中卫市卫生和计划生育局
信息安全管理制度

第一章　总则

第一条　为保证信息系统安全可靠稳定运行，降低或阻止人为或自然因素从物理层面对信息系统的保密性、完整性、可用性带来的安全威胁，结合单位及行业实际，特制定本制度。

第二条　本制度适用于中卫市卫生和计划生育局以及市属医疗卫生单位的信息系统安全管理。

第二章　职责

第三条　相关科室、单位职责:

一、 规划信息科

（一）负责组织和协调中卫市卫生和计划生育局及行业信息系统安全管理工作;

（二）负责建立中卫市卫生和计划生育局信息系统网络成员单位间的网络访问规则;对局内本部信息系统网络终端的网络准入进行管理;

（三）对局内互联网上网行为进行管理;

二、 各科室

（一）负责本科室信息安全管理工作。

（二）配合和协助业务主管科室相关制度建设，落实日常管理工作。

三、 市属各医疗卫生单位

（一）负责组织和协调本单位信息安全管理工作。

（二）对本单位建设的信息系统制定专项运维管理办法，明确信息系统安全管理要求，报中卫市卫生与计生委信息科备案。

第三章　信息安全策略的基本要求

第四条 信息系统安全管理应遵循以下七个原则:

一、 规范定级原则;

二、 依法行政原则;

三、 以人为本原则;

四、 注重效费比原则;

五、 全面防范、突出重点原则;

六、 系统、动态原则;

七、 特殊安全管理原则。

第五条 信息科应会同保密工作人员应根据业务需求和相关法律法规，组织制定信息安全策略。

第六条 信息安全策略主要包括以下内容:

一、 信息网络与信息系统必须在建设过程中进行安全风险评估，并根据评估结果制定安全策略;

二、 对已投入运行且已建立安全体系的系统定期进行漏洞扫描，以便及时发现系统的安全漏洞;

三、 对安全体系的各种日志(如入侵检测日志等)审计结果

进行研究，以便及时发现系统的安全漏洞;

四、 定期分析信息系统的安全风险及漏洞、分析当前黑客非常入侵的特点，及时调整安全策略;

五、 制定人力资源、物理环境、访问控制、操作、备份、系统获取及维护、业务连续性等方面的安全策略，并实施。

第七条 根据“谁主管、谁负责”的原则，局内建立信息安全分级责任制，各层级落实信息系统安全责任。

第四章 信息系统物理和环境安全管理

第八条 信息系统物理安全指为了保证信息系统安全可靠运行，不致受到人为或自然因素的危害，而对计算机设备、设施（包括机房建筑、供电、空调）、环境、系统等采取适当的安全措施。

第九条 信息科应采取切实可行的物理防护手段或技术措施对物理周边、物理入口、办公及生产区域等进行安全控制，防止无关人员未授权物理访问、损坏和干扰。

第十条 信息科应加强对信息系统机房及配线间的安全管理，要求如下:

一、 工作人员需经授权，方能且只能进入中心机房的授权工作区；确因工作需要，需进入非授权工作区时，需由该授权工作区人员陪同；做好机房出入登记。

二、 工作人员必须严格按照规定操作，未经批准不得超越自己职权范围以外的操作；操作结束时，必须退出已进入的操作

画面；最后离开工作区域的人员应将门关闭。

三、 非授权人员严禁操作中心机房UPS、专用空调、监控、消防及UPS供配电设备设施。

四、 未经授权，任何人员不得擅自拷贝数据和文件等资料。

五、 严禁将易燃、易爆、强磁性物品带入中心机房；严禁在机房内吸烟。

六、 发生意外情况应立即采取应急措施，并及时向有关科室和领导报告。

第五章　信息系统资产管理

第十一条 信息科应对信息和信息系统设备设施等相关资产建立台帐清单，并定期对其进行盘点清查。

第十二条 各相关科室应加强信息设备安装、调试、维护、维修、报废等环节的管理工作，防止因信息设备丢失、损坏、失窃以及资产报废处置不当引起的信息泄露。

第六章　网络与通信安全管理

第十三条 信息科采取必要的技术手段和管理措施，加强对网络和通信安全的管理，保障内外信息传递安全。网络安全管理包含网络访问控制、安全机制、网络服务、网络隔离等，要定期对重要网络设备运行情况进行安全检查，发现隐患及时上报或整改，并做好记录；定期备份重要网络和通信设备配置文件，确保发生故障时能及时恢复网络运行，保证网络的可用性。

第十四条 加强互联网安全管理，具体要求如下:

一、 互联网与内部网络必须有相关的逻辑隔离，涉及国家秘密的信息不得通过互联网传输。

二、 不得访问有关黑客网站，不得下载、安装黑客软件。

三、 局内员工访问互连网，必须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》等规定，不得利用国际互连网从事损害国家、局内及他人利益的活动。

第七章 信息系统供应商安全管理

第十五条 中卫市卫生和计划生育局对信息系统供应商实施安全管理。信息系统供应商包括设备类供应商、技术类供应商、咨询服务类供应商、或者是以上几类的任意组合。

第十六条 信息系统实施过程中，信息科应与供应商签订安全保密协议，明确信息安全要求。

第十七条 信息科应对供应商服务全过程进行监视和控制。

第八章 信息安全事件管理

第十八条 信息安全事件指导致信息资产丢失和损坏，影响信息系统正常工作甚至业务中断的事件。主要有:

一、 信息系统软硬件故障;

二、 网络通信系统故障;

三、 机房供配电系统故障 ;

四、 系统感染计算机病毒 ;

五、 信息系统遭水灾、火灾、雷击 ;

六、 信息网络遭遇入侵或攻击;

七、 信息系统内的敏感数据失窃、泄露;

八、 信息设备损坏、滥用或失窃 ;

九、 信息被非法访问、使用及篡改;

十、 违背信息安全策略规定的其他事项。

第十九条 信息安全事件管理包括组织机构、职责和规程的建立，信息安全事态及信息安全弱点的报告和评估，信息安全事件的应急处理等。

一、各市属医疗卫生单位应建立信息安全事件管理机构和应急预案，信息科负责处置信息安全事件，针对各类信息安全事件应分别制定相应的应急预案，开展必要的知识、技能、意识等培训。适时组织相关人员开展应急演练。

二、开展信息安全事态及信息安全弱点报告和评估。信息系统安全管理和维护人员应加强对网络信息系统日常检查维护，了解外部信息安全变化，充分掌握信息安全事态，及时发现和消除危及系统安全的各类安全隐患。当发现险情时，应立即报告信息安全事件处置责任科室。完成信息安全事件处理后，应及时进行评估和改进，避免再次发生，并做好记录。

三、各医疗卫生单位进行信息安全事件应急处理，要求如下:

（一）当信息系统出现险情时，维护人员和各级应急救援人员应正确履行应急预案所赋的职责和执行信息安全事件处置责任科室下达的指令。

（二）在发生网络与信息安全事件后，信息科应尽最大可能迅速收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围和评估事件带来的影响和损害。

（三）安全事件进行最初的应急处置以后应及时采取行动，抑制其影响的进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

（四）安全事件被抑制之后，通过对有关事件或行为的分析结果，找出其根源，明确相应的补救措施并彻底清除。

（五）在确保安全事件解决后，要及时清理系统、恢复数据、程序、服务恢复工作应避免出现误操作导致数据丢失。

（六）信息安全事件发生时，应及时向局机关汇报，并及时报告处置工作进展情况。事件处置中要作好完整的过程记录，保存各相关系统日志直至处置工作结束。

（七）系统恢复运行后，信息科应对事件造成的损失、事件处理流程和应急预案进行评估。对响应流程、预案提出修改意见、总结事件处理的经验和教训，撰写“信息安全事件处理报告”。同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料，属于重大事件或存在违法犯罪行为的第一时间向公安机关网络监察科室报案。

第九章　附则

第二十条 本制度由中卫市卫生和计划生育局负责解释。

第二十一条　本制度自下发之日起执行。