



复审和修订记录

日期	类型	内容	修改人	批准人
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			
	<input type="checkbox"/> 复审 <input type="checkbox"/> 修订 <input type="checkbox"/> 新增 <input type="checkbox"/> 删除			



信息安全管理要求

1 数据安全保障

- 1.1 计算机及其相关设备应放置在合适的位置, 放置地点和环境应符合厂商的规定(如通风、静电、温度、湿度), 保证其正常使用和工作方便。
- 1.2 计算机的放置应符合消防要求。对通行区内的电线和计算机缆线设定保护措施。在发生漏电或火灾的情况下, 应及时切断相应电源, 保护重要仪器设备的安全, 必要时使用灭火器灭火、通知实验室工作人员进行处理。
- 1.3 各台终端机分布于各专业组, 由相关使用人员每周清洁外部尘埃。
- 1.4 信息系统服务器和数据处理有关的计算机应配备不间断电源(UPS), 以防止数据的损坏或丢失。
- 1.5 信息科应建立异地容灾备份系统和相关工作机制, 保障重要数据在受到破坏后可紧急恢复。各容灾备份系统应具有一定兼容性, 在特殊情况下各系统间可互为备份。

2 计算机病毒感染及非法入侵防护

- 2.1.1 信息科应密切关注系统漏洞, 及时做好系统升级, 实时进行监控。
- 2.1.2 发生大规模计算机病毒感染导致系统故障或瘫痪等情况时, 应及时报告实验室主任和信息科, 及时对系统进行快速处置、恢复, 防止数据丢失, 保证信息安全。
- 2.1.3 由信息科负责对信息系统安装入侵监测系统, 实时监测对重要网段的主机系统的非法攻击行为。发生非法入侵时, 系统应及时关闭网关, 阻断非法攻击, 实行内部封闭运行, 确保系统和信息安全。

3 信息系统安全巡查与报告

- 3.1 信息管理员负责维护日常网络系统的安全, 负责杀毒软件的更新。如发现重大的无法解决的网络安全问题, 向信息中心报告。

4 培训与考核

- 4.1 信息管理员组织对信息系统使用人员进行培训, 使其掌握如何使用新系统及修改过的旧系统。
- 4.2 实验室应制定使用信息系统的使用人员、新上岗员工以及信息系统应急预案的培训与考核计划。
- 4.3 对员工的操作能力, 至少对信息系统新增功能、信息安全防护和执行信息系统应急预案的能力进行每年1次的评估。
- 4.4 科工作人员负责对计算机报警系统(通常是指检验硬件和软件运行的主计算机控制台)

5 信息保密

- 5.1 所有计算机用户应遵守中华人民共和国法律、法规和已有的安全操作规范。
- 5.2 连入网络的各部门和用户必须严格执行安全保密制度, 并对所提供信息负责。不得利用计算机和网络从事违反中华人民共和国法律、法规, 泄露本单位机密的活动, 不得制作、查阅、复制和传播有碍社会治安和不良信息。
- 5.3 系统软件、应用软件及信息数据必须实施保密措施。
- 5.4 任何人员未经授权不得泄露实验数据信息。
- 5.5 任何人员不得使用他人的账号和密码, 也不得将工作范围内可接触到的患者信息告诉其他任何未经授权的人员, 并在离开终端时及时退出程序或锁定计算机。
- 5.6 任何人员不得擅自修改数据库数据, 包括存档患者资料及相关管理数据。
- 5.7 科室工作区电脑除特定电脑外其他电脑主机均限制 USB 接口, 不得擅自拷贝信息或者复制不相关的



内容到工作电脑上,也禁止在工作电脑上娱乐。

5.7 上级部门及科室的数据查询、数据统计必须按医院和科室的有关规定,经部门领导、上级主管领导审批同意后执行。

5.8 科室内部管理文件、专业组的仪器 SOP 和项目 SOP 等文件员工未经授权不得擅自拍照、复印、电子传输给外单位或其他个人。若科室发展需要外单位人员审阅文件时,需与科室负责人签署文件保密承诺。

6 故障处理流程及应急预案

6.1 信息系统故障时,应立即向信息科报修。

6.2 应制定信息系统故障应急流程,并在发生故障时按应急流程进行处理,以便发生影响实验室提供服务能力的信息系统失效或停机时维持服务。

6.3 如果故障原因明确,信息科负责尽快恢复;如故障原因不明、情况严重,信息科主任负责召集相关工程人员评估系统故障修复时间。不能在短期内排除的,由信息科主任报告分管副院长。