1.信息化建设管理委员会负责医院信息安全管理。

1.1 医院主要负责人是医院信息安全管理第一责任人。

1.2 主要职责：加强和规范本单位信息安全的分析和研判工作，监督、检查信息安全措施的实施情况，对信息系统隐患及时做出整改决策，保障医院信息安全。

1.3 信息科负责信息安全措施的主要落实，相关职能科室协助完成。

1.4 每年召开信息安全会议，全面部署工作开展，同时，根据需要适时召开会议。

1.5 定期进行安全自查，开展应急演练。

2.数据安全管理

2.1 定期开展信息系统等级保护测评并备案。

2.2 对于外包的信息系统，与外包人员签订保密协议。

2.3 患者诊疗信息、医疗服务重要数据等需及时备份，存储和流通环节需保证安全性。

2.4 使用患者诊疗信息需合规、合法，不得擅自向他人或机构提供患者的诊疗情况。

2.5 定期开展信息网络安全自查，防止患者信息泄露、篡改、丢失。

2.6 严格用户数据使用权限审批流程。

2.7 安全管理员应随时监测网络安全，防止恶意入侵，及时察觉安全隐患。

3.计算机安全管理

3.1 医院计算机操作人员必须按照计算机正确的使用方法操作计算机系统。严禁暴力使用计算机或蓄意破坏计算机软硬件。

3.2 未经许可，不得擅自拆装计算机硬件系统，若须拆装，则通知信息科技术人员进行。

3.3 计算机软件的安装和卸载工作必须由信息科技术人员进行。

3.4 计算机的使用必须由其合法授权者使用，未经授权不得使用。

3.5 医院计算机仅限于医院内部工作使用，原则上不许接入互联网。因工作需要接入互联网的，需须书面申请，经主管部门负责人确认后，报分管院长审批。接入互联网的计算机必须安装正版的反病毒软件。并保证杀毒软件实时升级。

3.6 医院任何科室如发现或怀疑有计算机病毒侵入，应立即断开网络，同时通知信息科技术人员负责处理。信息科应采取措施清除，并向主管院领导报告备案。

3.7 医院计算机内不得安装游戏、即时通讯等与工作无关的软件。

3.8 妥善使用和保管移动医疗相关设备（平板电脑、手持PDA、心电蓝牙采集盒、导联线、导联球等设备）。

3.9 医院计算机严禁接入、使用来历不明的即插即用的存储工具和网络工具。

4.网络使用人员行为规范

4.1 不得在医院网络中制作、复制、查阅和传播国家法律、法规所禁止的信息。

4.2 不得在医院网络中进行国家相关法律法规所禁止的活动。

4.3 未经允许，不得擅自修改计算机中与网络有关的设置。

4.4 未经允许，不得私自添加、删除与医院网络有关的软件。

4.5 未经允许，不得进入医院网络或者使用医院网络资源。

4.6 未经允许，不得对医院网络功能进行删除、修改或者增加。

4.7 未经允许，不得对医院网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加。

4.8 不得故意制作、传播计算机病毒等破坏性程序。

4.9 不得进行其他危害医院网络安全及正常运行的活动。

5.网络硬件安全管理

网络硬件包括服务器、路由器、交换机、通信线路、不间断供电设备、机柜、配线架、信息点模块等提供网络服务的设施及设备。

5.1 各职能部门、各科室应妥善保管安置在本部门的网络设备、设施及通信线路。

5.2 不得破坏网络设备、设施及通信线路。由于事故原因造成的网络连接中断的，根据其情节轻重予以处罚或赔偿。

5.3 未经允许，不得中断网络设备及设施的供电线路。因生产原因必须停电的，应提前通知网络管理人员。

5.4 不得擅自挪动、转移、增加、安装、拆卸网络设施及设备。特殊情况应提前通知网络管理人员，在得到允许后方可实施。

6.软件及信息安全

6.1 计算机及外设所配软件及驱动程序交网络管理人员保管，以便统一维护和管理。

6.2 管理系统软件由网络管理人员按使用范围进行安装，其他任何人不得安装、复制、传播此类软件。

6.3 网络资源及网络信息的使用权限由网络管理人员按医院的有关规定予以分配，任何人不得擅自超越权限使用网络资源及网络信息。

6.4 网络的使用人员应妥善保管各自的密码及身份认证文件，不得将密码及身份认证文件交与他人使用。

6.5 任何人不得将含有医院信息的计算机或各种存储介质交与无关人员，更不得利用医院数据信息获取不正当利益。

6.6 拥有重要系统或重要数据的科室应该及时对数据进行备份，防止系统、数据的丢失；涉及数据备份和恢复的科室要由专人负责数据备份工作，并认真填写备份日志。

6.7 数据的备份、恢复、转出、转入的权限都应严格控制。严禁未经授权将数据备份出系统，转给无关的人员或单位；严禁未经授权进行数据恢复或转入操作。

7.用户与密码的设定

7.1 信息系统的用户可分为系统管理用户、应用维护管理用户、查询用户和一般操作用户。系统管理用户指的是信息系统所使用的操作系统、网络和数据库的管理用户。应用维护管理用户指的是信息系统应用软件和应用数据的管理和维护用户。查询用户指的是信息系统应用软件和应用数据的查询用户。一般操作用户指的是使用预先编写好的程序进行操作的用户。

7.2 信息系统各类用户的管理应做到权限合理、分工明确、责任清楚、操作规范，不得违章变更、修改用户权限，不得越权操作。

7.3 各信息系统的软、硬件系统应按照运行管理需要合理设置各类用户，所有用户均必须设置密码。

7.4 用户与密码的设置应遵循如下要求：

7.4.1 登录信息系统需要有用户账号，相当于身份标识，用户帐号一般为员工工号；

7.4.2 密码为保护信息安全而对用户账号进行验证的唯一口令。

7.5系统管理用户的设定

在初始配置安装网络系统、操作系统及数据库系统时，系统管理用户应首先设置密码。系统管理用户应由不兼容岗位人员分别管理。各系统一般不得开设多个系统管理用户。

7.6应用维护管理用户的设定

系统管理用户操作人员根据应用系统的使用要求，开设应用维护管理用户，设置初始密码，并分配相应的使用权限。应用维护管理用户操作人员取得初始密码后应立即设置双密码，并由不兼容岗位人员分别管理。

7.7查询用户的设定

系统管理用户操作人员根据应用系统的使用要求，开设查询用户，设置初始密码，并分配相应的使用权限，查询用户取得初始密码后需立即更改密码。

8.计算机病毒防范措施

8.1 各部门要高度重视计算机病毒潜在危害的严重性，采取“以防为主，以治为辅”的原则，认真组织做好计算机病毒的防治工作，构筑完备有效的计算机病毒防范体系。

8.2 在组织人员进行内控安全教育和培训过程中，应增加计算机病毒防范的内容，增强员工的计算机病毒防范意识和能力。

8.3 计算机应统一安装指定的防病毒软件，开启计算机病毒实时监控功能,及时更新软件的版本和病毒库。

8.4 新购、维修、借入及借出归还的计算机设备，必须立即加装指定的防病毒软件，并进行病毒检测，经确认无毒后方可使用。

8.5 新购、维修、借入及借出归还的软盘、光盘等存储介质，以及外来的系统软件与互联网下载的软件等，要先进行计算机病毒检测，确认无毒后才可使用。严禁使用未经检测的、来历不明的软盘、光盘、U盘、移动硬盘等存储介质。

8.6 计算机的管理员用户必须设置账号密码，应选择长度至少为8位、较复杂、不易破解的密码，并定期进行更改。同时避免设置共享目录，如确需设置共享目录，则应设置共享目录密码，以免病毒通过文件共享途径传播。

8.7 各计算机用户应从硬盘引导计算机，不得使用软盘、光盘引导计算机，以免感染引导型病毒。

8.8 严禁在工作计算机上安装、运行各类盗版软件、游戏软件及与业务无关、来历不明等未经授权和确认的软件。

8.9 应随时注意计算机使用过程中出现的各种异常现象，一旦发现，应立即用计算机防病毒软件进行扫描检查。

8.10 计算机中心对计算机办公终端进行不定期的查毒、杀毒巡检。

8.11 做好系统和重要数据的备份，并妥善保管，以便能够在遭受病毒侵害后及时恢复系统和重要数据。

8.12 计算机中心必须建立计算机病毒防范预报预警机制，密切关注计算机病毒情报，跟踪计算机病毒发展的最新动态，及时了解计算机病毒，特别是有严重破坏力的计算机病毒的爆发日期或爆发条件，通过发布计算机病毒通告和防治方案向全局做出预警。

8.13 各相关部门须密切关注计算机中心发布的计算机病毒预警通告，积极采取有关防范措施，防止计算机病毒大面积爆发。

8.14 切实加强计算机与网络设备的使用管理，严格区分内网用机和外网用机的使用，避免计算机病毒交叉感染。

8.15 计算机中心应在路由器、交换机和防火墙上加强访问控制，切断计算机病毒的感染途径，并关闭不必要的端口和服务，防止计算机病毒入侵。

8.16 各类网络服务器，要安装计算机网络防病毒软件，并对经过服务器的信息进行监控，防止计算机病毒通过服务器扩散、传播。

8.17 对共享的网络文件服务器，应控制读写权限，尽量避免在服务器上运行不必要的软件程序。

8.18 对经过网络传送或接收的程序或数据，必须经过计算机病毒检测，确认无毒后方可传送或接收。