定期梳理针对安全和网络服务，优化安全服务策略，及时调整发生变更或废止的信息资产安全策略，建立策略池和配置档案，提高安全运维质量和水平。  定期对安全策略进行梳理，并根据医院业务需求和管理要求，进行安全策略优化。  交付成果：《策略优化报告》 | 1项 |
| 4 | 安全加固服务 | 根据网络信息系统安全评估报告及等保测评问题，制定安全加固方案。安全加固方案应覆盖医院所有服务器和网络服务，以及不同类别的操作系统、数据库和应用系统。并在出现不符合规定要求的事项后，根据需要采取纠正措施与预防性措施。  每季度针对风险评估、基线检查、策略优化等情况，协助医院完成系统安全加固，安全加固信息资产更具实际需求确定。  交付成果：《安全加固工作报告》 | 1项 |
| 5 | 渗透测试服务 | 对医院内外网的所有目标系统进行模拟黑客攻击，不限制攻击路径，不限制攻击手段以夺取目标系统的控制权为最终目的，发现目标系统网络安全防御的不足，以对业务系统的安全现状、安全保护程度进行评估，对整体安全建设进行技术/管理上的优化调整指导。采用自动化渗透测试工具辅助开展渗透测试工作，渗透测试范围应包括操作系统、数据库、应用服务的已知漏洞、不安全配置以及Web应用程序的常见漏洞等。  并基于渗透测试结果撰写报告，内容涵盖漏洞描述、危害等级、验证过程以及修复建议等。  交付成果：《渗透测试报告》，《漏洞修复指导建议》 | 1项 |
| 6 | 漏洞扫描与处置服务 | 利用专业工具每月对已有系统提供漏洞评估分析，包括但不限于应用信息系统、数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描等。  对即将上线的新业务系统或重大版本升级的系统进行安全测试，包括前端安全防护机制及业务系统本身的业务安全防护机制，避免在正式上线后因潜在的安全威胁而导致重大的业务安全风险。  并对漏洞扫描结果情况进行复测以确保整改措施有效。  投标人须提供自行准备专业漏扫工具，扫描信息资产不低于：100个。  交付成果：《漏洞扫描月报》 | 1项 |
| 7 | 安全巡检 | 投标人须提供自动化检查工具，通过专业工具和人工检查相结合的方法巡检和核查信息资产，范围需覆盖医院全部在网运行的网络、安全、操作系统、数据库和中间件。  全面掌握医院网络安全状况，分析面临的安全威胁和风险，评估安全防护水平，查找突出问题和薄弱环节，提供有针对性的防范对策和改进措施。巡检时间安排根据实际情况进行，每季度至少对医院内安全和重要网络的安全策略全面巡检一次。定期对医院内业务系统进行安全渗透检测，检查和评估目标网站是否存在SQL注入、跨站脚本、木马上传等漏洞，分析掌握Web网站中存在的薄弱环节。  交付成果：《季度安全检查报告》 | 1项 |
| 8 | 等保测评证书 | 对单位的HIS（含EMR）、LIS、互联网医院平台（含OA办公系统）、体检中心系统三级系统进行测评，并提交最终评分合格的测评报告； 1.提供信息化资产梳理、运行状态监控、安全事件分析、威胁流量检测、安全信息通告和处置方案建议等服务。2.通过专业安全扫描工具对用户单位所有包括但不限于操作系统、网络设备和应用系统等IT资源进行漏洞扫描，并输出脆弱性扫描报告，针对高、中、低风险项进行漏洞验证、安全分析和加固建议。3.根据测评报告针对网络安全等级保护对象（信息系统）存在且可处理的高、中、低风险项进行风险补偿、配置优化和策略调整，采用专业的主机加固工具提供主机安全基线扫描、加固和防护服务。  交付成果：《等保测评证书》 | 1项 |
| 9 | 上网行为管理服务（含硬件） | **提供一套行为审计服务。安全区域边界需对进出区域的行为、内容进行审计、阻拦，并进行记录，同时具备路径冗余。**  **服务实现：**为满足《信息安全技术 网络安全等级保护基本要求》第三级安全要求中，安全区域边界对于安全审计的要求，提供的网络行为审计工具。  1、为保障上网行为管理服务工具能够满足医院的使用需求，工具性能需满足：  （1）需求满足≥6个千兆电口+2个千兆光口能力，网络层吞吐量（大包）≥3.6Gb，用户数≥1200，每秒新建连接数≥4000,最大并发连接数≥150000，带宽性能：300Mb，IPSEC VPN加密性能（最高性能）：100Mb，支持用户数：1500，包转发率：45Kpps，  （2）需求满足支持两节点及两节点以上同时做主机的部署模式；  2、为保障上网行为管理服务工具的功能符合医院的业务需求，工具需具备：  （1）业务需求支持客户端SSL解密，客户端会自动推送根证书安装；  交付成果：《上网行为管理服务设置报告》 | 1项 |
| 10 | 等保一体分析服务（含硬件） | **提供一套内部数据记录服务，针对内部进出数据、日志、操作痕迹等形成区域策略。**  **服务实现：**为满足《信息安全技术 网络安全等级保护基本要求》第三级安全要求中，安全管理中心对应的审计管理要求，提供对应日志管理工具。  为保障日志审计服务工具能够满足医院的使用需求，工具性能需满足：  需求满足具备≥4个千兆电口，≥2个万兆SFP+口能力，硬件参数：规格：2U，CPU：2颗Intel Sliver 4314 2.4G（16C），内存：4\*32GB DDR4 3200，系统盘：2\*240GB SATA SSD，缓存盘：选配，数据盘：选配，标配盘位数：12，电源：白金，冗余电源。  （1）要求支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体服务、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；  （2）要求支持接入TLS加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量；  （1）使用需求工具的原厂商具有相关资质的机构颁发的信息安全服务资质（安全工程类一级）；  交付成果：《综合分析服务配置报告》 | 1项 |