安全重保技术参数

## 总体要求

根据相关国家标准、规范要求，完成自合同签订日起两年内重大活动期间信息安全保障服务。做到重保前期安全检查、中期防护、后期总结分析、全过程安全信息通报预警，建立昆明医科大学第二附属医院的重大活动期间安全防护体系、降低安全风险、提升安全防护能力、提升隐患发现能力和应急处置能力，配合医院完善信息系统安全防护体系，达到网络安全等级保护的基本要求和网络安全法要求。

采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范；

《中华人民共和国网络安全法》

《网络安全等级保护测评过程指南》GB/T28449-2018

《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019

《信息安全技术 网络安全等级保护测评要求》GB/T 28448-2019

《信息安全技术 信息系统安全通用技术要求》GB/T 20271—2006

《信息安全技术 信息系统安全管理要求》GB/T 20269—2006

《信息安全技术 网络基础安全技术要求》GB/T 20270—2006

《信息安全技术 操作系统安全技术要求》GB/T 20272—2006

《信息安全技术 数据库管理系统安全技术要求》GB/T 20273—2006

《网络安全等级保护测评机构管理办法》公信安〔2018〕765号

## 服务内容

服务详细内容如下：

### **重大活动期间安全保障服务**

为保障昆明医科大学第二附属医院的重大时期、重点时段（如：国家护网、省护网、国家重要会议等）的网络安全运行，需要专业的技术团队指定安全保障计划，以保障昆明医科大学第二附属医院网络环境的安全运行，保障重要系统敏感时期业务稳定及数据安全，避免遭受通报等问题出现。服务方需进行开展重大活动期间安全保障工作，并提供一名安全工程师开展安全运维值守工作，**人员现场值守每年不少于40日。**

详细服务内容如下：

1.1安全漏洞扫描及验证测试，在重大活动开始前期，对医院所有资产提供漏洞扫描及漏洞验证测试，并协助进行加固整改，有效避免黑客攻击行为，防患于未然，输出《漏洞扫描及验证测试报告》

1.2网络安全巡检，在重大活动开始前期对医院网络安全设备、服务器等进行安全威胁检测，及时发掘安全系统的安全弱点，对所发现的风险点进行处置，输出《网络安全巡检报告》；

1.3渗透测试，在重大活动开始前期，在取得医院许可的情况下，对医院所有对外开放业务系统提供安全渗透测试及验证服务输出《渗透测试报告》。

1.4网络资产测绘分析，在重大活动开始前期必须通过公安部第一研究所网络风险资产监测分析系统自动梳理识别昆明医科大学第二附属医院相关网络设备、安全设备、服务器、应用软件、支撑组件等类别，可识别的资产信息包括IP地址、开放的端口、使用的服务、资产名称、厂商、组件、操作系统等内容。输出《网络安全信息资产测绘报告》。

1.5安全日志分析，在重大活动期间，需对网络、安全设备（系统）监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施，提出优化建议及方案，预防安全事件发生。输出《安全日志分析报告》。

1.6应急响应，在重大活动期间提供不定期信息安全应急支持，当医院信息系统发生安全事件时，第一时间解决问题，包括远程和现场的服务。

1.7安全运维值守

在重大活动期间，服务方需提供一名人员驻场服务进行开展现场值守工作，需及时对发生的可疑安全风险事件进行及时发现、确认、阻断、恢复、溯源等工作。人员现场值守不少于40日，输出《日常安全监测报告》、《重保值守总结报告》。

1.8总结分析

服务要求：在重大活动完成后，对整个重保期间工作开展情况进行复盘及总结汇报，并输出整个重保期间所产生的文档。

1.9安全威胁预警

在重大活动期间，服务方需依据最新的网络安全形势，收集和整理最新网络安全漏洞、网络安全事件、网络安全资讯等信息，通报给医院，并提供相应的解决办法。

1.10信息安全咨询，针对处理日常工作中遇到信息系统安全方面的问题，依据最新的网络安全政策、标准及技术应用，结合网络安全趋势，定位网络安全保障需求及策略提供合理的解决方案。2个工作日内提出实质性的书面解决方案。

### **临时专项检查支撑**

协助完成上级或监管等单位对医院在信息安全方面临时性布置保障的工作任务和整改任务。完成备查材料的准备，检查现场配合及过程资料归档等。

## 交付要求

重大活动期间安全保障服务1套。

服务采购期限：两年

服务时间：合同签订后两年。

采购交付或者实施和地点：采购方指定地点。

## 服务标准、期限、效率等要求

服务期限：合同签订后两年内

服务效率：根据采购人时间进度推进项目

## 采购标的验收标准

重大活动期间安全保障服务需提交以下资料: 《漏洞扫描及验证测试报告》、《网络安全巡检报告》、《渗透测试报告》、《网络安全信息资产测绘报告》、《安全日志分析报告》、《日常安全监测报告》、《重保值守总结报告》以及重保期间所产生的其他文档

## 采购标的其他技术、服务等要求

1、甲方具有对服务方所提供的所有参与本项目人员进行考核的权力

2、服务方指派项目经理需具有 CISP 证书。

3、在本项目工程结束前，参加本项目的人员变动必须取得甲方同意，并立即安排拟订候人员予以补充

4、甲方具有对服务方参与项目人员进行能力测试的权力。对于不满足甲方要求的人员，甲方有权要求服务商无条件更换，且不能影响项目进度

5、合同签订后需按照甲方要求的时间内完成工作

6、若由于服务方自身原因导致项目进度滞后于项目计划，甲方可根据合同要求追究服务方责任

7、服务需满足国家相关标准及要求。