**信息科管理手册**

目录

[目 录 - 1 -](#_Toc21834)

[第一章 信息科简介 - 3 -](#_Toc10059)

[第二章 信息科工作方针、目标 2](#_Toc13307)

[第三章 组织结构 3](#_Toc11963)

[第四章 职 责 4](#_Toc8509)

[第五章 信息科管理制度 14](#_Toc4578)

[第一章 总则 40](#_Toc22048)

[第二章 网络运行 40](#_Toc15058)

[第三章 网络用户管理 43](#_Toc23723)

[第四章 网络安全管理 44](#_Toc6852)

[第五章 网络管理系统 46](#_Toc31544)

[第六章 信息科业务工作规程与流程 74](#_Toc14481)

[第七章 信息系统故障处理应急预案 80](#_Toc6043)

[附件1：护士站信息管理系统应急预案 95](#_Toc23466)

[附件2：门诊护理信息系统应急预案 98](#_Toc14507)

[附件3：门诊收费系统应急预案 99](#_Toc12)

[附件4：住院部信息系统应急预案 101](#_Toc16613)

[附件5：检验科信息管理系统应急预案 102](#_Toc25304)

[附件6：药剂科信息管理系统应急预案 104](#_Toc4920)

[附件7：放射科信息管理应急预案 105](#_Toc13407)

[附件8：信息科机房故障应急预案 107](#_Toc6983)

[一、机房漏水防治应急预案 108](#_Toc9194)

[二、设备发生被盗或人为损害事件应急预案 108](#_Toc15519)

[三、机房长时间停电应急预案 108](#_Toc23185)

[四、通信网络故障应急预案 108](#_Toc2228)

[五、不良信息和网络病毒事件应急预案 109](#_Toc26064)

[六、计算机软件系统故障应急预案 109](#_Toc22942)

[七、黑客攻击事件应急预案 110](#_Toc22463)

[八、机房设备硬件故障应急预案 110](#_Toc8175)

[九、应急处置 110](#_Toc21016)

[十、善后处置 110](#_Toc25631)

[十一、应急通讯保障 111](#_Toc6774)

[十二、装备保障 111](#_Toc16473)

[十三、数据保障 111](#_Toc2411)

[十四、队伍保障 111](#_Toc32176)

[十五、宣传、培训和演习 111](#_Toc29536)

[十六、培训 111](#_Toc6152)

[十七、预案演习 111](#_Toc24923)

**目 录**

[第一章 信息科简介 III](#_Toc366699130)

[第二章 信息科工作方针、目标 2](#_Toc366699131)

[第三章 组织结构 3](#_Toc366699132)

[第四章 职 责 4](#_Toc366699133)

[信息科职责 4](#_Toc366699134)

[信息科科长岗位职责 4](#_Toc366699135)

[成员岗位职责 4](#_Toc366699136)

[信息系统管理员职责 5](#_Toc366699137)

[数据库管理员职责 5](#_Toc366699138)

[网络管理员岗位职责 6](#_Toc366699139)

[硬件维护人员岗位职责 7](#_Toc366699140)

[软件维护人员岗位职责 8](#_Toc366699141)

[网络系统管理人员职责 9](#_Toc366699142)

[网络中心工作职责 9](#_Toc366699143)

[系统维护人员职责 10](#_Toc366699144)

[监控人员职责 11](#_Toc366699145)

[维修人员职责 12](#_Toc366699146)

[第五章 信息科管理制度 14](#_Toc366699147)

[信息科工作制度 14](#_Toc366699148)

[医院信息系统建设保障措施 14](#_Toc366699149)

[信息安全管理制度 15](#_Toc366699150)

[信息保密制度 18](#_Toc366699151)

[医院信息共享制度 21](#_Toc366699152)

[信息使用与信息管理部门沟通协调机制 23](#_Toc366699153)

[账号和密码管理制度 24](#_Toc366699154)

[用户管理制度 24](#_Toc366699155)

[系统操作分级管理制度 25](#_Toc366699156)

[信息统计与报送制度 25](#_Toc366699157)

[信息统计管理制度 25](#_Toc366699158)

[工作流程 27](#_Toc366699159)

[信息报送制度 28](#_Toc366699160)

[网络管理制度 30](#_Toc366699161)

[Internet网的管理规章制度 30](#_Toc366699162)

[网络维护管理规章制度 31](#_Toc366699163)

[网络安全管理制度和规则 33](#_Toc366699164)

[网络安全管理制度 33](#_Toc366699165)

[网络安全管理规则 34](#_Toc366699166)

[网络技术管理规则 36](#_Toc366699167)

[网络工作站管理制度 36](#_Toc366699168)

[网络服务器管理制度 37](#_Toc366699169)

[网络设备管理制度 37](#_Toc366699170)

[网络运行管理与监督 40](#_Toc366699171)

[网络运行管理制度 40](#_Toc366699172)

[网络运行监督制度 46](#_Toc366699173)

[信息系统变更、发布、配置管理制度 47](#_Toc366699174)

[机房管理制度 48](#_Toc366699175)

[“外来人员”访问管理制度 52](#_Toc366699176)

[信息科监控制度 54](#_Toc366699177)

[网络运行监控、防病毒、防入侵管理措施 56](#_Toc366699178)

[医院信息系统运行维护评价和改进方案 57](#_Toc366699179)

[技术文档管理制度 62](#_Toc366699180)

[信息科联席会议制度 64](#_Toc366699181)

[信息科值班、交接班制度 66](#_Toc366699182)

[信息科人员管理 67](#_Toc366699183)

[信息科人员录用制度 67](#_Toc366699184)

[信息科培训制度 68](#_Toc366699185)

[授权审批及人员离岗制度 69](#_Toc366699186)

[信息科人员考核制度 71](#_Toc366699187)

[医院信息来源追溯管理制度 72](#_Toc366699188)

[第六章 信息科业务工作规程与流程 74](#_Toc366699189)

[一、信息科科长工作规程与流程： 74](#_Toc366699190)

[二、综合管理岗位工作规程与流程： 74](#_Toc366699191)

[三、网络系统管理岗位工作规程与流程： 75](#_Toc366699192)

[四、硬件设备管理岗位工作规程与流程： 76](#_Toc366699193)

[五、应用系统管理岗位工作规程与流程： 77](#_Toc366699194)

[六 医院信息来源可追溯程序 78](#_Toc366699195)

[第七章 信息系统故障处理应急预案 80](#_Toc366699196)

[一、总则 80](#_Toc366699197)

[二、组织机构和职责 80](#_Toc366699198)

[三、医院信息系统出现故障报告程序 81](#_Toc366699199)

[四、医院信息系统故障分级及处理原则 82](#_Toc366699200)

[五、发生网络整体故障时的应急协调 82](#_Toc366699201)

[六、应急数据恢复工作规定 85](#_Toc366699202)

[七、故障处理程序 85](#_Toc366699203)

[八、应急转入手工操作后各系统的应急计划 88](#_Toc366699204)

[九、应急数据恢复工作规程 93](#_Toc366699205)

[十、网络服务器故障应急处理规程 93](#_Toc366699206)

[十一、应急保障 94](#_Toc366699207)

[附件1：护士站信息管理系统应急预案 95](#_Toc366699208)

[附件2：门诊护理信息系统应急预案 98](#_Toc366699209)

[附件3：门诊收费系统应急预案 99](#_Toc366699210)

[附件4：住院部信息系统应急预案 101](#_Toc366699211)

[附件5：检验科信息管理系统应急预案 102](#_Toc366699212)

[附件6：药剂科信息管理系统应急预案 104](#_Toc366699213)

[附件7：放射科信息管理应急预案 105](#_Toc366699214)

[附件8：信息科机房故障应急预案 107](#_Toc366699215)

# 第一章 信息科简介

医院信息科负责医院信息资源管理，处理，服务，及信息化建设的科室，全科围绕医院的科研、教学、医疗进行服务。

通过医院医疗、医技、行政、后勤各科室的信息整合，建立完善、高效的信息系统，做到信息的共享、统计、分析，实现资源的优化配置，为院领导提供数据支持，帮助院领导进行决策。有效地提高工作效率，提高医院市场反应能力，提高医院生产自动化水平，改善医院内部管理，提高实现风险控制能力，提高医院的核心竞争力，促进医院科学发展。

随着现代化医院的任务和工作性质要求的科学性和可靠的实用性要求，实施新管理系统。

1、 建立、完善医院信息管理系统（HIS）、电子病历系统（EMR）、[实验室信息系统](http://baike.baidu.com/view/1768887.htm" \t "_blank) (LIS)、医学影像信息系统（PACS）、放射学信息系统(RIS)、合理用药监测系统，使其系统化、完整化，逐步实施现代化。

2、信息管理系统（HIS）包括系统管理、价表管理、药库管理子系统、药房管理系统、医嘱摆药子系统、处方管理程序、消耗品管理子系统、住院登记子系统、住院收费管理系统、住院医生站、病区护士工作站、医技科室-计价录入子系统、门诊持卡就医综合管理系统、门诊挂号收费子系统、门诊医生工作站、转记帐系统（发票管理）、血库管理、术后登记与手术划价子系统、院长辅助决策支持系统、传染病与院内感染管理系统、医疗质量管理系统、医院人力资源管理系统、供应室管理系统、设备与固定资产管理系统、多媒体查询系统等基本模块。

3、曼荼罗电子病历系统（EMR）包括电子病历、病历质控、移动医疗等模块。

3、[实验室信息系统](http://baike.baidu.com/view/1768887.htm" \t "_blank) (LIS)：检验科信息系统（覆盖检验各专业）、微生物系统及与WHONET接口、质量控制管理、试剂物资管理、设备管理、科室主任工作站、、人事文档管理、排队叫号功能、项目管理、条形码管理、检验数据中心、标本流转管理、自助报告系统等功能。

4、合理用药监测系统：药物咨询及用药安全监测系统、处方审核与点评系统、抗菌药品使用分析及控制系统、临床药物咨询系统等模块。

5、医学影像信息系统（PACS）、放射学信息系统(RIS)：登记工作站软件、质控工作站软件、诊断报告工作站软件、主任管理统计工作站软件等模块。

信息科现在共计各类技术、服务人员3名。

# 第二章 信息科工作方针、目标

1、信息科工作方针：

安全稳定、互联互通、信息共享、实用高效。

2、信息科工作目标：

（1）信息科管理符合三甲医院及山东省基本现代化医院的基本要求。

信息系统建设完成率≥95%

信息更新及时率≥95%

网络运行完好率≥90%

网络故障处理及时率100%

网络设备完好率≥95%

软件运行正常率≥95%

网络系统安全事故发生次数在2次内

泄密事件发生次数0次

部门费用预算达成率≥95%

培训计划完成率100%

（2）监控网络运转，保证数据畅通运行，做好数据备份。

（3）做好数据统计，确保信息统计的准确性，提供决策依据。

（4）做好充足的准备，随时应对网络的突发事件。

（5）病人服务满意度100%。

（6）科室服务满意度100%。

（7）做好网络信息系统设备的维护保养工作，确保系统24小时正常运行。

# 第三章 组织结构

**医院信息化领导小组**

组 长：

副组长：

成 员：各职能部门负责人、各科主任护士长。

下设办公室：在信息科

办公室主任：

成 员：

**成员职责**

组长：负责信息化建设总体规划设计决策，项目决策，流程决策、人员调配决策。

副组长：负责具体项目规划、设计，负责人员召集，组织实施等工作，对工程质量负责。

成员职责：负责组织本部门的人员培训，流程制定，提出需求，协助实施，协调科室与信息化之间的关系。

办公室职责：在信息化领导小组的领导下，完成方案起草，流程收集，需求汇总等工作。负责系统调试、系统维护、人员培训、人员组织、安全管理等具体工作。

# 第四章 职 责

## 信息科职责

1、职能：在院长、分管院长的领导下，负责全院计算机网络及信息管理工作。

2、请示与上报：院长、分管副院长

3、负责医院信息化建设、管理工作。

4、制定医院信息化建设战略规划，年度工作计划并组织实施。

5、建立健全信息管理的各项规章制度。

6、利用互联网的优势，做好医院对外宣传工作。

## 信息科科长岗位职责

1、在院长领导下，负责医院信息科的日常工作。

2、制定本科室的工作计划并认真实施，做好年度工作总结。

3、负责组织全院各类应用系统的管理。

4、负责组织与外部有关部门的计算机联网和信息交换。

5、负责组织全院网络和综合数据的安全管理。

6、遵守医院各项保密制度。

## 成员岗位职责

1、参与制定信息化工作规划与年度计划。

2、负责信息化相关文档资料的归档整理工作和有关资料的统计上报工作。

3、负责院内对外数据交换。

4、负责计算机及附属设备的档案管理。

5、负责本部门各类文件收发、运转和档案资料管理。

6、协助本科室领导办理行政、对外交流和思想政治工作，负责科室内部行政事务工作。

7、完成部门领导交办的其他工作。

## 信息系统管理员职责

1、负责对工程建设各方相互往来的一切书面资料（包括信件、电报等）进行妥善保管。

2、使用和维护统一的项目管理信息系统子系统和医院办公、人力资源、项目管理软件系统，按发包人和医院要求要求录入相应的基础数据（安全质量检查记录、验工计价等）和其他资料。

3、建立数据采集系统，负责数据收集、审核、处理实现数据共享。

4、对技术资料各种文件、退件、报告的收发应办理签收登记手续，签收的资料应及时转交给相关人员，以便确认资料的完整性、准确性和有效性。

5、对各专业监理工程师确认返回的文件资料进行分类整理归类。

6、负责文件资料的借阅、办理借阅手续。

7、完成总监理工程师交办的其它工作。

## 数据库管理员职责

1、数据库管理员全面负责数据库系统的管理工作，保证其安全、可靠、正常运行。

2、负责中心的数据库服务器的管理工作，做好服务器的运行记录，当服务器出现故障时，迅速会同相关人员一同解决。

3、负责数据库系统的建设，做好服务器的维护、数据库软件的安装、数据库的建立工作，定期对数据库进行备份。

4、负责数据库服务器的安全防范管理工作。

5、协助软件开发人员完成数据库软件开发所需的各类数据库的信息。

6、为相关科室提供应用系统无法直接提供的数据

7、数据库管理员要不断加强专业知识的学习，掌握新技术和新设备，做到“一专多能”

## 网络管理员岗位职责

一、维护和保障网络与应用平台的正常运行

1、维护路由器、更换网络、交换机等网络设备；

2、保障电脑文件共享和服务器的稳定运行；

3、不定期对网络设备进行检查是否正常工作；

4、及时掌握对于系统和网络出现的异常现象应及时进行分析，处理，采取积极应对措施。

5、区内气象信息网络运行情况，发现问题及时处理；每月对信息网络运行情况进行统计分析，针对存在问题提出整改意见。

6、做好气象信息网络日常维护管理，强化灾害性天气过程、重大活动、突发事件应急处置的气象信息网络工作的技术支持，加强与上级单位的沟通协调和对基层台站的业务指导，必要时为基层台站提供现场服务，确保气象信息网络系统安全、稳定运行。辖区内主要上行资料传输及时率和数据质量达到省定标准水平。

7、建立网络使用和管理制度并贯彻执行；

8、协助硬件资产登记，使用情况记录；

二、处理各种系统故障

1、处理计算机软硬件和办公设备故障；

2、服务器安全运行和数据备份；

3、制定服务器的防病毒措施，及时下载最新的病毒库，防止服务器受病毒的侵害，协助各部门进行数据备份和数据归档；

4、负责单位所有电脑的维护和维修；

5、常规服务器、用户帐户以及密码管理；服务器、用户操作系统安全补丁升级管理；

三、负责网站的相关工作

1、保障网站信息平台的稳定运行；

2、保管好网站后台、FTP密码，严禁对外泄露；

## 硬件维护人员岗位职责

1、及时高效地完成领导分配的硬件维修等各项任务，保证硬件的正常工作。

2、维护人员要熟悉计算机原理和操作规程，熟悉仪器仪表使用方法。维护工作应遵循微机故障与维修的操作步骤、基本原则和维修方法进行。

3、经常检查供电系统是否正常，电器连接点是否牢固，用电器温度有无异常；检查机箱、显示器上的开关是否完好。对键盘、鼠标等易损件进行常规检查；对硬件系统进行外观和静态检查；对微机系统进行全面的动态检查，发现问题及时解决。

4、要定时对其进行开机上电操作，以使机器内部保持干燥。

5、网络连接线路在使用过程中会出现各种故障，如某一工作站不能连接上网或一组工作站不能连接上网，这需要维护人员熟悉网络拓扑结构，通过检查网线、网络连接点、网卡、服务器以及集线器、交换器等网络设备，找出故障点给予排除。

6、当硬件发生故障时，及时排除故障，尽快恢复系统的运行。

7、定期进行硬件的例行维护，建立每台机器的维护档案。

8、每次维修必须进行登记，包括更换的设备和配件。

9、积极参加业务学习，不断提高业务水平。

## 软件维护人员岗位职责

1、及时高效完成软件维护等各项任务，保证计算机系统的正常运行。

2、日常维护保养时，开机关机一定要严格遵守操作规程，不可随意进行，特别在微机运行过程中不能随意冷启动机器。机器运行当中，软件维护人员应时刻观察有无异常情况，及时发现及时处理。

3、软件维护人员应备有各种工具软件、常用应用软件、操作系统软件和程序语言软件并留存实验中心一份。

4、软件维护人员平时要实时、定期对计算机病毒进行查杀。及时对杀毒软件进行升级，保证杀毒的有效性。要从预防病毒入手，对外来的软件或文件应事先查杀再使用。断绝病毒传播途径。

5、积极协调硬件维护人员排除硬件故障。

6、平时应根据实验内容和计算机技术发展水平及时调整和更新网络中的各种软件，以适应运用计算机进行教学的需要。

7、平时要做好系统保护与数据备份工作，系统出现问题后能够快速恢复。

8、认真参与业务学习，不断提高自身的软件维护水平。

9、做好软件的安全保密工作。

## 网络系统管理人员职责

（1）系统管理人员负责注册用户、设置口令、授予权限，并适时加以修改，以便增强系统的保密程度；

（2）对网络和系统进行监视并适时协调管理；

（3）对系统设备经常检测和维修，防微杜渐，保证网络和系统设备处于良好的工作状态；

（4）坚持经常到站点巡视，了解各站点的人员、设备、系统应用等改正情况，以便适时进行调整和维护。

## 网络中心工作职责

（1）负责网络维护工作，对全院网络情况实施监控，随时解决网络中出现的各种情况，并在适当时候，根据医院的需求，对网络实施改造和更新；

（2）负责新上网络系统的调试，参与制定启用计划，并指导应用；

（3）负责网络计算机的安装、调试、保养和维修工作；

（4）负责对医疗信息、设备资料及消耗材料进行管理，使之充分发挥作用；

（5）负责全院人员计算机知识，系统应用的培训指导工作，使全院人员都能正确地利用计算机进行工作；

（6）设置数据库管理员，保证数据库24小时正常工作，做好数据月、周、日备份工作，备份介质由专人登记、归档、保管，确保数据的准确无误；

（7）采取严格的保密措施，防止非法用户入侵，防止病毒传播；

（8）根据医院的特点，适时开发新的应用系统，以满足医院信息的要求，扩展网络的应用范围。

## 系统维护人员职责

（1）公共字典维护人员职责

①了解公共字典库在系统应用中的作用、相互关系及目前使用情况；

②正确掌握公共字典库的创建、维护及各种参数的作用；

③对公共字典进行监控和管理，防止擅自修改字典库；

④及时调整公共字典库的内容，确保系统的正常运行，对出现的问题能够及时加以处理。

（2）系统字典库维护人员职责

系统字典是系统本身定义的、相对固定的数据。系统字典库的维护人员要保证系统字典的完整性，不要随意修改。确实需要对系统字典进行修改时，要全面考虑其作用以及与其他表的相互关系，在保证不影响其应用的前提下进行修改。

（3）药品字典库维护人员职责

①了解药品字典库在系统中的作用、地位、使用情况及药品字典库与其他字典库的关联关系；

②正确掌握药品管理的规则，合理地创建药品字典库，使各系统之间协调一致，正常有序地运行；

③对药品字典库进行监控，对出现的异常情况及时予以排除，及时对药品字典库的内容进行更新，以满足各子系统的应用；

④积累药品字典库的维护经验，加强药品字典库的维护，确保优质高效地为临床服务。

（4）价表字典库维护人员职责

①了解价表字典库在全院医疗信息中的中坚作用、地位、使用情况及字典库变化引起的连锁反应；

②根据国家物价局有关文件，合理创建价表字典库，使医院收费合理、清楚；

③及时对价表字典库进行监测和维护，处理收费项目的漏费、交计费等情况，努力使得医疗费用准确收取；

④对价表字典库的更新要考虑周全，确保各系统正常运行的情况下进行运作，同时把改变情况通报有关人员，并做记录归档。

## 监控人员职责

1、收费管理监控人员职责:

①负责监控门诊收费处、住院收费处规章制度落实情况；

②负责监控价表项目是否符合当地收费标准，新增项目是否有严格的申报审批手续，以及会计项目分类、核算项目分类归类的准确性；

③负责监控收费费别、身份、体系合同单位及收费项目等基础数据录入的准确性，发票打印是否标准，项目归类是否准确，底联发票保存是否按照财务制度要求执行；

④负责监控预交金录入的及时性、准确性，监控病人医疗过程的预交金使用情况，按规定及时进行摧款，防止病人欠费、逃费，严格执行奖罚规定，对有欠费、逃费病人的科室予以处罚；

⑤负责监控收费结帐人员执行医院有关减免费、费别修改审批权限及减免额度的情况；

⑥参与门诊收费和住院收费的日结、月结工作，监控日结帐与医疗会计现金交接工作；监控核对会计转记帐数据准确性；参与监控成本核算数据的准确性、可靠性。

2、医疗质量监控人员职责：

①负责指导和监督所有医疗信息工作站的业务工作，如门诊挂号、住院登记、入出转院、数据录入、护士工作站、差错与事故、病案编目、病案流通、综合查询等系统；

②负责监控门诊就诊病人、住院病人的费别、体系单位等病人基本信息的准确性；确保诊断、入院时间、 入院科室等医疗信息的准确性；监控住院病人入科时间、等级护理、病情状态等数据的准确性；监控病人入出转院情况，确保流动日报的准确性；监控医技科室工作量录入的准确性；监控手术例数与大、中、小手术数据的准确性；

③负责制定本院医疗质量等级标准，监控数据分析结果的质量和可靠性，并用于指导科室工作。

## 维修人员职责

一、热爱本职工作，工作认真负责，有较强的事业心和责任感。

二、遵纪守法，不以职权谋私利，不收受红包、回扣及礼品。

三、负责全院电脑和打印机的维修、保养；参与设备的安装及验收；对新装设备的质量进行监控、检验、装配和维护。

四、接到报修电话后，必须及时到现场进行诊断及处理。并填写维修反馈表。

五、对电脑和打印机的使用状况做出正确的判断，对应报废的设备作出鉴定并上报科室主管领导。

# 第五章 信息科管理制度

## 信息科工作制度

1、在院长领导下积极主动地做好全院信息管理工作。严格执行岗位职责和请示报告制度。

2、定期组织、督促、检查医院信息网络系统的各项工作，充分发挥信息功能作用，向业务科室提供信息反馈资料。

3、定期开展医疗质量和成本效益分析工作，向院领导提供医疗、管理信息，为领导决策提供服务。

4、模范遵守医院各项规章制度，尽职尽责做好本职工作，及时完成领导交给的各项任务。

5、按照国家有关规定，做好信息的保密工作。

## 医院信息系统建设保障措施

1、信息系统建设是一个系统工程，需要医院多部门共同参与和配合，才能够达到预期的目标，取得预期的效果；

2、医院信息化建设需要有中长期规划；

3、成立院级信息化领导机构，并定期召开专题会议；

4、建立信息使用与信息管理部门沟通协调机制；

5、根据医院规模和信息化建设需求，有信息化建设及运行维护的年度预算；

6、信息系统建设要有年度工作计划，并根据医院年度预算执行良好；

7、信息系统运行过程中要有相应的管理制度，保障信息系统正常运行；

## 信息安全管理制度

为保证医院计算机网络的正常运行和健康发展，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、和国家有关法律规定，结合我院实际情况，针对医院信息安全，特制定本规定。

（一）医院局域网（院内网）信息安全制度

一、医院局域网（院内网）的工作人员和连入院内网络的所有用户必须遵守《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和国家有关法律、法规，严格执行本条例。

二、院内网信息由医院信息化领导小组管理，建立健全医院的计算机网络安全管理制度，配备网络安全员，负责本部门内网络的信息安全管理工作。

三、院内网的管理部门是信息科，负责院内网的规划、建设、应用开发、运行维护与用户管理。保障网络信息、运行环境的安全;保障网络系统的正常及安全运行，用户上网采用工号登陆方式，上网操作人员须经信息科考核合格后才能上网操作。

四、院内网的信息安全监查工作由信息科负责。院内网的所有工作人员和用户必须接受医院有关部门的监督检查，并对医院采取的必要措施给予配合。

五、院内网的IP地址由信息科统一管理，任何人不得盗用未经合法申请的IP地址入网。

六、为了防止计算机病毒的侵入，凡接入院内网的工作站一律禁止使用软驱、光驱、移动硬盘、U盘等设备。如果要新安装必要的应用程序，必须事先向信息科申请并同意后，由信息科派专人在固定的机器上确保无病毒后再操作。

七、禁止自行安装任何软、硬件，禁止更改、删除任何系统文件、设置等，违反规定造成病毒传播、系统软（硬）件损坏，对整个网络造成堵塞、瘫痪等严重后果的，按情节轻重严肃处理。

八、每台计算机必须安装防病毒软件，并定期对计算机进行查毒、杀毒，升级，落实预防措施。

九、院内网的计算机一律不准上公共网络（Internet），与公共网络严格物理隔离，以确保防止病毒的感染和扩散。

十、在院内网上不允许进行任何干扰网络用户、破坏网络服务和网络设备的活动;不允许在网络上发布不真实的信息或散布计算机病毒;不允许通过网络进入未经授权使用的计算机系统;不得以不真实身份使用网络资源;不得窃取他人帐号、口令使用网络资源。

十一、院内网所有工作人员及用户必须对所提供的信息负责; 不得利用计算机网络从事危害国家安全、泄露国家秘密的活动;不得查阅、复制和传播有碍医疗秩序和淫秽、色情等不良的信息。

十二、院内网的所有用户有义务向网络管理员和有关部门报告违法犯罪行为和有害、不健康的信息，发现有上述行为者。用户必须在24小时内报告信息科。

十三、为了切实做好病毒防治工作，确保医院的计算机网络不会因感染病毒而造成停机和不必要的损失，全院各部门必须服从信息科人员的管理，积极配合做好工作。

十四、凡因违章操作，导致计算机系统病毒感染，造成严重后果者将追究当事人责任。

（二）宽带上网信息安全管理制度

一、宽带上网的所有用户必须遵守《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和国家有关法律、法规，严格执行本条例，不得在网络上接收和散布危害国家安全、宣布邪教以及不健康或色情的信息，或任何含有法律、行政法规禁止的其他内容。

二、院外网信息安全由信息化领导小组管理，建立健全医院的计算机网络安全管理制度，配备网络安全员，负责本部门内网络的信息安全管理工作。

三、宽带上网的管理部门是信息科，保障网络系统的正常及安全运行。

四、宽带上网的的信息安全监查工作由信息科负责。上网的所有工作人员和用户必须接受医院有关部门的监督检查，并对医院采取的必要措施给予配合。

五、宽带上网的IP地址由信息科统一管理，任何人不得盗用未经合法申请的IP地址入网。

六、宽带上网目前只限于部分科室。确因业务开展需要上网，须经相关审批同意后方可开通。

七、不得利用网络资源看电影、玩游戏、聊天或做其他任何与工作无关的事情。

八、不得随意将口令告诉他人或借他人账户使用网络资源，不得在网上工作过程中随意将计算机交由不熟悉的人使用。

九、不得擅自复制和使用网络上未公布和未授权的文件，不得在网络中擅自传播或拷贝享有版权的软件。严禁利用网络侵犯他人的知识产权，窃取别人的研究成果或受法律保护的资源。

十、严禁修改本机或他人IP地址及任何计算机的网络设置。不得随意搬动已联网的电脑或私自将其他电脑接入宽带。

十一、不得使用软件或硬件的方法窃取他人密码，非法入侵他人计算机系统，阅读他人文件或电子邮件，滥用网络资源，攻击计算机上系统，不得随便打开来历不明的电子邮件附件。

十二、不得在网络上捏造事实侮辱、诽谤、损害他人、单位或地区声誉的信息。

十三、不得从网上随意下载软件，以免感染病毒，造成不必要的损失。

十四、联网的电脑必须安装杀毒软件，并定期上网更新，上网工作时必须开启杀毒软件的实时监控系统。重要资料请及时备份，以防丢失。

十五、凡违反上述有关规定的，除严肃通报批评外，按医院奖惩管理条例处理。违反国家规定的，按国家法律法规处理。

## 信息保密制度

为保持医院信息系统正常运行，保护集体数据财富，保障医院和谐发展，遵循《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国保守国家秘密法》等相关国家和省有关法律法规，结合医院实际情况，制订本管理规定。

第一章 总 则

第一条 本管理规定适用于院内所有使用计算机、服务器和相关辅助设备、设施的科室和部门。

第二条 计算机信息系统的保密管理，实行控制源头、归口管理、分级负责、突出重点、有利发展的原则。

第三条 医院信息化领导小组主管全院计算机信息系统保密管理工作。医院计算机信息系统由专人负责管理相应的信息保密工作，要定期监督、检查保密管理规定的执行情况。网络管理员对信息系统的管理和操作应严格遵守保密管理规定。

第二章　保密制度

第四条　涉及国家秘密及工作秘密的计算机（含笔记本电脑）和计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相联接，必须实行物理隔离。涉密计算机（含笔记本电脑）专人专用，严禁擅自将涉密计算机（含笔记本电脑）带出办公场所。

第五条　接入国际互联网或其他公共信息网络的计算机（含笔记本电脑）不得处理、存储涉密信息。

第六条　上网信息的保密管理坚持“谁上网谁负责”的原则。

第七条 存储涉及国家秘密和工作秘密的涉密移动存储介质（含移动硬盘、优盘、软盘、光盘等）不得接入或安装在非涉密计算机上，复制和确因工作需要外出携带涉密存储介质的，须经主管领导批准。

第八条　凡在网上开设电子公告系统、聊天室的用户，应由相应的保密工作机构明确保密要求和责任。任何人不得在电子公告系统、聊天室上发布、谈论和传播国家秘密信息和工作秘密信息。

第九条　用户使用电子函件进行网上信息交流，应当遵守国家有关保密规定，不得利用电子函件传递、转发或抄送国家秘密信息和医院工作秘密。

第十条 各接入计算机信息系统（HIS）部门要对医院信息资料安全负责，严禁外来人员登录医院信息系统查询、打印有关信息资料。

第十一条 连接计算机信息系统的计算机，未经信息科许可，严禁安装、运行非日常工作需要的任何软件；严禁安装任何厂家、任何版本的操作系统以及任何有可能干扰、破坏计算机信息系统保密管理的程序。

第三章　保密监督

第十二条　涉密计算机进行维护检修时，对涉密信息应采取涉密信息转存、删除、异地转移存储等安全保密措施。无法采取上述措施时，单位保密人员和涉密计算机维护人员必须在维护现场，对维修人员、维修对象、维修内容、维修前后状况进行监督并做详细记录。涉密计算机和涉密移动存储介质淘汰、报废的一律送保密工作领导小组办公室统一销毁。

第十三条　处理涉及国家秘密文件和工作秘密文件的数字复印机、多功能一体机一律不得接入电话线，接入电话线的数字复印机、多功能一体机一律不得处理涉及国家秘密和工作秘密的文件。

第十四条 计算机个人工作桌面或开放文件夹不得摆放敏感文件和资料，办公桌禁止摆放敏感介质。

第十五条 保密工作领导小组要定期对计算机信息系统的保密检查，查处各种泄密行为。一旦发现国家秘密或工作秘密泄露或可能泄露情况，每个工作人员都有义务立即向保密工作领导小组办公室报告。对网上涉及国家秘密和工作秘密的信息要严格按照保密要求，及时予以删除。

## 医院信息共享制度

根据卫生部《医院信息系统运行与应用管理规章制度》的统一要求，特制定信息共享管理制度。

1、信息标准化管理制度

（1）所有数据都必须在指定地点连续输入并供全系统使用。

（2）同一个模板准许多人操作，但必须统一按标准执行。

（3）对系统的使用、管理、质量评估也需要按照统一标准执行。

（4）系统设计必须根据相应的标准，在设计和使用中如发现有新标准应补充完善标准。

（5）一切标准和规范都必须符合法律、法规。

（6）实现信息的标准化还应遵守统一格式，因此应遵循一定原则，主要有唯一性原则（尽管每一个元素在不同的系统中可能有不同的叫法、不同的描述，但基本原编码、含义只能有一个）、规范性原则（数据标准要规范化，这样才能提高其稳定性和可靠性）和稳定性原则（是指遵循有关标准基础形成的，不可随意改动）。

（7）凡格式化数据都应是规范的标准的，所有名词术语和项目名称都必须规范并有一个合理的代码；一切分类、统计、查询都必须依据代码进行；数据传输、交换必须依据标准。

（8）数据字典编码标准。数据字典包括国家标准数据字典、行业标准数据字典、地方标准数据字典和用户数据字典。为确保数据规范，信息分类编码应符合我国法律、法规、规章及有关规定，对已有的国家标准、行业标准及部门标准的数据字典，应采用相应的有关标准，不得自定义。使用允许用户扩充的标准，应严格按照该标准的编码原则扩充。

2、信息查询制度

（1）在医院门诊大厅和住院大厅放置的触摸查询系统，与医院内信息系统实时连网，方便病人查询医疗服务价格和药品价格。

（2）住院费用清单。每日由病区向住院病人提供医药费用汇总清单，住院病人对费用有疑问，病区护士站应及时向病人或家属解释清楚。出院病人由住院处提供明细清单。

（3）门诊病人提供配药明细清单。门诊病人对费用有疑问，可在触摸屏上查询，对不会使用触摸查询的病人，门诊服务站给予协助说明。

（4）凡门诊及住院病人对医疗费用有疑异，可向相应服务台咨询，做到有问必答，有错必纠，并做好病人的查询及投诉记录。

（5）非医院信息部门系统维护人员不得私自进入医院内网数据库进行信息查询，如因工作需要调阅数据库信息，须由本科室申请，经主管部门或主管院长签字批准后，在信息管理科安全管理员的协助下方可实施查。

（6）电子病历查询严格按照《电子病历管理制度》执行。

3、信息共享的基本要求和总体原则

（1）实现信息共享是医院信息化建设及政务公开的基本任务，是开展电子政务的重要内容之一。

（2）实施信息共享是各科室的责任和义务，各科室要本着规范公开的原则，主动上报共享信息。

（3）为了更好地进行信息共享工作，各部门在规定时间内将本部门需要发布的信息汇总到信息科发布并存档。

（4）信息共享工作由信息科负责信息的存档、网上发布及相关技术工作。

（5）根据信息的具体情况要实施安全分级管理、分内外网管理，设置不同的权限，并落实安全管理到人，严格执行安全保密制度。

## 信息使用与信息管理部门沟通协调机制

为了使科室各项计划目标顺利实现，信息科必须与职能部门、临床科室密切配合，相互协调，依据正确的政策、原则和工作计划，运用恰当的方式方法，及时排除各种障碍，促进医院信息系统的正常运转和工作全面发展。

一、信息的使用

1、信息的使用应做好记录，做到遇到问题及时沟通解决，建立问题处理记录本，涉及到系统代码等信息科不能解决的问题做好记录并交软件医院解决。

2、平时应注意与各科室负责人沟通，了解使用者遇到的问题及时反馈，方便临床工作。

二、沟通协调机制

1、建立信息反馈制度

建立信息反馈表（意见和建议等），信息反馈存根，协调完成信息化建设的相关科室使用，将填完的表格交给信息化建设负责科室。各科室应对信息化建设工作高度的重视，抓紧组织落实，增强科室间的写作能力。

2、情况通报制度

各科室在使用过程中有情况应及时通报信息科，各科室有建议权、知情权，对信息化建设的过程应知道并做到有好的想法可以直接向相关负责人员建议。

3、责任追究制度

在使用过程出现破坏系统等现象进行责任追究，有知情不报同时进行追责。

4、做好系统使用的培训

系统使用培训是各科室完成信息化建设首要的一步，良好的沟通也从这里开始，好的培训会使应用人员在短时间内掌握软件。

## 账号和密码管理制度

### 用户管理制度

1、只有院长有权向信息科索取员工的账号和密码。

2、医院员工对本人账号和密码必须遵守以下规定：

（1）新员工凭人事科报到单，到信息科配置账号和密码；员工离院时：到

信息科注销账号和密码；人事科凭信息科“已注消账号和密码”的依据同意员工调出或离院；财务科凭信息科“已注消账号和密码”的依据结付相关费用。

（2）员工不得将本人的账号和密码告诉其他人或写在任何其他人可得到的书面资料上，并每隔60天定期修改密码，对有疑问的密码应及时修改。

（3）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数据告诉其他任何未经授权的人员，并在离开终端时及时退出计算机系统。

（4）密码应至少为六位，可以是字母与数字的组合。

### 系统操作分级管理制度

1、本院系统管理首先确定为管理对象重要级别。从1-3级别区分，以一级为最高等级。不同的级别制定相应的密码权限安全管理方案。

2、一级设备为主数据库服务器和核心网络设备。这些设备的密码保存人为信息科主任与服务器管理员。所能操作人员仅限于服务器最高权限的管理员。采取统一入口管理。在一些重大操作，必须有文字记录。

3、二级设备主要是普通服务器、接入交换机和数据库密码。密码保存人为信息科主任与信息科工作人员。对于一些重大操作，必须有文字记录。

4、三级设备为安装在各使用部门的电脑，密码由相关科室设备负责人自行保管。

5、对于设备具体分级细则，在遵循以上原则的情况下，细节由信息科内部协商判断而制定。

6、对于密码，数据泄露，造成业务中断，或相关私密数据泄露。将临时通过技术手段保护与监控相应设备。待问题解决后。整理所有相关数据整理后上报医院存档。

## 信息统计与报送制度

### 信息统计管理制度

一、医院统计工作一般包括出入院数、治愈率、好转率、床位使用率、床位周转次数、平均住院天数、病员疾病分类、初诊与最后诊断符合率、临床与病理诊断符合率、手术前后诊断符合率、手术量、收入归集、工作量统计等。信息科及时做好各种统计，核对准确、完整，经院领导审签后按时上报。

二、在我院各种基础数据录入准确的基础上，根据《2007国家卫生统计调查制度》，明确数据需求、计算公式、数据来源及时限，保证各统计数据的完整、及时与准确，统计数据经使用管理部门复核后方可使用。

三、各种医疗登记，要填写完整、准确，字迹清楚，并妥善保管。对各种统计查询数据应建立健全原始记录、登记表、台账和统计资料档案管理，确保统计查询数字数出有据，准确无误。

四、信息数据由归口管理部门提出需求，明确统计指标解释、计算公式等并对各临床科室及部门发布数据，信息科在我院各种基础数据录入准确的基础上，按照归口管理部门提出的需求及统计指标解释、计算公式等负责对明确需求的数据及时收集、整理，及时反馈给归口管理部门，但不对第三方提供查询数据与发布信息数据。

五、对于已出院病人的费用等信息数据的查询，信息科在我院各种基础数据录入准确的基础上，只提供对归口管理部门的查询，不对第三方及个人提供查询数据。

六、对未经领导批准的任何个人的数据查询，信息科不予提供统计。

七、各科室的基础数据维护人员及时维护基础数据，若需信息科维护时，由归口管理部门提供由归口管理部门领导签字的申请。

八、禁止未经授权私自统计数据，禁止超越权限统计数据，禁止超范围与盗用他人账号进行数据统计查询。未经允许不得私自提供统计数据给其他单位与个人。禁止对数据进行篡改、破坏。

九、核心、重要数据的统计、使用获得批准后方可执行，同时做好记录。未按相关规定执行造成数据流出、泄密的已经发现严肃处理，造成重大损失和影响的报医院处理。

### 工作流程

一、定期收集整理医院his系统中的基础数据，根据《2007国家卫生统计调查制度》，明确数据需求、计算公式、数据来源及时限，生成统计报表，核对准确、完整后经院领导审签后按时上报，上报完成后，归档保存；

二、在我院办公网上制定信息数据查询需求表，如下表：归口管理部门可根据自己的需求填写下表，信息科给与及时反馈。本查询需求表是根据《2007国家卫生统计调查制度》，结合我院的实际情况制定的，信息科定时收集该需求表，并及时回复信息数据查询需求表

|  |  |  |
| --- | --- | --- |
| 查询目的 | |  |
| 查询范围 | |  |
| 查询对象 | |  |
| 查询起至日期 | |  |
| 查询说明 | 查询指标解释 |  |
| 计算公式 |  |
| 备注 | |  |

三、对于提供给本单位以外的第三方个人的信息数据查询，需有归口管理部门提出申请并明确需求及统计指标解释、计算公式等，经领导签字批复后，信息科方可提供信息数据查询。

四、以上步骤完成后，信息科及时对归口管理部门回复。

### 信息报送制度

第一章 总则

第一条  根据《统计法》与卫生行政部门规定，完成医院基本运行状况、医疗技术、诊疗信息和临床用药监测信息等相关数据报送工作，推动信息工作步入制度化、规范化、科学化轨道，充分发挥信息工作在正确决策、科学管理、宣传服务中的重要作用，促进医院和谐、快速、持续发展，特制定本工作制度。

第二章 组织机构及其职责

**第二条**  医院信息报送工作由分管院领导直接领导，由医务科、政工科、器械科、信息科、财务科、病案室等部门共同组成，根据卫统报表要求各部门及时整理数据并汇总审核后报信息科，由统计人员及时按卫统报表要求直报上级卫生部门。

**第三条**  各归口医院管理部门的主要职责：

（一）医务科负责上报医疗服务数据及出院病人调查表的数据的审核工作。

（二）政工科负责提供人力资源表的数据并审核数据。

（三）器械科负责提供医用设备调查表的数据并审核数据。

（四）财务科负责提供医疗收入等数据并审核数据。

（五）病案室负责提供医院出院病人调查表的数据并审核数据。

（六）信息科负责提供医疗服务数据并及时汇总按卫统报表要求直报上级卫生部门。

**第四条** 各归口医院管理部门要明确1名工作人员为本单位兼职信息员，从事具体信息报送工作。

**第五条**各归口医院管理部门信息员的工作职责：

根据上级卫生统计工作报送要点，结合本部门实际工作，完成本部门信息的收集、编写、报送工作，定期向信息科报送信息，信息科直报统计人员汇总后及时上报卫生统计部门。

第三章 信息报送程序及要求

**第六条** 各归口医院管理部门应按以下程序进行信息报送：

（一）各归口医院管理部门医务科、政工科、器械科、信息科、财务科、病案室等部门的信息员共同配合直报人员完成人力、财务和设备等统计年报、季报、月报和实时报数据上报工作。经所在部门主管负责人审核同意后，“年报”于次年1月底前报送到信息科,“月报”于次月初报送，“及时报”在最短时间内报送。

（二）对于报送上级的卫统报表信息，由信息科汇总，整理成文，经分管校领导签字后上报。

（三）对于各部门工作范围内的突发事件或其他重大紧迫事项，各部门信息员应首先及时告知信息科，同时向分管院领导报告；并在口头报送后及时向信息科补送相关文字材料。

**第七条** 信息报送的基本要求：

（一）各归口部门信息员报送信息必须坚持时效性、真实性、完整性、准确性的原则，做到及时、准确、全面、实事求是。

（二）重大突发性事件的报送必须注意时效性。重大事故、突发事件在发生后立即电话通报。

（三）各部门信息材料一般采用电子邮件的方式报送。

**第八条** 上报卫生部门的信息材料由信息科及时转交档案馆存档。

**第四章 核查和问责制度**

**第九条** 各归口医院管理部门对报送的数据进行全面核查，信息科定期对各归口部门报送信息进行统计整理，适当的信息将发布于院内网站，实现信息资源共享。

**第十条 信息统计人员应对统计数据准确性负责，新建、重大统计指标需第二人复核。因工作疏忽造成的统计失真或**自行修改统计资料、编造虚假统计数据**一经发现严肃批评教育，造成重大影响的交医院处理。**

**第五章 附 则**

**第十一条** 本办法由信息科负责解释，并根据施行情况适时修订。

**第十二条** 本办法自公布之日起施行。

## 网络管理制度

### Internet网的管理规章制度

1、 未经信息科同意，不得随意拆卸和移动计算机；严禁随意拆卸计算机上的任何接口；严禁擅自修改计算机系统设置。

2、各科室应指派专人负责管理，管理人员变动时需与信息科联系，由院部更换密码，由信息科对新任管理人员进行上网所需的各种培训。

3、 凡上机操作者，均应接受院内计算机的使用培训，或在本科室具有院内网络上机合格者的指导下使用微机；上机操作者应严格按要求进行操作，不得做任何与工作无关的操作。

4、未经院部允许，不得使用其他软件；严禁使用游戏软件和有毒软盘；杜绝未经审批的外源磁盘上机。

5、 网络设备（微机或打印机等）出现故障时，应保持现场并及时与信息科联系，严禁擅自盲目处理，以免造成更大的损坏。

6、 违反操作规定，造成人为损坏，由责任人和使用者赔偿所造成损失的全部金额，并按院规院纪处理。

7、使用计算机，严禁“黄毒”，严防“病毒”；注意防毒软件的升级，数据资料常备份，防患于未然。

8、 做好安全管理工作，数据保密；安全用电，防火、防雷、防水；爱护微机，防尘、防震、防盗，保持微机处于良好的工作状态。

9、 严禁吸烟；严禁使用电热器具；不得存放各种易爆、放射性物品；配备防盗、防火、防雷等安全防范设施，人人都会使用安全防范设施。

10、加强业务学习和专业培训，做到行为规范，忠于职守；严禁有违背道德规范的事情发生，树立良好的工作作风，积极维护医院形象。

11、注意节约电、纸、电话、磁盘、磁鼓等用品的消耗。

12、本制度适用于院内计算机管理系统及部分科室的网络系统。

### 网络维护管理规章制度

第一章 总 则

为全面完成网络维护各项任务，保障各项工作有序进行，结合我院网络维护的具体情况，特制定本办法。

网络维护各岗位人员，都要遵照岗位职责和本办法规定, 认真学习，严格执行。

第二章 组织机构及责任

网络维护下设维修协调小组、网络小组、软件小组三个班组，各司其职，全面负责各专业技术维护、后勤支撑工作。

网络维护实行责任落实到人，并张贴“宁二院网络维护分布表”。每人分管一部分网络设备，使个人责任更加明确，做好网络维护工作。

网络维护各工程师负责网络维护的技术、维护管理的日常工作，负责组织日常技术培训工作。

第三章 职 责

一、贯彻执行医院下达的各项规章制度，落实技术维护规程和网络安全运行措施。

二、负责组织全网性网络优化方案的制定，逐步提高网络安全和资源利用率，积极探索客户端网络延伸业务的新内容。

三、负责解决网络设备运行中出现的热点和难点问题；研究并提出提高网络运行质量和安全的技术措施。

四、负责对维护作业计划执行情况、设备及网络运行情况方面的检查及考核工作。

五、负责设备、系统等的数据或计费数据备份，做好相关记录，备份介质由专人统一存放和保管。

六、负责医院IP地址的管理、分配及网络安全。

七、负责已建立网管系统的实时监控，做到及时发现障碍及时处理。

八、认真制定所维护设备、服务器、系统等的年度和月度维护作业计划，做好相应系统的基础维护工作。发现问题，及时解决，认真填写维护要求的各种规范记录。

九、负责各种辅助支撑系统，业务平台、部门办公内、外网的网络安全管理，按照相关设备网络安全指导手册，采取有效防范措施，保证网络系统安全。定期对服务器等进行杀毒并及时更新病毒库。负责对整个部门的各种终端安全防护、查毒等安全工作进行监督和指导，保证各维护小组做好终端的安全保护。

第四章 规章制度

考勤制度

一、全体人员必须按时上下班, 不得迟到早退，做到有事请假。节假日及八小时外轮流值班。

二、机房值班成员之间不得随意调班与代班。遇特殊情况确需调班或代班时，需事先征得领导同意方可。

安全稳定责任制度

一、网络维护以安全、稳定为第一责任。

二、网络维护设立兼职安全员，安全员在领导下负责安全维护和消防工作的日常管理，对网络维护内的安全运行及消防工作进行检查、监督。

三、负责网络平台设备要保持清洁卫生。

四、网络维护人员要定期检查网络平台设备。

五、针对医院网络，要做好应急预案，事先对故障隐患彻底排查，消除隐患，并加强巡查防范，确保网络安全正常运行。

## 网络安全管理制度和规则

### 网络安全管理制度

（1）计算机网络系统的建设和应用，应遵守国家有关计算机管理规定参照执行；

（2）计算机网络系统实行安全等级保护和用户使用权限控制；安全等级和用户使用网络系统以及用户口令密码的分配、设置由计算机中心专人负责制定和实施；

（3）计算机中心机房应当符合国家相关标准与规定；

（4）在计算机网络系统设施附近实施的维修、改造及其他活动，必须提前通知信息科一边做好有关数据备份，不得危害计算机网络系统的安全。如无法避免而影响计算机网络系统设施安全的作业，须事先通知计算机中心，经信息科负责人和分管院长同意并采取相应的保护措施后，方可实施作业；

（5）计算机网络系统的使用人，都必须遵守计算机安全使用规则，以及有关的操作规程和规定制度。对计算机网络系统中发生的问题，有关使用单位负责人应立即向计算机室有关工程技术人员报告；

（6）对计算机病毒和危害网络系统安全的其他有害数据信息的防范工作，由计算机中心负责处理，其他人员不得擅自处理；

（7）所有上网计算机绝对禁止进行国际联网或与院外其他公共网络直接连接。

### 网络安全管理规则

（1）网络系统的安全管理包括系统数据安全管理和网络设备设施安全管理；

（2）网络系统应有专人负责管理和维护，建立健全计算机网络系统各种管理制度和日常工作制度，如：值班制度、维护制度、设备管理制度等，以确保工作有序进行，网络运行安全稳定；

（3）设立系统管理员，负责注册用户，设置口令，授予权限，对网络和系统进行监控。重点对系统软件进行调试，并协调实施。同时，负责对系统设备进行常规检测和维护，保证设备处于良好功能状态；

（4）设立数据库管理员，负责用户的应用程序管理、数据库维护及日常数据备份。每周、每月必须进行一次全备份，每日进行一次日志备份，数据和文档及时归档，备份介质应由专人负责登记、保管；

（5）对服务器必须采取严格的保密防护措施，防止非法用户侵入。系统的保密设备及密码、密钥、技术资料等必须指定专人保管，设专用库房或专柜存放。拷贝或者借用涉密载体必须按同等密级文件确定权限，履行审批手续，严禁擅自拷贝或者借用；

（6）系统应有切实可行的可靠性措施，关键设备需有备件，出现故障应能够及时恢复，确保系统不间断运行

（7）所有进入网络使用的软盘，必须经过严格杀毒处理，对造成“病毒”蔓延的有关人员，应严格按照有关条款给予行政和经济处罚；

（8）网络系统所有设备的配置、安装、调试必须指定专人负责，其他人员不得随意拆卸和移动；

（9）所有上网操作人员必须严格遵守计算机及其相关设备的操作规程，禁止无关人员在工作站上进行系统操作；

（10）保持机房的清洁卫生，并做好防尘、防火、防水、防触电、防辐射、防雷击等安全防护工作；

（11）计算机工程技术人员有权监督和制止一切违反安全管理的行为。

### 网络技术管理规则

（1）计算机工程技术人员是网络系统技术管理的直接责任者，应为满足系统功能要求和用户需求而对网络系统进行操作和维护的全部活动进行管理；

（2）网络系统中种类设备的配置，由系统负责人提出规划和计划，报医院信息系统建设领导小组审批后实施。系统硬件设备的购买、使用、保管、登记、报废等，均按医院医疗设备管理规定执行；

（3）系统软件在交付用户使用前，计算机工程技术人员必须严格按照功能要求全面调试，达到系统功能要求后交用户使用；

### 网络工作站管理制度

（1）各工作站一律不配软驱和光驱，避免因病毒传播造成数据丢失或网络瘫痪；

（2）严格按照计算机操作使用规程进行操作。操作中必须做到细致认真、快速准确，及时完成各项录入工作

（3）经常保持各种网络设备、设施整洁，认真做好网络设备的日清月检， 使网络设备始终处于良好的工作状态；

（4）机房内严禁存放易燃、易爆、易腐蚀及强磁性物品；遇有临时停电及雷电天气，应采取保护措施，避免发生意外；机房内不准吸烟、进食、会客、大声喧哗；严禁无关人员上机操作或进行其他影响网络正常运行的工作；

（5）做好工作纪录，严格交接班制度，工作中遇到的问题要及时妥善报告和处理。

### 网络服务器管理制度

为确保医院信息系统安全可靠运行，提高工作效率，保证各部门正常使用，特制定本办法。

一、服务器管理维护制度

（一）服务器必须有完整的技术文档和维护方案；

（二）服务器由服务器管理员和科室主管负责管理，日常操作维护由服务器管理员负责并实时记录，未经主管同意，其他人不得对服务器进行操作；

（三）科室派专人承担服务器管理员工作；

（四）中心服务器必须要有热备份；

（五）服务器管理员应对服务器每月进行1次检测维护并保持其清洁；

（六）微机服务器必须每月进行1次常规性检查，小型机必须每3个月进行1次常规性检查。

二、服务器密码管理制度

（一）服务器管理员密码仅限管理员及科室主管掌握，密码必须每3个月进行1次修改，并有书面记录，严格保管；

（二）密码设置不得使用简单易猜数字，其长度必须8位以上。

三、服务器的定期维护和升级制度

服务器的维护和升级必须有预案和实施记录。

### 网络设备管理制度

一、网络通讯管理设备

（一）网络通讯管理设备由信息科统一配置和安装，由网络管理员负责参数设置和管理，并做文字记录；

（二）禁止其他人员擅自改动网络配置和网卡的参数设置。如遇非法改动须及时校正，并记录在册，追查相关人员的责任；

（三）路由器、交换机等网络设备由医院统一规划，放置于一般人不易触及的地方，使用部门不能随意挪动；

（四）网络设备的管理和定期清洁维护，全院公用的由网络管理员负责，各科室的由其操作应用的班、组长负责，要保证设备的电源供给稳定，线头接插稳固；

（五）监护室、急救室等场所应避免使用无线网络设备；

（六）发现不正常工作的设备由信息科及时更换。

二、网络安全设备

（一）网络安全设备必须通过公安部门的安全认证；

（二）网络安全设备由网络管理员负责其参数的设置和管理，定期升级。

三、磁盘阵列设备

（一）磁盘阵列设备应由系统管理员定期检测，及时发现坏区并进行维护。

（二）维护信息必须记录在册。

四、打印设备

（一）打印设备应由操作人员定期进行清洁。

（二）管理人员应定期维护，保证打印设备的正常使用。

（三）保证打印机专机专用。

五、其他设备

（一）其他设备包括读卡设备、语音设备、显示设备、鼠标、键盘等。

（二）医保读卡设备及鼠标、键盘等必须配备一定数量的备用设备。

（三）应定期对设备进行检查、维护和清洁，保证其正常使用。

（四）禁止没有使用权的人员使用设备。

六、消耗材料

（一）消耗材料包括打印机色带、墨盒、打印纸，软盘，计算机网卡、网线、网络接头等。

（二）操作人员应定期检查消耗材料使用情况，及时更换色带、墨盒、打印纸等消耗材料，保证设备正常使用。

（三）网卡、网线、网络接头等应由管理员进行更换。

（四）必须配备足够数量的消耗材料。

七、电源

（一）中心机房的供电应与手术室等重要部门的供电等级相同，采取二路供电方式。

（二）服务器必须配备至少能支持半小时的不间断电源设备。

（三）急诊挂号、收费、发药等重要场所设备必须配备至少能支持30分钟的不间断电源设备。

（四）UPS定期放电（每三月一次）

八、线路

（一）网络布线要尽量避免交叉，交叉处要注意防止短路。

（二）易损线路须加套管保护。

（三）与市医保等单位通讯的线路不得挪作他用。

（四）定期检测线路，保证与市医保等单位通讯线路的畅通。

（五）主干网络及重要场所的线路应布设不同走向的备用线路。

九、设备安全

（一）凡院内、外涉及到网络线路、系统设备、停电等问题必须事先通知信息科和相关部门，以便预先做好应对措施。

（二）凡涉及设备搬迁、设备维修、系统升级等原因需要信息系统停止运行，应在预定停机前报告。

## 网络运行管理与监督

### 网络运行管理制度

第一章 总则

为了加强网络管理，提高网络服务质量，更好地为临床、教学、科研管理提供高质量的网络传输服务。同时也为了网络中心更好地与其他部门协调工作，明确网络运行人员的工作范围、工作内容、工作职责，特制定本网络运行管理规范，供网络运行管理人员参照执行。

第二章 网络运行

网络运行主要包括医院各科室的运行、监控、维护和管理工作，负责保存和维护网络运行的各种工作日志，具体工作内容和要求如下：

一、工作内容

网络中心在各楼层的机房设备管理、主干节点管理、网络故障管理、网络运行日志管理、设备配置管理、网络设备维修与更换、网络异常处理、IP地址规划分配与管理、设备端口分配与管理、VLAN划分与分配、文档资料管理、网络安全管理、网络用户管理、网络管理系统的使用与维护等。

二、主干设备管理

对于分布在各建筑物内网络配线间的主干设备，做到每半年巡检一次，检查电源情况、设备运行状态、通风散热情况等，对发现的问题及时处理。

三、设备配置管理

设备配置管理包括以下几个方面：

（一）设备分配和安装，对安装在各处的网络设备登记，建立设备分布台账，详细记录各设备的型号、硬件配置、软件版本、购置日期、安装日期、使用单位、负责人、设备保修等信息；

（二）建立各设备的配置信息电子档案，历次配置更改记录、密码信息、设备标识、IP地址，配置更改时间、修改人员等，建立设备配置文档。

（三）对于分布在各楼宇的网络设备应安排专人对设备的配置进行维护和更改。

四、IP地址的规划、分配与管理

（一）根据各用户对IP地址的需求，规划制定IP地址的分配方案，分配方案要有一定的余量，对于不足的IP地址应及时以书面形式申请。

（二）建立IP地址分配文档，详细记录IP地址对应的MAC地址、使用单位、VLAN信息、使用人、机器位置、接入位置、分配日期等。

（三）对已分配的IP地址能够方便的查询、收回、禁用和开通。

五、端口分配与管理

建立各设备的端口分配档案，建立端口分配文档，记录的信息包括：设备信息、端口号、楼号和房间号、房间内信息插座编号、下连设备类型、使用单位、分配时间、接入时间等，保持设备配置与档案的一致，方便查询和更改。

六、网络故障管理

（一）网络故障的现象包括网络不通、网络性能严重降低、无法访问指定的网络资源、网络时通时断、重复认证等；

（二）网络不通的原因包括：设备故障、端口故障、线路故障、端口分配错误、地址绑定错误、路由错误、IP地址冲突、终端本身的故障等；性能下降的原因可能是网络异常流量、网络拥塞、设备故障、线路通信质量等；无法访问指定的网络资源可能是网络不通、域名解析问题、资源本身的问题等；

（三）网络故障的来源包括：用户投诉、网管系统报警、日常网络检查、定期巡检等；

（四）故障记录，建立网络故障日志文档，对发现的各种故障现象进行详细的记录，记录内容包括：故障发生的时间、故障现象、故障位置、故障来源、故障记录人员等；

（五）故障分析与定位：根据故障现象和故障位置，对故障进行分析，找出故障的原因和发生的具体位置，并记录到故障日志中；

（六）故障处理：根据故障的具体情况，尽量采取备用资源尽快恢复网络通讯，对不同的故障类型，制定不同故障处理响应时间，对网络运行人员不能处理的故障（如电源、空调、线路等），应尽快通知相关部门。对故障的处理情况也应记录到故障日志中；

（七）故障恢复，对于用户投诉的故障，在故障处理后应通过相应的途径给用户反馈处理结果，并对故障恢复的结果、时间记录到日志中。对于不能及时恢复的故障应通知用户，说明情况和原因；

（八）故障设备报修，对确定存在故障的设备，记录详细的故障信息，以书面或邮件的形式报办公室处理，具体规定参见《网络设备管理规范》。

七、网络维护与停网

在需要网络维护时，如果需要停止部分或全部网络传输，应提前作出网络维护计划，并提前通知受影响的网络用户，停网的时间尽可能短，影响的范围尽可能小，并且选择在下班以后的时间进行。

第三章 网络用户管理

一、接入申请与登记

网络运行人员接到接入申请后，根据网络资源（端口、线路等）的情况，决定是否允许接入，对接入用户的信息，应建立相应的数据库进行登记，以方便管理和查询。

二、办公网络用户管理

（一）接入外部网络或内部网络，每台入网计算机在信息科登记备案，备案信息包括：VLAN、IP地址、MAC地址、接入位置、使用单位、负责人、开通时间等。

（二）安装专用的服务器管理接入用户的备案信息。

（三）网络运行人员负责各服务器的运行维护工作，做到定期检查、实时监控，保证服务器系统的正常运转，安排专人负责服务器系统的管理。

（四）网络运行人员负责用户接入信息的录入、维护工作。

第四章 网络安全管理

一、网络异常流量

采取技术措施，对网络异常流量进行检测，对发现的流量异常进行分析、定位和隔离，并做好日志工作。

二、网络病毒

对于网络中的蠕虫病毒，应采取技术手段进行检测。对发现的网内病毒源通过关闭端口及时进行隔离，并通知有病毒的计算机负责人进行处理。对病毒的检测和处理要做好日志工作。对于外网进入的网络病毒应在边界路由器上做针对性地访问控制，对已实施的访问控制要做好日志和备案工作。

三、对外扫描

应严格控制内部网络用户的对外扫描，采取相应的技术手段加强对扫描的检测，对发现的扫描事件，及时分析，落实扫描源，通过禁用IP、关闭端口等措施进行隔离，并做好日志备案工作。

四、网络攻击

采取必要的技术手段，对网络攻击事件进行检测。对发现的攻击事件，及时分析，定位责任人，调整安全措施，做好日志记录工作。

五、未经允许的网络服务

根据目前我院网络的具体情况，不允许各接入用户提供以下网络服务。网络运行人员负责对网上存在的非法服务进行检测，并强制其停止。

（一）不允许在内部或外部网络上提供DHCP动态地址分配服务。目前我院内外网采取静态IP地址分配，并且捆绑到用户和计算机；

（二）不允许在网络上提供NAT地址转换服务，目前信息科可以提供足够IP地址满足用户的需求；

（三）不允许在网络上提供各种网络代理，包括HTTP代理、SMTP代理、FTP代理、Socket代理，各网络用户应使用分配的合法IP地址直接访问互联网；

（四）不允许提供未经备案的其他网络服务，有些网络服务由于技术方面的原因，对网络带宽占用很大，影响其他网络用户的正常应用。

六、网络安全隐患检查

网络运行人员主要负责各路由器、交换机的安全管理，也包括几个用户认证服务器、用户接入管理服务器、计费服务器的安全管理。检查系统的版本信息，确定最新的版本和补丁，并及时进行升级维护。定期检查系统运行日志，发现系统存在的安全隐患，采取相应的措施。对于服务器、路由器、交换机的管理密码加强管理，定期更换，保证不泄密。

七、安全对策与技术措施可以采取以下措施加强网络系统的安全：

（一）对网络运行中需要的服务器系统，进行安全漏洞扫描，及时进行版本升级、安装补丁程序，配置相应的主机防火墙防止攻击。定期分析系统日志，消除安全隐患；

（二）对路由器、交换机系统，跟踪最新的安全更新信息，及时升级和打补丁程序；

（三）对于确定的安全责任事件，如网络病毒、对外扫描、对外攻击、流量异常、国际流量超标，及时采取封IP地址、封接入端口、取消接入资格等措施，督促责任人进行整改，整改完成后，责任人应以书面报告的形式，经本单位备案盖章后，报信息科申请恢复开通网络。

（四）安装必要的攻击检测系统，实时监测网上的攻击事件，并进行相应的处理。

第五章 网络管理系统

目前在网络上安装了网络管理系统，能够对全院的主干网络设备进行监控和管理，网络运行人员应熟练掌握该系统的使用，充分利用该系统对网络进行管理，发挥网管系统应有的作用。

一.设备状态监视

网络运行人员每天定期察看系统中的网络状态，及时发现存在的问题。

二、用户追踪

网络运行人员应能够熟练掌握在系统中快速定位特定用户接入信息的方法，发现用户的接入位置，为采取进一步的措施提供信息。

三、网络拓扑

利用该功能，对整个网络进行全局的监控。网络运行人员应熟练掌握该功能的使用，能够通过网络拓扑图快速了解网络的运行状态。

四、网络性能分析

借助网络管理系统，以及其他的网络管理活动，及时掌握网络的整体运行性能和网络瓶颈，提交网络性能和需求分析报告，为网络扩容或升级改造提供决策依据。

### 网络运行监督制度

计算机室对计算机网络系统安全保护工作行使下列监督职权：

（1）监督、检查、指导计算机网络系统安全保护工作；

（2）查处危害计算机网络系统安全的违规行为；

（3）计算机工程技术人员发现计算机网络系统安全隐患时，可立即采取各种有效措施予以消除；

（4）计算机工程技术人员在紧急情况下，可以主涉及计算机网络安全的特定事项采取特殊措施进行防范；

（5）履行计算机网络系统安全保护工作的其他监督职责。

## 信息系统变更、发布、配置管理制度

1、为规范信息系统变更、发布、配置与维护管理，提高软件管理水平，优化软件变更与维护管理流程，特制定本制度。

2、信息系统变更、发布、配置工作可分为下面三类类型：功能完善维护、系统缺陷修改、统计报表生成。功能完善维护指根据业务部门的需求，对信息系统进行的功能完善性或适应性维护；系统缺陷修改指对一些系统功能或使用上的问题所进行的修复，这些问题是由于系统设计和实现上的缺陷而引发的；统计报表生成指为了满足业务部门统计报表数据生成的需要，而进行的不包含在应用系统功能之内的数据处理工作。

3、信息系统变更、发布、配置工作以任务形式由需求方（一般为业务部门）和维护方（信息科和软件厂商）协作完成。信息系统变更、发布、配置过程类似软件开发、发布、配置，大致可分为四个阶段：任务提交和接受、任务实现、任务验收和程序下发上线。

4、需求部门提出系统需求，并将需求整理成《信息系统变更申请表》，由部门负责人审批后提交给信息科。

5、信息科负责接受需求并上报给信息科分管院长。分管院长分析需求，并提出系统变更建议。信息科根据变更建议审批《信息变更申请表》。

6、信息科根据部门提供的需求与软件开发商联系协同实现信息系统变更需求，产生供发布的程序。

7、信息科组织相关业务部门的信息系统最终用户对系统程序变更进行测试。

8、信息系统变更程序测试完成后，由信息科配置完善信息系统，正式发布并通知需求部门。

9、信息科出具信息系统变更验收报告，需求部门签字验收。

## 机房管理制度

一、日常行为准则：

（一）注意环境卫生。禁止在机房吃食物、抽烟、随地吐痰；对于意外或工作过程中弄污机房地板和其它物品的，必须及时采取措施清理干净，保持机房无尘洁净环境。

（二）机房应安排人员值日，负责机房的日常整理和行为督导。

（三）进出机房必须换鞋，雨具、鞋具等物品要按位摆放整齐。

（四）注意检查机房的防晒、防水、防潮，维持机房环境通爽，注意天气对机房的影响，下雨天时应及时主动检查和关闭窗户、检查去水通风等设施。

（五）机房内部不应大声喧哗、注意噪音／音响音量控制、保持安静的工作环境。

二、机房安保制度：

（一）出入机房应注意锁好防盗门。对于有客人进出机房，机房相关的工作人员应负责该客人的安全防范工作。最后离开机房的人员必须自觉检查和关闭所有机房门窗、锁定防盗装置。应主动拒绝陌生人进出机房。

（二）工作人员离开工作区域前，应保证工作区域内保存的重要文件、资料、设备、数据处于安全保护状态。如检查并锁上自己工作柜抬、锁定工作电脑、并将桌面重要资料和数据妥善保存等等。

（三）工作人员、到访人员出入应登记。

（四）外来人员进入必须有专门的工作人员全面负责其行为安全。

（五）未经主管领导批准，禁止将机房相关的钥匙、保安密码等物品和信息外借或透露给其它人员，同时有责任对保安信息保密。对于遗失钥匙、泄露保安信息的情况要即时上报，并积极主动采取措施保证机房安全。

（六）禁止带领与机房工作无关的人员进出机房。

（七）绝不允许与机房工作无关的人员直接或间接操纵机房任何设备。

（八）出现机房盗窃、破门、火警、水浸、110报警等严重事件时，机房工作人员有义务以最快的速度和最短的时间到达现场，协助处理相关的事件。

三、机房用电安全制度

（一）机房人员应学习常规的用电安全操作和知识，了解机房内部的供电、用电设施的操作规程。

（二）机房人员应经常实习、掌握机房用电应急处理步骤、措施和要领。

（三）机房应安排有专业资质的人员定期检查供电、用电设备、设施。

（四）在真正接通设备电源之前必须先检查线路、接头是否安全连接以及设备是否已经就绪、人员是否已经具备安全保护。

（五）严禁随意对设备断电、更改设备供电线路，严禁随意串接、并接、搭接各种供电线路。

（六）如发现用电安全隐患，应即时采取措施解决，不能解决的必须及时向相关负责人员提出解决。

（七）禁止在无人看管下在机房中使用高温、炽热、产生火花的用电设备。

（八）在使用大功率的用电设备前，必须得到上级主管批准，并在保证线路保险的基础上使用。

（九）在外部供电系统停电时，机房工作人员应全力配合完成停电应急工作。

四、机房消防安全制度

（一）机房工作人员应熟悉机房内部消防安全操作和规则，了解消防设备操作原理、掌握消防应急处理步骤、措施和要领。

（二）任何人不能随意更改消防系统工作状态、设备位置。需要变更消防系统工作状态和设备位置的，必须取得主管领导批准。工作人员更应保护消防设备不被破坏。

（三）如发现消防安全隐患，应即时采取措施解决，不能解决的应及时向相关负责人员提出解决。

（四）最后离开的机房工作人员，应检查消防设备的工作状态，关闭将会带来消防隐患的设备，采取措施保证无人状态下的消防安全。

五、机房硬件设备安全使用制度

（一）机房人员必须熟知机房内设备的基本安全操作和规则。

（二）应定期检查、整理硬件物理连接线路，定期检查硬件运作状态（如设备指示灯、仪表），定期调阅硬件运作自检报告，从而及时了解硬件运作状态。

（三）禁止随意搬动设备、随意在设备上进行安装、拆卸硬件、或随意更改设备连线、禁止随意进行硬件复位。

（四）对会影响到全局的硬件设备的更改、调试等操作应预先发布通知，并且应有充分的时间、方案、人员准备，才能进行硬件设备的更改。

（五）不允许任何人在服务器、交换设备等核心设备上进行与工作范围无关的任何操作。未经上级允许，更不允许他人操作机房内部的设备，对于核心服务器和设备的调整配置，需经领导同意后才能进行。

（六）要注意和落实硬件设备的维护保养措施。

六、软件安全使用制度

（一）禁止在服务器上进行试验性质的软件调试，禁止在服务器随意安装软件。需要对服务器进行配置，必须在其它可进行试验的机器上调试通过并确认可行后，才能对服务器进行准确的配置。

（二）对会影响到全局的软件更改、调试等操作应先发布通知，并且应有充分的时间、方案、人员准备，才能进行软件配置的更改。

（三）不允许任何人员在服务器等核心设备上进行与工作范围无关的软件调试和操作。未经上级允许，不允许带领、指示他人进入机房、对网络及软件环境进行更改和操作。

七、机房资料、文档和数据安全制度

（一）禁止任何人员将机房内的资料、文档、数据、配置参数等信息擅自以任何形式提供给其它无关人员或向外随意传播。

（二）对于牵涉到网络安全、数据安全的重要信息、密码、资料、文档等等必须妥善存放。外来工作人员的确需要翻阅文档、资料或者查询相关数据的，应由机房相关负责人代为查阅，并只能向其提供与其当前工作内容相关的数据或资料。

八、机房财产登记和保护制度

（一）机房的日常物品、设备、消耗品等必须有清晰的数量、型号登记记录，对于公共使用的物品和重要设备，须建立一套较为完善的借取和归还制度进行管理。

（二）物品机房工作人员应有义务安全和小心使用机房的任何设备、仪器等，在使用完毕后，应将物品归还并存放于原处，不应随意摆放。

（三）对于使用过程中损坏、消耗、遗失的物品应汇报登记，并对责任人追究相关责任。

（四）未经主管领导同意，不允许向他人外借或提供机房设备和物品。

## “外来人员”访问管理制度

一、“外来人员”定义

“外来人员”——指除院内与网络系统相关的操作、管理和咨询人员以外的所有人员，包括院外的系统开发供应商、交流访问人员、咨询人员、病人及其家属、外单位人员以及医院内与“网络系统”无关的人员。

二、制度适用系统定义

本制度所适用的系统，为医院用于信息化管理的所有网络布线、网络设备、计算机设备、计算机外围设备、服务器、数据库以及在这些系统上运行的所有数据和程序。其中包括医院HIS系统、医院PACS系统等。

三、实体访问规定

本制度所指实体为医院中心机房、医院信息科以及医院内计算机设备专用场所或机柜，同时包括所有系统操作终端所在部门或机房。

“外来人员”在工作时间未经允许，不得进入这些场所；如需进入必须由院内相关人员全程陪同，不允许“外来人员”人员单独滞留于上述场所；“外来人员”人员在滞留期间未经允许不得查看、使用场所内任何设施或文档。在非工作时间原则上不允许“外来人员”人员进入，如确有需要则必须通知总值班，由相关人员全程陪同并记录在案。

四、有关逻辑访问的规定

外来人员人员原则上不允许操作、访问医院的信息系统，如确有需要则必须在工作人员的全程陪同下使用系统的最低权限用户（如guest）进入系统进行所允许的操作。如果无最低权限用户而使用了其他用户进入系统，在外来人员离开后必须立即更改密码。

外来人员在访问系统期间未经许可不允许使用任何方法（如拷贝磁盘、刻录光盘、打印数据、手工记录等）带走任何数据和程序。

五、有关系统开发供应商访问的规定

（一）在其所供产品实施期内的安全访问规定

在开发实施期间，开发商必须明确实施人员及其负责内容，规定所有人员的安全权限级别并上报医院信息科归档保存。在其所负责的信息系统中享有与信息科管理人员等同的权限以及对内部实施人员的权限划分。但只适用于其当前正在实施的系统。

（二）在其所供产品验收后服务期内的安全访问规定

在产品验收之后，开发商必须上交所有权限并指定相对固定的人员为服务人员，并且由医院信息科分配合适的权限。

（三）在其所供产品服务期之后的安全访问规定

过服务期后，开发商的访问等同于“外来人员”访问。

## 信息科监控制度

随着医院信息化进程的不断深入，医院各项业务越来越依赖于局域网及计算机系统，保护局域网及计算机系统的正常运转就是保护医院的正常运营，是系统管理员义不容辞的责任，为了加强医院机房的管理，确保信息系统的正常使用和安全运行，充分发挥其作用，特制定本制度。

1、系统监控对象

1.1 防范各种常见攻击

①防范利用漏洞（输入法漏洞、IIS漏洞、服务系统漏洞等）攻击。②防范特洛伊木马等计算机病毒的攻击。监控措施为是否及时为系统和应用程序打补丁，是否定期升级病毒定义库。

1.2 保证系统时时处在加固的状态

对系统的加固措施有：分区为NTFS，有足够的磁盘剩余空间，删除不必要的共享目录，定期更改用户密码且密码可靠，删除不必要的用户和服务，禁用GUEST帐户，设置帐户锁定策略，建立安全审核策略，安装杀毒程序，安装最新补丁等。

1.3 监控数据备份

为了保障数据的安全，应监控HIS数据备份策略实施情况，记录备份所用时间、备份文件大小。当备份时间过长或备份文件突然超长，应引起管理员注意，分析原因，采取必要措施。

1.4 监控系统性能

为了监测系统性能，及时发现性能问题，应建立系统性能基线。日常监控时，将系统实时性能曲线与同一时段的基线对照，及时发现问题，找出原因，采取适当优化措施。

2、注意防潮、控制恒温，经常检查各系统运行情况，保证系统设备处于良好工作状态；

3、信息科人员必须具有高度的工作责任心,认真负责完成好医院赋予的安全信息科任务, 及时掌握各种信息系统运行情况,对运行过程中发现的情况及时进行处理和上报；

5、信息科人员必须严格执行值班制度，按照规定时间上下班,不准随意离岗离位,个人需处理事务时, 应征得主管领导的同意方可离开；

6、信息科人员爱护和管理好信息科室的各项装配和设施,严格操作规程,确保信息科系统的正常运作；

7、密切注意信息科设备运行状况，保证信息科设备系统的正常运作，发现设备出现异常和故障要及时报修，并向设备管理人员或领导报告；

8、不得擅自改变信息系统设备，设施的位置和用途；

9、不得删改、破坏资料原始数据记录；

10、不得擅自复制、提供、传播信息。

11、严禁擅自开发、修改、升级、删除、安装影响信息科系统正常运行和安全的程序或软件；

12、务必保障通信联络畅通，不得用电话接、打私人电话；不得无故中断信息系统程序；

13、信息资料应妥善保存，未经允许，不得随意更改、删除原有资料。

## 网络运行监控、防病毒、防入侵管理措施

为了保护我院数据与网络的安全，保证网络的正常运行，促进网络更好的应用和发展，制定本制度。

1、利用防火墙将内部网络、Internet外部网络、安全监控与备份中心进行有效隔离，避免与外部网络直接通信。

2、利用防火墙建立网络各终端和服务器的安全保护措施，保证系统安全。

3、利用防火墙对来自外网的服务请求进行控制，使非法访问在到达主机前被拒绝。

4、利用防火墙使用IP与MAC地址绑定功能，加强终端用户的访问认证，同时在不影响用户正常访问的基础上将用户的访问权限控制在最低限度内。

5、利用防火墙全面监视对服务器的访问，及时发现和阻止非法操作。

6、对网络边界点的数据进行检测，防止黑客的入侵；

7、对服务器的数据流量进行检测，防止入侵者的蓄意破坏和篡改；

8、监视内部用户和系统的运行状况，查找非法用户和合法用户的越权操作；

9、对用户的非正常活动进行统计分析，发现入侵行为的规律；

10、实时对检测到的入侵行为进行报警、阻断，能够与防火墙/系统联动;

11、内外网物理隔离，在内网客户端上，禁止使用USB存储设备，阻止病毒通过U盘传播。

12、病毒库更新管理机制

（1）为提高医院信息安全管理水平，规范医院内部局域网终端管理流程，保证信息系统的通畅、高效、安全运行，我院购买杀毒软件并定时升级。

（2）信息科每周检查杀毒软件的病毒库，上传到院内网，供各科室自行更新，信息科工作人员在巡视时进行检查并人工更新。

## 医院信息系统运行维护评价和改进方案

一、总则

1．为了加强医院计算机网络系统的领导和运行维护管理，促进医院信息系统的应用和发展，保障系统有序运行，制定本方案。

2．本方案所称的计算机网络系统，是由计算机及其相关配套的设备、设施构成，按照系统应用目标和规则对医院信息进行采集、加工、存储、传输、检索等处理的人机系统。

3．医院计算机网络系统运行维护管理是为了保障系统建设和应用，保障系统功能的正常发挥，保障运行环境和信息的安全，满足各工作站操作和维护的全部活动的正常进行。

4．本方案适用于医院信息系统运行维护管理科室。

二、组织运行维护管理

1、成立信息系统质量运行维护管理组织：

组 长：院长

副组长：副院长

成 员：信息科主任、职能科室负责人、各科室主任

2、质量运行维护管理组织职能和任务：

（1）制定医院信息系统建设和应用总体规划及阶段实施计划，审查和制定系统应用中工作流程、技术规范、性能指标、有关人员职责和规章制度。

（2）协调解决工程实施和系统应用中的质量问题。

（3）组织安排系统建设和应用中的重要活动，如规则制定，网络运行维护管理、系统配置，人员培训等。

（4）对医院信息科存在的问题或缺陷提出整改意见并敦促实施。

三、信息系统运行维护

（一）网络的技术运行维护管理

1．计算机工程技术人员是网络系统技术运行维护管理的直接责任者，应以实现系统功能为目的，以满足用户需求为宗旨，对网络系统的操作和维护进行运行维护管理。

2．网络设备的配置，由系统负责人提出配置规划和计划，报有关领导审批后实施。

3．每一子系统或挂接的可执行程序在上网运行前，计算机工程技术人员必须严格按照功能要求在备用服务器上进行全面调试，达到功能要求且排除一切可能的数据冲突后交用户实际使用。

4．网络系统负责人负责各工作站模块登录口令密码的设置并做好记录。工作站操作人员更换时，要立即做好口令的更改。

5．出现技术问题或故障时，应遵循《网络服务器故障应急处理规程》处理。

（二）网络系统安全运行维护管理

1．网络系统的安全运行维护管理包括：数据库安全运行维护管理和网络设备设施安全运行维护管理。

2．系统负责人和计算机工程技术人员必须采取有效的方法和技术，防止网络系统数据或信息的丢失、破坏或失密。

3．利用用户运行维护管理模块或其他技术手段对系统用户访问权限进行运行维护管理，用户的访问权限由系统负责人提出，领导小组核准。

4．系统运行维护管理人员应熟悉并严格监督数据库使用权限、用户密码使用情况，定期更换用户口令密码。

5．计算机工程技术人员要主动对网络系统实行查询、监控，及时对故障进行有效的隔离、排除和恢复，对数据库及时进行维护和运行维护管理。

6．所有进入网络使用的软盘，必须经过网络中心负责人同意和检毒，未经检毒杀毒的软盘，绝对禁止上网使用。

7．网络系统所有设备的配置、安装、调试必须由计算机工程技术人员负责，其他人员不得随意拆卸和移动。所有操作人员必须严格遵守计算机以及其他相关设备的操作规程，禁止其他人员进行与系统操作无关的工作。

8．保持机房的清洁卫生，并做好防尘、防火、防水、防静电、防高压磁场、防低磁辐射等安全工作。

9．计算机工程技术人员有权监督和制止一切违反安全运行维护管理及破坏网路设备的行为。

（三）工作站运行维护管理

1．各工作站所有使用人员必须严格遵守操作规程以及有关的计算机运行维护管理制度。

2．严格按照计算机操作使用规程进行操作。操作中必须做到精力集中，细致认真、一丝不苟、快速准确，及时完成各项数据录入．

3．经常保持各种网络设备、设施整洁干净，认真做好网络设备的日清月检，使网络设备始终处于良好的工作状态。

4．加强设备定位定人运行维护管理，未经计算机工程技术人员允许，不得随意挪动、拆卸和外借所有网络设备、设施。

5．机房内严禁存放易燃、易爆、易腐蚀及强磁性物品；遇有临时停电及雷电天气，应采取保安措施，避免发生意外．

6．机房内不准吸烟、进食、会客、大声喧哗；严禁无关人员上机操作或进行其他影响网络正常运行的工作。

7．严格交接班制度，工作中遇到的问题要及时报告。

四、医院信息系统的效益评价

1. 经济效益评价：在医院物资运行维护管理中应用计算机信息系统，将能够减少资金占用，保证供应，取得较直接的经济效益。

2.财务管理评价：医院信息系统用于医疗收费和财务数据处理等工作，可以大大提高医院经济运行维护管理的效率和活力。

3.医院管理评价：医院信息系统可以为医院运行维护管理人员提供运行维护管理和决策信息，为决策者及时调整各种人员和物资的安排提供了可靠的依据。

4.社会效益评价：在医疗中应用信息系统可以使医院和社会两方面取得明显的效益。医疗中需要及时准确地得到各种病人检查结果，以使医师能及时进行治疗，信息系统的应用能大大提高病情及诊疗结果传递效率，减少病人的平均住院日。病人平均住院日的减少意味着医院可以收治更多的病人，医院的设施得到充分使用，收到更好的经济效益。有更多的病人更快康复，回到各自的工作岗位上去，其效益是很难用金钱来估计的。

5.人力资源评价：医院信息系统在加速培养高水平医务人员上能起到非常大的作用。医疗中应用计算机系统后，各种检查结果、病人病案记录等资料，都能及时提供给医师，使医师能及时、全面了解病人病情，并能对资料进行对照比较分析。这有利于培养医师的临床工作经验和培养高水平医师。

五、实施全程信息系统质量运行维护管理与持续改进

1、严格执行技术操作规范、常规和标准，加强基础信息系统质量、环节信息系统质量和终末信息系统质量运行维护管理；认真执行信息系统质量和信息系统安全的核心制度；切实落实和系统安全责任制、信息系统安全等级制度、信息使用与运行维护管理部门协调机制、值班交接班制度、医院信息资源共享制度、信息系统基本功能规范、电子病历书写基本规范与运行维护管理制度等，在全程信息系统质量运行维护管理中及时发现信息系统质量和信息系统安全隐患并进行动态监控。

2、特别警惕“三个重点”的信息系统安全防范，重点部门、重要岗位如门诊收费处、药房等；重点（关键）环节如药库运行维护管理、病人信息运行维护管理、权限操作等；重要岗位如机房值班、系统维护医院要采取督导检查、落实制度等多种方式保障重点部门、重点环节和重点岗位信息系统质量安全。

3、重点做好三大重点工作（①建立新的信息系统质量考核体系，②合理检查，③合理分配。）抓好四个重要环节（①进一步提高信息质量，②进一步提高运维质量，③进一步提人员技术质量，④进一步提高安全质量。）加强四个层次运行维护管理（①抓好信息科人员的规范化培训和运行维护管理，②加强使用操作运行维护管理、④充分运行维护管理小组发挥的作用）。

4、严格审核与新开展的信息系统技术或项目相适应的技术力量、设备与设施，实施确保信息安全的方案，并建立相应的运行维护管理制度，对新开展的信息系统技术的安全、质量、效过、费用等情况进行全程追踪运行维护管理和评价。

5、通过检查、反馈、评价、整改等措施，持续改进信息系统质量。

## 技术文档管理制度

一、系统信息保护制度

（一）支持系统运行的操作系统信息

内容：操作系统的版本号、授权证书、原始安装介质（光盘和软盘）、序列号、安装手册、使用说明书、参考手册、升级包（光盘或软盘介质）、安装和升级记录（书面），其他有关附件；

（二）开发应用系统的工具软件信息

内容：工具软件的版本号、授权证书、原始安装介质（光盘和软盘）、序列号、安装手册、使用说明书、参考手册、安装和设置（指应用软件常用基本模块、基本属性，书面），其他有关附件；

（三）应用系统网络配置信息

指支持应用系统运行的网络协议介质（光盘或软盘，棣属于何系统等）、内容（通讯协议、文件传输协议等）、网络配置（如方式、数量、书面），其他有关附件；

（四）应用系统的病毒防护信息

指安装在应用系统运行环境下的防杀病毒的专用软件（杀毒软件、病毒防火墙软件）的版本号、原始安装介质（光盘和软盘）、序列号、安装手册、使用说明书、安装和升级记录（书面），其他有关附件；

二、系统开发和维护管理制度

应用系统的开发，一般应按软件工程的规范化要求进行，在应用系统开发及投入使用前应作用户需求分析、概要设计、详细设计并进行独立测试，建立相应的需求分析文档、概要设计文档、详细设计文档及独立测试文档。这些文档贯穿于整个开发过程，在开发过程中不断修改、补充、完善，是应用系统技术文档的基础，是日后应用系统正常工作、维护的依据，对应用系统运行的正确和稳定、数据处理、保存的安全性等均有决定意义，也是技术安全文档管理的主要对象。

建立系统开发和维护挂历制度即对应用系统在开发、调试、完善过程中的应用信息的完整性、安全性进行监控，保障应用系统投入运行后有良好的安全机制。

三、用户数据保护制度

应用系统环境数据文件、用户信息文件、运行的结果数据文件构成用户数据文件，是应用系统的支持文件，也是应用系统的运行结果和存储形式。

建立和完善用户数据保护制度，切实作好数据保护工作，是技术安全文档管理的重要内容。

四、技术文档管理机制

系统信息保护、系统开发和维护管理、用户数据保护需要相应的技术安全文档管理机制作保证。

（一）保管制度

建立专人保管制度，使每项内容都有案可稽、查有实处；落实保管设施，配备必需的、可靠的设备，以保障各类技术文档的安全和完整，这是技术安全文档管理的基础。

（二）记录制度

指做好应用系统的使用记录和各类技术文档的更改记录，使每次、每个环节的变动都有记录，可回溯，便于分析可能产生的故障原因或进行技术更新、升级。

（三）维护制度

应用系统的删除、重装，防杀病毒记录，系统清理、数据迁移记录需及时记录在册，保证应用系统始终运行于安全环境下，并要求保证用户数据文件记录的完整性和备份的完整性。

（四）检查制度

定期检查以上各项制度，检查各类技术文档的管理是否依制度而规范，同时也可把检查点作为应用系统的运行节点，使操作人员对医院应用信息系统的运行状况有清晰的了解和把握，即设立运行节点，保留节点信息，使系统有还原点。以后遇因突发故障可依据技术文档（含数据、有介质保存）保留的节点信息予以恢复，缩短故障排除时间和恢复时间，减小经济损失。

## 信息科联席会议制度

一、联席会议的组建

1、组建信息化联席会议是为了协调好各科室之间的工作，提供交流平台，使信息畅通，对医院运行状况共同协商、共同决策。

2、会议组建

信息化联席会议由分管信息化的院领导专门负责，由信息科牵头组织召开。

负责人：张茂桐

成 员：信息科全体成员、临床科室及门诊、供应室、医技科室护士长。

3、联席会议的主要职责

（1）在信息系统的使用管理制度下，保障各科室各正常使用，为患者提供优质的服务。

（2）研究讨论信息系统运行中各个环节的弊端，结合实际工作，对存在问题定期分析、反馈，研究持续改进措施。提供更加优质的环境。

（4）加强各部门之间的沟通和协调，保持信息通报渠道畅通，定期通报系统使用状况。

4、联席会议的工作规则

（1）原则上联席会议每半年召开一次全体会议，由信息科负责召集，联席会议成员参加，必要时可邀请有关部门（医院感染管理科、医务科、护理部）负责人参加。

（2）联席会议召开的时间、地点和议题由信息科拟定并请示负责人后通知各成员。

（3）信息科负责日常联络工作，并抓好落实联席会议作出的工作部署和决定。

（4）各联席会议成员必须按时参加联席会议，如因故不能参加应提前向负责人请假，并指定本科室副护士长（或主管护师以上人员）代替参加会议。

5、会议内容

（1）通报：各成员提出问题的落实情况，各成员提出质量安全问题的持续改进情况等内容。

（2）议题：需要医院或其他各委员会、其他部门协助或支持的项目工作，在会前由信息科拟定，在会议上宣布，征求医院或其他委员会、其他部门的意见，布置、协调相关工作。

（3）总结：信息科工作情况、质量持续改进情况。

（4）互动平台：针对医院信息科工作中的重大、重点、难点问题专题讨论，商议解决方案；各成员提出的关于医院信息化工作存在问题及改进意见及建议，共同协商、改进。

## 信息科值班、交接班制度

一、值班制度：

1 、值班人员务必做好防火、防盗、防雷、防潮、防高温等工作，发现异常及时向主管领导汇报或报警。

2、值班人员必须认真监测网络服务器、空调等设备运行情况，做好值班记录和交接班工作。

3、值班人员必须及时解决网络问题，遇到网络故障，马上组织力量排除，并及时报告主管领导，如不能及时排除，须向用户解释说明。

4、值班人员未经主管人员批准，不得擅自更改网络配置及其网站信息。

5、整理内务，保持机房整洁卫生。

二、交接班制度：

1、值班人员和接班人员要按时到岗，仔细查阅值班日志和检修记录，了解设备运行情况。

2、了解上级有关任务变动的通知。

3、清点机房所有设备、仪器、仪表、工具、资料等办公用品及卫生情况。

4、在交接班中若发生设备故障、信号传输故障，由交接班人员负责处理，接班人员协助处理完后再交接班。

5、交接班要严肃认真，详细交接，发生漏交、错交均由交班人员负责，接班人员疏忽未能发现的问题，由接班人员负责，交接不清的由接班人员负责，交接由双方认为交接完毕后签字方可下班，早晚班应记录好各项日志及留言，签字方可下班。

## 信息科人员管理

### 信息科人员录用制度

一、为实现信息系统安全稳定运行，对信息科技术人员的录用、考核做出以下管理制度。

二、确定用人单位岗位编制的原则：

1、符合医院及本科室长远发展规划、经营战备目标的需要；

2、符合目前或近期业务的需要；

3、有助于提高工作效率和促进业务开展，避免人浮于事；

4、能适应用人单位领导的管理能力和管理幅度。

三、聘用人员均首先要求具有良好的品德和个人修养，在此基础上选择具有优秀管理能力和专业技术才能的人员。各岗位人员要力争符合德才兼备的标准。有下列情况之一或多条者，不得成为我单位员工：

1、剥夺政治权力尚未恢复，被判刑或被通缉，尚未结案；

2、参加非法组织；

3、品行恶劣，吸食毒品；

4、拖欠公款，有记录在案；

5、经医院体检，本单位认为不合格；

6、年龄未满18周岁。

四、新录用人员，到政工科报到，并填写新进人员审批单，由信息科安排具体工作，政工科同时向财务科报送新进人员名单。

### 信息科培训制度

一、培训制度

1、业务学习培训计划由信息科根据年度工作计划作出安排。

2、成立业务学习小组，定期组织业务学习；

3、工作人员每年必须参加不少于20个课时的专业培训。

4、工作人员必须完成布置的学习计划安排，积极主动地参加信息部组织的业务学习活动。

5、有选择地参加其它行业和部门举办的专业培训，鼓励参加其它业务交流和学习培训。

6、支持、鼓励工作人员结合业务工作自学。

二、培训内容：

1、计算机安全法律教育定期组织本单位工作人员认真学习《网络安全制度》、《计算机信息网络安全保护》等业务知识，不断提高工作人员的理论水平，提高操作员的防范能力。

2、计算机职业道德教育

（1）、工作人员要严格遵守工作规程和工作制度。

（2）、不得制造，发布虚假信息，向非业务人员提供有关数据资料。

（3）、不得利用计算机信息系统的漏洞偷窃客户资料。

（4）、不得制造和传播计算机病毒。

3、计算机技术教育

（1）、操作员必须在指定计算机或指定终端上进行操作。

（2）、机房管理员，程序维护员，操作员必须实行岗位分离，不得串岗，越岗。

（3）、不得越权运行程序，不得查阅无关参数。

（4）、发现操作异常，应立即向机房管理员报告。

三、培训方法：

1、结合专业实际情况，指派有关人员参加学习。

2、有计划有针对性，指派人员参加相关学术会议。

3、每月举办一次科内学术交流，互相学习取长补短。

4、所有上岗工作人员或换岗工作人员应经过培训上岗。

5、自订学习计划，参加专业函授学习成绩及时反馈有关部门，良好学业者给予奖励。

### 授权审批及人员离岗制度

授权审批及人员离岗制度信息系统作为资源管理系统，必须有其安全性和职责权限，特制定本管理制度。

1、登录我院信息系统需要有用户帐号，相当于身份标识，新用户由政工科根据其取得的相应的资格证书通知信息科直接办理帐号，刚取得相应资格证的工作人员帐号由该工作人员提出书面申请，由本部门负责人员签字后交信息科办理后统一分发至相应职能部门，由相应职能部门根据工种性质进行科室调配。

2、各部门主管领导负责本科室相关系统模块的权限，管理和该模块的数据安全。

3、各部门人员以书面形式向本科室主任或护士长提出权限申请，由各部门主管领导进行审批设置；

4、信息系统用户因离岗或转岗，所拥有的系统用户权限需相应变更时，需在将有本部门权限负责人签字确认提交到信息科；信息科对离岗或转岗的帐号进行注销并签字；政工科方可办理离岗或转岗手续。

5、帐号的注册所有者应对该帐号在系统中所做的操作结果负全部责任。用户申请\变更\注销流程1用户新增\变更流程：

（1）由用户本人提出申请；

（2）申请人所属部门权限负责人核准；

（3）信息科根据书面申请增加用户帐号并分发至主管职能部门，由主管职能部门再依次分配至各科室，权限由该科主任进行授予。

（4） 申请人应在收到通知的当天修改初始口令。

6、用户注销流程：当用户由于工作变动、调动或离职等原因需要对用户的访问权限进行修改或注销时：

（1）用户提出书面申请，经部门权限负责人签批后，到政工科签批；

（2）信息可科根据接到两部门签批申请单后对该用户信息进行注销，并出具注销确认证明；

（3）政工科收到信息科注销确认证明后方可为该用户办理离岗或转岗的手续。

### 信息科人员考核制度

根据医院科室考核意见，对科室人员制定本考核办法，以完成医院对我科制定的服务考核项目。

1、认真遵守医院及科室内的各项规章制度，如有一次违反扣x分，依次加倍。

2、严格遵守劳动纪律，不迟到、不早退，如有一次无故迟到或早退现象依据情节扣除x分，依次加倍。

3、工作态度认真，按时完成上级交给的各项工作任务，如有一次无故未按时完成，影响工作进度扣x分，依次加倍。

4、牢固树立为临床一线服务的思想，服务及时到位。如出现一次无故不到位（院内科室投诉），经查属实，扣x分，影响医疗工作，造成严重后果的扣除当月x分值。

5、值主班人员负责接听电话和处理问题，安排值白班人员到现场处理，做好终端反馈故障登记、处理表的登记工作，每班，进行交接班制度，对物品（备用机数量、待完成工作、维修工具数量等）进行交接；借出物品要填写信息科物品借出登记（包括备用机去向）；当日有接收和安装的设备，要填写科室个人办公电脑、打印机登记表，以上如有漏项和填写不全者，每项扣质量分x分。

6、接听服务电话，以值主班人员为主，需要下科室调试和维修的，主班人员有权安排其他人员下科室服务，电话无人接听x分钟，扣质量分x分,依次加倍。

7、值白班人员要服从值主班人员的安排，无故不服从安排的，一次扣质量分x分。白班人员下科室维修硬件设备的，要填写硬件维护表，值白付班的还要负责当日的室内卫生，检查卫生不合格扣质量分x分，依次加倍。

8、维修设备时，维修人员必须协助科室填写计算机及其外围设备维修申请单，项目要求填写齐全，维修费用以此单作为扣除费用凭据。因填写项目不全，引起纠纷，所发生的费用由填写维修单的维修人员负担。

9、机房管理员负责服务器端配置登记表、机房日常故障登记表、机房运行日志、硬件特殊维护表的填写，发生一次未填写记录或填写项目不全者扣质量分x分，室内检查有灰尘，一次扣质量分x分。

10、设备使用状态表由××负责整理，设备使用状态每月登记一次，分片负责维护，维护记录少一次，扣5分，设备维护少一台，扣1分。

11、按包片区人员进行下科室巡回服务，填写信息科下科室检查登记，每周1-次，服务后的内容由科主任或护士长签名确认。

12、加班一次（2小时1分）加1分，值主班除外。

## 医院信息来源追溯管理制度

为保证医院医疗质量与安全管理相关工作均可追溯，在需要时，能够第一时间回复事件原貌或者追究责任人，特别是保证医院相关信息的收集做到“及时、客观有据、真实准确”，特制定本制度。

一、在日常工作中，医院信息收集责任人员应当遵循“及时、客观有据、真实准确”的原则，特别是涉及政策及法律的相关数据。不得选择性收集、谎报、瞒报。

二、医院信息的可追溯性，就是对医院信息数据及来源、收集人、责任人、审批人等相关信息进行规范的原始记录和存档。

三、医院信息可追溯的实现方式：

1、制订规范的管理流程，设计合理的记录要求及格式，并将可追溯作为制度、流程设计是否科学合理的重要指标；

2、具体执行中，据实记录参与者、工作过程，保留执行过程中产生的全部资料，对流程规范中没有的过程，应双人核对后再誊写到规范的记录或表格中，相关责任人必须签字以示负责。对某项工作中反复使用的非正式记录方式，应考虑适当规范，并纳入保存范围；

3、每个汇总环节均应进行核实，并保留上一节点的原始资料。

4、信息再编辑及加工，应保留原始凭据，并有保证其与原始记录内涵一致的操作、审核流程。

四、上级主管部门、医院信息科主管领导，应定期不定期检查信息收集与上报是否及时、规范和可溯源。发现问题，及时要求整改。

# 第六章 信息科业务工作规程与流程

## 一、信息科科长工作规程与流程：

（一）组织协调好全科各项工作。

（二）组织落实制定医院信息化年度工作计划，并组织对计划落实情况的检查。

（三）组织落实计算机设备、网络的使用和维护,对硬件故障、设备报废情况报告，提出处理意见报院长；组织落实全院信息系统的论证、调研、系统分析、开发及应用软件的使用与维护。

（四）组织落实全院网络和综合数据的安全管理，遵守各项保密制度。

（五）完成上级交办的各项任务。

## 二、综合管理岗位工作规程与流程：

（一）协助部门领导，起草全院信息化年度工作计划，并实施对计划情况的检查。

（二）协助部门领导，制定医院信息化工作的有关管理制度及考核办法，并负责组织实施。

（三）组织落实信息化技术培训计划。

（四）按照上级规定及要求，完成信息化相关文档资料的归档整理以及有关资料的统计上报。

（五）经领导同意，负责对外交换数据并对数据进行处理，做好登记工作。

（六）计算机设备、耗材的购置要严格按照政府采购办法、医院相关管理规定，按照各部门的需求，结合工作实际进行论证后，拟订设备购置计划报告报院长。

（七）要建立设备档案，同时与院固定资产管理部门核对。内容包括型号、设备配置、设备来源、安装地点及变动情况、启用时间、使用科室（人员）、设备故障情况及检修记录等。遇到设备变更，应及时登记变更。

（八）负责注册用户、设置口令、授予权限，并适时加以修改，以便增强系统的保密程度。

（九）负责本部门各类文件收发、运转和档案资料管理，并及时归档。

（十）协助部门领导做好本院各项信息化工作的日常监督，办理行政、对外交流和思想政治工作以及内部行政事务工作。

（十一）遵守各项保密制度，做好安全保密工作。

## 三、网络系统管理岗位工作规程与流程：

（一）协助部门领导起草网络建设年度工作计划，并实施对计划情况的检查。

（二）网络建设必须采取防火、防水、防雷击、防电磁干扰、防盗等防护措施，确保全院的通信设备及网络设备的安全与畅通。

（三）网络的日常管理和维护：

１、每日检查计算机网络的运行情况，确保线路畅通、网络设备安全稳定运行，做好运行日志。

２、运用防、杀病毒软件、防火墙对网络实行实时防护，一旦发现病毒或“黑客”侵入立即向主任汇报并迅速组织清除。

３、定期检查内网计算机是否与互联网实行物理隔断。

（四）负责落实各项网络安全管理制度和用户管理，做好客户端操作系统权限控制、应用系统操作权限分级控制、数据库操作权限分级控制。

（五）做好网络运行状态监督与数据库数据备份工作；对计算机网络操作系统和大型数据库系统的运行情况每工作日进行检查，有异常的立即向主任汇报并迅速组织排障。

（六）负责网络管理资料的整理和归档。

（七）遵守各项保密制度，做好安全保密工作。

（八）完成部门领导交办的其他工作。

## 四、硬件设备管理岗位工作规程与流程：

（一）计算机设备的维护和保养

1、对计算机设备操作人员的维护、保养情况进行检查，检查的主要内容是机器清洁、防尘情况；是不是有随意拆装、调试情形；有无对硬件进行技术改动等。检查每季进行一次，同时结合日常抽检，检查时做好记录。

2、接到设备异常情况报告单后，要查清故障原因，并记录故障信息；分别情况给予维修，每次维修工作完成后，在设备档案中要做详细的维修记录。

3、确实无法自行修复的，持各科室报送的设备维修单交主任签字后将报修设备送计算机维修医院维修。

4、如遇特殊情况，须经技术论证后，书面报主任批准后实施。

5、对所辖范围内计算机运行所发生的各类事故应当日查明情况，以书面形式报主任。

（二）每日检查计算机机房和UPS等的运行情况，做好运行日志。

（三）协助专业人员做好机房内各类应用服务器操作系统的安装、集成工作，并做好记录。

（四）每日检查各服务器操作系统的运行情况，确保各服务器安全稳定运行，做好运行日志。如遇系统运行中出现异常情况应立即报告部门领导，并组织排查。

（五）积极普及和宣传计算机基础知识并负责指导有关科室及部门开展计算机使用工作。

（六）负责计算机等硬件设备管理的资料整理和归档。

（七）遵守各项保密制度，做好安全保密工作。

## 五、应用系统管理岗位工作规程与流程：

（一）日常管理

1、在全院范围内积极普及和宣传计算机管理知识并负责指导有关科室及部门开展计算机应用系统管理工作。

2、维护好各系统软件，掌握好系统软件和测试软件的使用，

3、每日检查应用系统的运行情况，确保各应用系统安全稳定运行，做好运行日志。

4、如遇系统运行中出现异常情况应立即报告部门领导，并组织排查。

（二）对各科室提出的软件需求修改申请时

1、经调研、分析后应在工作日24小时内填写维护申请单报部门领导审核，并做好记录。

2、收到软件更新通知后，在测试环境下全面测试，测试无误后报主任审核。

（三）及时通知各科更新各工作站端程序，并随时检查程序更新情况。

（四）根据上级主管部门标准化管理规定，对应用系统的技术标准、数据标准、应用标准及规范性制度加以实施。

（五）负责医院网站的软件开发、应用培训、安全管理。

（六）负责组织医院应用软件使用的专业培训。配合部门制定培训计划。

（七）对于各科室使用的其它应用系统，根据有关操作说明，协助其正确安装，并尽力解决程序运行中出现的问题。

（八）负责应用系统管理资料的整理和归档。

（九）遵守各项保密制度，做好安全保密工作。

## 六 医院信息来源可追溯程序

1.目的

本文件规定了对医院信息的可追溯性的内容和要求，目的是确保每个医院信息的唯一标准并加以记录，在有追溯要求的场合可以准确得到医院信息的收集、记录等资料，以利于采取纠正和预防措施。

2适用范围

本文件适用于对医院信息可追溯性的控制管理。

3.职责

3.1信息科是医院信息可追溯性的归口管理部门。

3.2各职能部门、科室负责保持原信息的记录，建立适宜的信息档案。

3.3各职能部门负责医院信息在使用中质量信息的反馈和记录。

3.4信息科负责对采购信息进行验证并记录，负责医院信息发出编号的编制和标识。

4.工作程序

4.1信息科对惧的医院信息进行检验或验证，对医院信息进行检验或试验，并作好记录。

4.2各职能部门、各科室应根据医院信息应分类要求进行分类保存存，对应类别区进行唯一标识。

4.3医院信息发出编号作为医院信息唯一性标识。

4.4信息收集人员进行信息收集时应记录部门名称或科室名称、信息编号、信息类别、联系电话等，应做到信息记录来源标识唯一性。

4.5医院信息发出的信息，应记录医院信息的发出编号、用户名称、地址、联系电话等，应做到信息发出的唯一性。

5.相关记录

5.1 医院信息收集记录表

5.2医院信息检验或验证记录

5.3医院信息发出记录表

5.4医院信息汇总记录表

5.5医院信息分析记录

5.6 医院信息存在问题与缺陷记录

5.7医院信息存在问题与缺陷改进与评价

# 第七章 信息系统故障处理应急预案

## 一、总则

（一）目的

为有效防范医院信息系统运行过程中产生的风险，预防和减少突发事件造成的危害和损失，建立和健全医院计算机信息系统突发事件应急机制，提高计算机技术和医院业务应急处理和保障能力，确保患者在特殊情况下能够得到及时、有效地治疗，确保计算机信息系统安全、持续、稳健运行。

（二）编写依据

根据《国家网络与信息安全应急预案》及国家信息安全相关要求和有关信息系统管理的法律、法规、规章，并结合医院的实际，编制本预案。

（三）工作原则

统一领导、分级负责、严密组织、协同作战、快速反应、保障有力

（四）适用范围

适用于医院计算机网络及各类应用系统故障应急处理

## 二、组织机构和职责

根据医院应急管理的总体要求，由医院信息化领导小组（简称领导小组）负责领导、组织和协调全院计算机信息系统突发事件的应急保障工作。

1．应急处理领导小组

组 长：

副组长：

成 员：信息科、总务科、院办、医务科、护理部、门诊办公室、保卫科等部门主要负责人组成。

2．“应急预案”实施责任制

　　⑴建立以分管院长为第一责任人、职能部门和各相关部门负责人参加的信息系统安全运行领导小组；

　　⑵领导小组负责全院突发事件的“应急预案”实施和全院信息系统日常安全运行管理的组织协调及决策工作；

　　(3)信息科负责应急恢复信息系统运行的技术保障；

　　(4)总务科负责应急恢复信息系统供电保障；

(5)各行政和业务职能部门负责维持正常的医疗秩序，并根据“应急预案”实施相应的应急措施。

## 三、医院信息[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)出现故障报告程序

1、当各工作站发现计算机访问数据库速度迟缓、不能进入相应程序、不能保存数据、不能访问网络、应用程序非连续性工作时，要立即向信息科报告。信息科电话：内线号码：82024；外线号码：0538-6232024。

2、信息科工作人员对各科室工作站提出的问题必须高度重视，接到故障报告后，应立即展开调查，若断定是网络存在问题时，应安排专人打电话通知相关科室关机，并对来电询问科室做好解释工作，同时报告信息科长。

3、情况核实后，信息科及时给各工作站反馈故障信息，同时召集有关人员及时进行讨论，如果故障原因明确，可以立刻恢复的，应尽快采取措施恢复系统工作；如故障原因不明、情况严重、不能在短期内排除的，应立即报告院领导。在网络不能运转的情况下由院领导协调全院各部门工作，以保障全院医疗工作的正常运转。

## 四、医院信息[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)故障分级及处理原则

1、根据故障发生的原因和性质不同分为三类：

（1）一类故障：由于服务器不能正常工作、光纤损坏、主服务器数据丢失、备份硬盘损坏、服务器工作不稳定、局部网络不通、价表目录被人删除或修改、重点终端故障、规律性的整体、局部软件和硬件发生故障等造成的全院性计算机网络瘫痪。

（2）二类故障：由于单一终端软、硬件故障，单一病人信息丢失、偶然性的数据处理错误、某些科室违反工作流程引起局部[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)故障。

（3）三类故障：由于各终端操作不熟练或使用不当造成的错误。

2、故障分类等级的处理原则：

（1）一类故障：由信息科科长上报院领导，由医院组织协调恢复工作。

（2）二类故障：由网络[管理](http://www.gongwen123.com/Article/zongjie/nianzhong/index.htm)人员上报信息科科长，由信息科集中解决，并做好相关记录。

3、三类故障：由网络[管理](http://www.gongwen123.com/Article/zongjie/nianzhong/index.htm)员单独解决，并详细登记维护情况。

## 五、发生网络整体故障时的应急协调

1、当信息科一旦确定为网络整体故障时，首先是立刻报告院领导，同时积极组织恢复工作，并充分考虑到特殊情况对故障恢复带来的时间影响。各部门根据故障恢复时间的程度将转入手工操作,详见（六），具体时限明确如下：

30分钟内不能恢复——门诊挂号、住院登记、药房等部门转入手工操作。

6小时内不能恢复——各护士工作站、药房、急救中心、手术室、医技检查转入手工操作（具体时间由信息科通知）。

24小时以上不能恢复——全院各种业务转入手工操作。

2、各部门的具体协调安排：

（1）所有手工操作的统一启动时间，须由信息科工作人员判断所需修复时间，报告院领导同意后通知相关部门，各科室应严格按照通知的时间协调各项工作，在未接到新的通知前不准私自操作计算机。

（2）门、急诊工作由门诊办主任负责联系协调。网络恢复后，门、急诊工作人员要及时将中断期间的患者信息输入到计算机。

（3）门、急诊收费处工作由财务科长负责总体联络协调，要与信息科保持联系，及时反馈沟通最新[消息](http://www.gongwen123.com/Article/zongjie/jihua/index.htm)；当网络[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)运行中断超过30分钟时，要通知收款员转入手工收费程序；

①门诊收款员要建立手工发票使用登记本，对发票使用情况做详细登记；

②当[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)恢复正常时，由收款员负责对网络运行稳定性进行监测，如不稳定，及时向信息科反馈情况；

③在接到信息科发出可使用计算机的通知时，应重新启动运行后，收款员逐步转入机器操作。

（4）住院处的工作由财务科长总体负责联络协调；

①当[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)停止运行超过24小时，对普通出院患者，推迟出院结算时间。对急诊出院的患者应根据病历和临床护士工作记录，进行手工核算，出具手写发票。

②在网络停止运行期间，出院患者急需结算时，应由该科护士追查是否还有正在进行的检查项目，并向出院结算处提供详细费用情况后，方可送交结算。

③在网络停止运行期间，入院患者急需输入院手续时，实行手工输入院手续。系统恢复时补录病人所有资料。

（5）护士工作站由护理部主任负责总体联络协调：

①网络故障期间医护人员应手工详细记录患者的所有医嘱、护理记录和费用执行情况；详细填写每位患者的药品请领单（包括姓名、住院号、费别、药品名称及用量），一式两份，一份用于科室补录医嘱，另一份送药房作为领药凭证。

②接到信息科通知恢复网络运行时，按要求补录医嘱、护理记录和在本科发生的费用执行情况。

（6）医生工作站由医务科长负责总体联络协调：

①网络故障期间临床科室应手工详细记录患者的所有医嘱、病历记录，并详细记录治疗执行情况、病情进展情况。

②接到信息科通知恢复网络运行时，按要求补录各种记录。

（7）医技检查工作站由医务科长负责总体联络协调：

①在网络停运期间应详细留取、整理检查[申请](http://www.gongwen123.com/Article/dtgz/zhuanzheng/index.htm)单底联；

②网络恢复后根据检查单底联登记，通过手工补录患者在本科发生的费用（注意与临床科室联系沟通）。

③对即将出院或有出院倾向的患者，主治医师要在检查[申请](http://www.gongwen123.com/Article/dtgz/zhuanzheng/index.htm)单上要注明，检查科室应及时通知科室或住院处，及时沟通费用情况。

（8）药房工作由医务科长负责总体联络协调：

①严格按照信息科通知的时间及要求进行操作；

②网络故障时，根据临床科室提供的药品请领单发药；

③网络恢复时对临床科补录的摆药医嘱进行确认，同时与发药时药品请领单内容详细核对，如发现内容不符，须详细追查；

④网络恢复后对出院带药处方及时进行确认。

## 六、应急数据恢复工作规定

1、各工作站接到信息科发出的重新运行通知时，需重新启动计算机；整体网络故障的工程恢复工作，由信息科严格按照服务器数据[管理](http://www.gongwen123.com/Article/zongjie/nianzhong/index.htm)要求进行恢复工作；由网络[管理](http://www.gongwen123.com/Article/zongjie/nianzhong/index.htm)员按《数据备份恢复方案》进行[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)恢复。

2、由信息科科长指定专人负责恢复，当人员变动时应有交接手续。

3、当光纤损坏时应立即使用备用光纤进行恢复；交换机出现故障时，应使用备用交换机。

4、对每次的恢复细节应做好详细记录。

## 七、故障处理程序

1、网络故障应急处理程序

①信息科接到科室操作人员的故障信息后，应立即展开调查，先通过自己工作站试验是否存在相同情况，或查证是否有数据库锁表情况、查证是否数据服务器空间已满。当软件情况都被排除以后，进入机房看交换机指示灯是否全部不再闪动，或闪动很慢，若是则基本上可以断定是网络存在问题，这时安排一个人专门打电话通知相关科室关机及对科室来电做解释工作。

②采用排除法确定故障位置：先将与交换机相连的双绞线逐一拔出，同时观察交换机指示灯是否闪动正常，逐一拔出除服务器的所有连接终端，若仍不能解决问题，则逐一拔出内部的光纤接口，一般到此完全可以排除是由哪条线影响到网络速度，先隔离开这条网线让其他用户先使用网络。

③发现是由某一光纤影响，信息科人员应到该交换机处采用同样排除法逐个拔双绞线，直到找出是由哪条线路、哪个终端工作站影响到整个网络。

④通过这种方法，一般可以在最短的时间内找到各种网络故障的原因，若在15分钟不能解决问题，应上报到信息科长，同时告知各科室出现问题的简要情况及解决方案，30分钟内仍不能解决问题，应上报到医院院长，同时通知相关的门诊与临床业务将转入手工运作，直至网络恢复。

⑤信息科应时常与硬件网络集成商保持较好的联系，一旦出现交换设备或光纤线路损坏，能及时通知他们以最快速度赶来救援，同时做好线路备份工作。

2、服务器故障应急处理程序

①遇到服务器指示灯非正常显示，不可随便关机，根据指示灯面板符号，判断是电源、风扇、硬盘故障，此时服务器处于病态运行，一旦关机可能无法重启。

②及时与供货商或服务器定点维修站取得联系，汇报服务器状态，初步确定故障原因，由维修医院前来维修。

③任何时候关机前，先通知该服务器连接用户关机，再将数据备份，并导出到异地保存。

④若在可接受的时间范围内（例如2小时停机）修复服务器，则通知联接用户大约修复时间，若不能接受长时间停机，则将此服务器的数据转移到其他服务器运行，更改相应的应用程序的配置，直至服务器修复后再转回来。

⑤若服务器突然死机，且服务器内数据无法抢救出来，则启动备份机制，将最近一次的备份数据取出，在另外一台服务器上恢复，当日工作继续进行，同时通知各科室和财务科对断点后的数据进行补录。

⑥信息科在网络服务器恢复后，应按人员技术水平不同分片包干，协助重要科室进行数据补录工作。

⑦在数据库恢复与补录过程中，应及时与软件医院取得联系，随时获得技术支持或让软件医院技术支援，安排人员参与医院抢救和补录工作，确保将损失和影响降到最低。

3、网络服务器故障一旦发生，信息科应设24小时专人值班，监控网络运行。发现问题，在及时处理的同时迅速向科室领导汇报。故障排除后，应完成故障报告，在技术讨论会上汇报。

4、遇到较大故障，信息科工作人员应迅速集合，集体攻关。具体分为3个组做以下工作：

①故障检修组：集中[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)[管理](http://www.gongwen123.com/Article/zongjie/nianzhong/index.htm)员继续分析故障、查找原因修复[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)。

②技术联络组：迅速与软、硬件供应商联系，采取有效手段获得技术支持。

③院内协调组：通知全院各科室故障情况，并到关键科室协助数据保存。

5、全院各信息[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)使用科室应制定相应的[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)故障数据保护措施，并建立数据抢录小组，发现停机，应保存断点，保护原始数据，断点前后表单分开存放。

6、在停机期间，相关科室应组织数据抢录小组在岗待命，一旦[系统](http://www.gongwen123.com/Article/ldjh/rdzx/index.htm)恢复，当日应立即完成对重要数据的录入，第二天完成全部数据补录。

7、故障排除后2天内，信息科应组织技术研讨会，分析故障原因，制定预防措施，完成故障排除报告并上报院领导。

## 八、应急转入手工操作后各系统的应急计划

**1、故障发生的风险等级划分:**

根据可能产生的后果风险对医院的影响程度，量化评估如下：

|  |  |  |
| --- | --- | --- |
| **影响级别** | **影响性质** | **评估标准** |
| 4 | 灾难性 | 造成全院系统崩溃、数据丢失等灾难性的影响。 |
| 3 | 严重 | 严重影响病人正常就医，造成病人或医务人员极大不便。 |
| 2 | 较严重 | 对医院正常工作和病人就医有一定影响，但损失不大。 |
| 1 | 可承受 | 受影响程度很小，可以接受。 |

**2、各系统应急方案**

（1）主服务器、主交换机

责任部门：信息科，风险等级：4级（灾难性）。

现状：HIS系统主服务器采用ORACLE医院的RAC技术，在集群环境下实现双机共享数据库，以保证应用的高可用性，实现数据库在故障时的容错和无断点恢复。电源：1台30KVA UPS。

应急准备：定期检查UPS使用情况，保证供电正常。定期检查交换机。每日检查服务器、UPS运行使用情况。

应急计划：根据具体发生的情况，采取以下措施。

供电故障：临时外接电源，重新启动服务器。

服务器硬件故障：关注正常的服务器的运行状态，关闭大量查询统计的业务，保证以下关键业务的正常运行：门急诊挂号收费、药房发药、住院结算、病区医生站、病区护士站、病区药房、门诊医生站。

主交换机故障：用普通交换机替代，保证关键业务。

30分钟内不能解决，门诊收费启用门诊挂号收费应急系统。白天1小时内、晚上6小时不能解决，上报应急领导小组，建议全院各部门启用应急方案。

1. 门诊挂号收费

责任部门：门诊收费处，风险等级：3级（较严重）。

现状：门诊收费另有一套收费应急系统，收费标准和药品代码单价等数据字典与最近连接主服务器时一致。当联结主服务器出现故障时，启动收费应急系统。等待系统恢复，可以把应急数据自动更新至主服务器。

应急准备：手工发票、复写纸、笔、算盘、计算器等记帐用品，检查化验收费价目。

应急计划：根据具体情况，采取以下措施：

网络、服务器故障：启用门诊收费应急系统。

系统瘫痪：手工划价记帐。系统恢复后，把手工单子补入计算机。

（3）门诊药房（中、西、急诊）

责任部门：门诊药房，风险等级：2级（严重）。

现状：收费后确认发药及退药确认。（配备单机版药品代码单价等数据字典备用）。

应急计划：凭处方或发票发药。待系统恢复正常后，确认发药以减库存。

（4）药库（中、西）

责任部门：药库，风险等级：2级（严重）。

应急计划：先用手工记帐，把药品分发至药房，保证药房的供应。待系统恢复，再补发放。对于调价，直接通知门诊收费处。

（5）门诊医生站

责任部门：门办，风险等级：3级（较严重）。

应急准备：手工处方、各类检查单、门诊日志表。

应急计划：手工处理。

（6）门诊叫号

责任部门：门诊护士，风险等级：2级（严重）。

应急计划：人工叫号。

（7）医技管理系统

责任部门：各医技部门，风险等级：2级（严重）。

应急准备：医技记帐单、各自医技项目单价表。

应急计划：手工登记、划价。对于住院病人，及时把划价单送住院收费处。

（8）LIS系统

责任部门：检验科，风险等级：3级（较严重）。

现状：LIS系统单独有服务器、可以脱离医院主服务器工作。

应急准备：化验收费价目、手工化验报告单。

应急计划：根据具体情况，采取以下措施：

服务器故障。保存在各检验仪器的工作站上，改集中打印为到每个站点打印报告单。然后送到门诊、病房。

系统瘫痪：仪器独自工作，人工抄写报告单。待系统恢复后，再人工输入。

（9）PACS（放射、超声、内镜、病理）

责任部门：放射科、超声、内镜、病理，风险等级：3级（较严重）。

现状：整个PACS系统有独立的服务器和存储系统，单独的汇聚网络交换机。所有的PACS数据库都在一台备份服务器上建立镜像服务，数据实时同步到镜像服务器，一旦主服务器数据库故障，可以及时启用镜像数据库，保证正常PACS业务工作。

应急准备：手工报告单。定期检修UPS。

系统瘫痪：手工出报告单，但无图像。

（10）门办管理系统

责任部门：门诊办公室，风险等级：1级（可承受）。

现状：门办系统主要用于统计和查询工作量。 待系统恢复即可。

（11）住院收费

责任部门：住院收费处，风险等级：2级（严重）。

应急准备：笔、预缴款收据。

应急计划：网络、服务器故障。启用应急系统。

系统瘫痪：手工开预缴款收据，手工入院。对于出院病人，记录通信地址，先出院，待系统恢复再补办。

（12）住院药房

责任部门：住院药房，风险等级：3级（较严重）。

应急准备：记帐单。

应急计划：先发药，再到住院处记帐或系统恢复后记帐。

（13）住院护士站

责任部门：住院护士，风险等级：3级（较严重）。

应急准备：执行单等。

应急计划：手工处理。

（14）住院医生站

责任部门：住院医生，风险等级：3级（较严重）。

应急准备：医嘱单、化验单、手术单等。

应急计划：手工处理。开临时医嘱先取药。

（15）电子病历

责任部门：住院医生，风险等级：2级（严重）。

应急准备：病历纸等。

应急计划：手工处理。

（16）手术、麻醉管理系统

责任部门：手术室、麻醉科，风险等级：2级（严重）。

应急计划：手工处理。所发生费用直接在住院处记帐。

（17）血库管理系统

责任部门：血库，风险等级：2级（严重）。

应急准备：记帐单，项目单价表。

应急计划：手工登记、划价。及时把划价单送住院收费处。

（18）院长查询系统

责任部门：院领导，风险等级：1级（可承受）。

现状：待系统恢复即可。

（19）病案统计系统

责任部门：病案统计室，风险等级：1级（可承受）。

现 状：待系统恢复即可。

3、应急预案的结束

（1）应急预案结束的前提条件:

①系统恢复正常，业务可正常办理。

②工作站完成应急业务补记账工作。在自助渠道关闭的前提下先开启工作站应用系统。

③所有挂失业务处理完毕，补账工作完成，账务核对无误。

（2）应急预案结束的指令发布:

应急预案的结束由领导小组决定。运行部门根据指令全面恢复应用系统，相关人员开启自助设备。

（3）应急预案结束后的主要工作:

①业务支持工作组、技术支持工作组和安全及法律保障工作组继续监控事件解决后的运作情况，直至确定可持续正常运作为止。

②领导小组对本次故障进行全面总结。领导小组汇总应急工作开展情况，对本次突发事件的起因、造成的不良影响、资金损失以及应急工作本身等进行全面总结分析，并提出改进意见，督查改进情况，进一步优化应急流程。

③信息科负责备份应急数据至工作站，每半天一次同步。在应急业务结束后及时删除应急数据，防范风险。

## 九、应急数据恢复工作规程

1、当服务器确认出现故障时，由网络管理员按《数据备份恢复方案》进行系统恢复。

2、网络管理员由信息科主任指定专人负责恢复。当人员变动时应有交接手续。

3、当网络线路不通时，网络管理员应立即到场进行维护，当光纤损坏时应立即使用备用光纤进行恢复，交换机出现故障时，应使用备用交换机。

4、对每次的恢复细节应做好详细记录。

5、平时应定期对全系统备份数据要进行模拟恢复一次，以检查数据的可用性。

## 十、网络服务器故障应急处理规程

网络服务器故障是因硬件或软件原因致使医院信息管理系统运行停止，一旦发生故障，按下列规程处理。

1、信息科应设专人管理，监控网络运行。发现问题，在及时处理的同时迅速向科室领导汇报。故障排除后，应完成故障报告，在技术讨论会上汇报。

2、遇到较大故障，信息科工作人员应迅速集合，集体攻关。具体分为3个组做以下工作：

（1）故障检修组：集中系统管理员继续分析故障、查找原因、修复系统。

（2）技术联络组：迅速与软、硬件供应商取得联系，采取有效手段获得技术支持。

（3）院内协调组：通知全院各科室故障情况，并到关键科室协助数据保存。

3、全院各系统使用科室制定相应的系统故障数据保护措施，并建立数据抢录小组，发现停机，应保存断点，保护原始数据，断点前后表单分开存放。

4、在停机期间，相关科室应组织数据抢录小组在岗待命，一旦系统恢复，当日应立即完成对重要数据的录入，第二天完成全部数据补录。

5、故障排除后，信息科工作技术组应按制定方案分片包干，协助重要科室进行数据补录工作。

6、故障排除后2天内，信息科应组织技术研讨会，分析故障原因，制定预防措施，完成故障排除报告院领导。

## 十一、应急保障

（一）平时网络与信息安全的防护

1、组织管理措施：应急组织机构要进行层层把关，层层落实，对组织机构中的人员及联系方式，要做到及时更新，并进行定期的安全知识培训。

2、技术保障：一方面进行网络设备的安全加固，例如增加防火墙、入侵监测设备等，对已知的系统漏洞及时安装补丁程序，另一方面要进行技术储备，对内部进行人员定期培训，同时采取通过向专业网络安全医院购买安全服务的方式，加强处理紧急情况的能力和效率。

3、在网络工程建设和规划方面，要切实加强网络安全方面考虑，设计时要考虑设备的冗余备份，信息存储的异地备份等。

（二）应急预案演练

应急小组要定期进行应急预案的演练，增强应急响应的能力和意识。

### 附件1：护士站信息管理系统应急预案

本应急方案适用于某一个或多个部门的信息系统因故障不能正常使用，甚至全院整个系统崩溃。例如火灾、停电等外界不可预见的问题，受计算机病毒及黑客的攻击，引起系统故障甚至系统瘫痪，关键设备（如服务器、交换机等）故障、检修、更新等引起的系统的瘫痪，因软件故障引起的系统不能正常的运行等均属于该范围。对于某工作站局域性故障一般采用备用机器的办法，不启动应急方案。

1. 遵守医院的信息管理应急预案。
2. 建立应急小组：总指挥为护理副院长，成员包括科护士长、护士长、护理组长、秘书。部门直接负责的护士长为现场应急指挥者，协调部门内的工作及与其他部门保持联系。
3. 根据故障可能产生的后果、风险，及对医院影响的严重性，在医院信息系统发生整体故障时，护理部门的风险等级为3级。
4. 护理部门在信息科不可预知系统能否恢复的情况下，经医院信息领导小组负责人通知，启用应急预案后，采用人工抄写的方式。
5. 部门应急备份医疗文件:

1、位置：病区护士站。

2、内容：普通医嘱单、化疗医嘱单、TPN单、手术通知单、X线、B超申请单、CT申请单、给药单、体温单、护理系统评估单各一百张。

3、使用方法：接到护理部启用紧急预案的通知后，由护士长将备份医疗文件包取出，协调医生、护士使用医疗文书，恢复手工操作。

4、使用的原则：医生将普通医嘱（包括抗生素医嘱及入院新医嘱）开具在普通医嘱单上，特殊性药物如化疗使用化疗医嘱单，TPN使用TPN单，原则上仅限为病人在紧急病情变化的状态下更改医嘱。护士治疗及给药工作参照前一天护士执行单，新医嘱处理根据为两人核对新产生的手工医嘱清单后执行医嘱，转抄并记录在给药单上。病人的生命体征记录以手工的方式记录在体温单上。

1. 在紧急状态下各成员职责：

1、日间：

首先发现计算机系统故障的工作人员，应立即与信息科联系，电话8015或8100。确认为网络故障时立即向护士长汇报。护士长按意外事件汇报程序进行报告。

（1）护士长职责：

立即向科护士长、信息科主任、护理副院长汇报。

协调医生使用医疗文书，实行人工操作。

协调部门工作人员有次序地进行工作，保证病房工作正常运行。

（2）护理秘书职责：

接收书面医嘱。

根据医嘱抄写化验标签。

根据检查申请单安排病人进行各项检查。

接收辅助科室的各种检查报告，发现异常及时与医生联系。

接听各种电话通知的检查结果并记录。

（3）护士组长职责：

将护理评估信息记录在书面的护理系统评估单上。

配合主管医生查房，并从前一天的医嘱执行单、口服药单、静脉输液单等处获得病人治疗及检查信息。

核对责任护士处理的医嘱信息。

（4）责任护士职责：

根据前一天的医嘱执行单、口服药单、静脉输液单等获得病人治疗及检查信息。

将书面医嘱抄写到给药单上，正确给药后签名记录。

（5）药班：

与药房及中心配置室进行药物的正确核对。

2、夜间

首先发现计算机系统故障的工作人员，应立即与信息科联系，直接用虚拟网与信息科值班工作人员联系。确认为网络故障时立即向值班护士长汇报。值班护士长按意外事件汇报程序进行报告行政总值班。

（1）护士长职责：

立即向科护士长、信息科主任、护理副院长汇报。

协调医生使用医疗文书，实行人工操作。

协调部门工作人员有次序的进行工作，保证病房工作正常运行。

（2）护士组长职责：

接收书面医嘱。

根据医嘱抄写化验标签。

根据检查申请单安排病人进行各项检查。

接收辅助科室的各种检查报告，发现异常及时与医生联系。

接听各种电话通知的检查结果并记录。

将护理评估信息记录在书面的护理系统评估单上。

从最近一天的医嘱执行单、口服药单、静脉输液单、新医嘱批处理等处获得病人治疗及检查信息。

核对责任护士处理的医嘱信息。

（3）责任护士职责：

从最近一天的医嘱执行单、口服药单、静脉输液单、新医嘱批处理等处获得病人治疗、检查信息。

将书面医嘱抄写到给药单上，正确给药后签名记录。

与药房及中心配置室进行药物的核对。

（七）系统恢复后的处理:

根据系统中断的时间，在信息科的协助下，将书面信息进行补录入信息系统内。

（八）门诊护理及ICU、ER参照本部门情况制定的应急预案。

### 附件2：门诊护理信息系统应急预案

本应急方案适用于某一个或多个部门的信息系统因故障不能正常使用，甚至全院整个系统崩溃。例如火灾、停电等外界不可预见的问题，受计算机病毒及黑客的攻击，引起系统故障甚至系统瘫痪，关键设备（如服务器、交换机等）故障、检修、更新等引起的系统的瘫痪，因软件故障引起的系统不能正常的运行等均属于该范围。对于某工作站局域性故障一般采用备用机器的办法，不启动应急方案。

（一）遵守医院计算机系统的应急预案。

（二）建立部门现场应急指挥小组：

总指挥：护士长

成员：小组长、秘书以及当班护士。

（三）紧急状态下小组各成员的职责：

1、护士长：立即协调和指挥门诊所有护理人员的行为，保证电脑故障期间的门诊工作有序，期间及时有序地向上级部门汇报，传达紧急通知的内容，确保门诊病人均得到合适的安排和照顾。

2、秘书：立即把备用的手写处方、常用的门诊书写记录、治疗单分发到各护士台。

3、小组长：立即通知所在区域的门诊病人，告诉实情，请他们谅解并安慰一些情绪紧张的病人，说明医院的应急措施，同时通知医生作好病人的解释工作。

（四）具体操作：

电脑系统瘫痪，门诊护士站及诊间使用脱机版的门诊诊间程序：

1、仍遵循常规门诊流程。

2、导医台的护士，在给病人分诊时，因给予合适的解释，及时纠正一部分病人因电脑故障造成的各种问题，并及时与护士长沟通。

3、与门诊办公室共同协商，张贴有关信息。

4、医生使用脱机版的门诊诊间程序，操作方式与原有系统一致。

5、护士台的工作程序不变，按工作区域解决诊间程序使用中的问题，妥善安排及时疏散就诊病人。

6、对于治疗单的收费形式，使用手工书写。

### 附件3：门诊收费系统应急预案

本应急方案适用于某一个或多个部门的信息系统因故障不能正常使用，甚至全院整个系统崩溃。例如火灾、停电等外界不可预见的问题，受计算机病毒及黑客的攻击，引起系统故障甚至系统瘫痪，关键设备（如服务器、交换机等）故障、检修、更新等引起的系统的瘫痪，因软件故障引起的系统不能正常的运行等均属于该范围。对于某工作站局域性故障一般采用备用机器的办法，不启动应急方案。

（一）遵守医院的信息管理应急预案。

（二）建立应急小组：总指挥为财务科主任，成员包括门诊收费工作人员。协调部门内的工作及对其他部门保持联系。

（三）在医院信息系统发生整体故障时，门诊收费的风险等级为3级。

（四）在信息科不可预知系统能否恢复的情况下，在医院信息领导小组负责人通知启动应急预案后，恢复手工操作。

1、挂号

（1）初诊病人：

启用临时病历号段，等系统恢复后重新补录。

由收费员在导医台手工编号，同时登记病人一览表，在一览表上注明病人的名字、性别，同时在病人填写的门诊病历首页上注明其病历号码。

根据病人所挂临床科室，注明科室，并由相应门诊护士站进行手工登记，维持就诊次序。

医生恢复手工操作，门诊收费处将各种检查单及门诊处方进行手工收费。

（2）复诊病人：

由收费员在导医台根据病人原有编号，登记病人一览表，在一览表上注明病人的名字、性别，等系统恢复后重新补录。

根据病人所挂临床科室，注明科室，并由相应门诊护士站进行手工登记，维持就诊次序。

医生恢复手工操作，门诊收费处将各种检查单及门诊处方进行手工收费。

2、收费

（1）门诊病人：

医生开具手工申请单、手工处方，请病人到相关检查科室、药房划价，窗口根据申请单及处方上所划价格收取费用，开具手工发票，并告知病人：等系统恢复后补开电脑发票（尤其是医保病人，以手工发票换取电脑发票）。

（2）急诊病人：

病人拿手工处方到药房划价，收费窗口根据所划价格收取费用，开具手工发票，并告知病人等系统恢复后补开电脑发票（尤其是医保病人，以手工发票换取电脑发票）。

各项手工申请单无法划价的，先由急诊室开具一式两份的手工记帐单，先向病人收取一定金额的押金，开具押金单，给病人记帐，请其先去做检查，等电脑修复后，由急诊医生和护士将病人已做的检查输入电脑，病人凭押金单来结帐，开具电脑发票。

### 附件4：住院部信息系统应急预案

本应急方案适用于某一个或多个部门的信息系统因故障不能正常使用，甚至全院整个系统崩溃。例如火灾、停电等外界不可预见的问题，受计算机病毒及黑客的攻击，引起系统故障甚至系统瘫痪，关键设备（如服务器、交换机等）故障、检修、更新等引起的系统的瘫痪，因软件故障引起的系统不能正常的运行等均属于该范围。对于某工作站局域性故障一般采用备用机器的办法，不启动应急方案。

（一）遵守医院的信息管理应急预案。

（二）建立应急小组：总指挥为财务科主任，成员包括出入院处工作人员，协调部门内的工作及对其他部门保持联系。

（三）在医院信息系统发生整体故障时，出入院处的风险等级为3级。

（四）出入院处在信息科不可预知系统恢复的情况下采用人工操作的方式。

1、住院流程：

病人出示医生开具的、床位协调处已安排好相应床位的住院证，手工办理入院手续。

收取相应的预缴款，并手工开具预缴款收据，等电脑系统修复后输入电脑。

手工记录下住院病人的相关信息，等电脑系统修复后，及时录入电脑。

2、出院流程：

凭住院病区工作人员开具的出院通知单，记录下该病人的联系电话，手工开具出院病人凭证，不办理结账手续，病人可去病区药房领取出院带药。并告知病人待系统恢复后来院办理出院手续。

系统修复后，出、入院处工作人员应及时完成电脑信息补输入，并与出院未结帐的病人进行联系，办理结帐手续。

### 附件5：检验科信息管理系统应急预案

本应急方案适用于某一个或多个部门的信息系统因故障不能正常使用，甚至全院整个系统崩溃。例如火灾、停电等外界不可预见的问题，受计算机病毒及黑客软件的攻击，引起系统故障甚至系统瘫痪，关键设备（如服务器、交换机等）故障、检修、更新等引起的系统的瘫痪，因软件故障引起的系统不能正常的运行等均属于该范围。对于某工作站局域性故障一般采用备用机器的办法，不启动应急方案。

（一）遵守医院的信息管理应急预案。

（二）建立应急小组：总指挥为检验科主任，成员包括检验科网络管理员和检验科工作人员，协调部门内的工作及与其他部门保持联系。

（三）在医院信息系统发生整体故障时，检验科部门的风险等级为3级。

（四）检验科在信息科不可预知系统恢复的情况下采用人工抄写的方式，如果医院信息系统中门诊医生工作站和住院医生工作站可以使用单机版程序，则使用单机版进行电子申请代替手写申请。如无法使用，则流程仍然通过手工模式进行。

1、门急诊处理流程：

由医生用空白化验单开出检验申请，收费处手工通费，采样处凭盖章的手工申请单进行采样并手工抄写标签贴上容器，检验科手工填写检验结果后发出报告。待系统恢复后，将信息补录入系统内。

2、住院处理流程：

由医生开出书面检验医嘱，护士采样并手工抄写标签贴上容器送检，检验科工作人员手工填写检验结果后发出报告。待系统恢复后，将信息补登入系统内。

（五）标本处理流程：

所有急诊标本紧急情况下按手术、急诊、ICU、病房急诊和门诊急诊的先后次序进行仪器测定，先将结果电话通知主管医生或护士。系统恢复后，将信息补录入系统内。

非急诊标本手工将结果抄至化验单上发送，等网络恢复后再将病人资料和结果重新输入电脑保存，发送正式报告。

### 附件6：药剂科信息管理系统应急预案

本应急方案适用于某一个或多个部门的信息系统因故障不能正常使用，甚至全院整个系统崩溃。例如火灾、停电等外界不可预见的问题、受计算机病毒及黑客的攻击、引起系统故障甚至系统瘫痪、关键设备（如服务器、交换机等）故障、检修、更新等引起的系统的瘫痪、因软件故障引起的系统不能正常的运行等均属于该范围。对于某工作站局域性故障一般采用备用机器的办法，不启动应急方案。

（一）遵守医院的信息管理应急预案。

（二）建立应急小组：总指挥药剂科主任，成员包括药剂科工作人员，协调部门内的工作及与其他部门保持联系。

（三）在医院信息系统发生整体故障时，药剂科的风险等级为3级。

（四）药剂科在信息科不可预知系统恢复的情况下采用人工操作的方式。

1、门诊药房

（1）使用脱机版医生诊间系统时,患者凭已付费盖章处方取药;计算机系统恢复正常后,减去库存。

（2）使用手工处方,启用脱机版药价查询系统, 安排人员手工划价。

2、病区药房与配置中心

（1）临时医嘱处理流程

由医生提供一式三联的手工医嘱（一联留护士站，两联根据用药情况送药房——配置中心或病区药房），配置中心药师按医嘱手工填写输液标签、一式两联发送单，按发送单发送普通针剂、片剂，一联发送单交护士核对，一联留作收费凭证，系统恢复后收费。

（2）长期医嘱处理流程

统计各病区用药清单，清单包括病人姓名、床号、药品名称、规格、用法、用量，一式两联，一联作为发送凭证，交于护士核对，一联留存作为药房收费凭证。静脉输液统计清单送配置中心，配置中心药师按清单手工填写输液标签，配置员按常规摆药配置。片剂及其他针剂清单发送到病区药房，药师按清单发放。系统恢复后收费。

3、药库

先用手工记帐方式向外面领药部门发放药品, 以保障临床病人医药, 待计算机系统恢复正常后再补入电脑。

### 附件7：放射科信息管理应急预案

本应急方案适用于某一个或多个部门的信息系统因故障不能正常使用，甚至全院整个系统崩溃。例如火灾、停电等外界不可预见的问题，受计算机病毒及黑客的攻击，引起系统故障甚至系统瘫痪，关键设备（如服务器、交换机等）故障、检修、更新等引起的系统的瘫痪，因RIS\PACS软件故障引起的系统不能正常运行等均属于该范围。对于某工作站局域性故障一般采用备用机器的办法，不启动应急方案。

（一）遵守医院的信息管理应急预案。

（二）建立应急小组：总指挥为放射科主任，成员包括放射科工作人员、部门登记人员。放射科副主任协调部门内的工作及对其他部门保持联系。

（三）在医院信息系统发生整体故障时，放射科的风险等级为3级。

（四）医院网络与放射科网络连接出现故障，而放射科内部系统运行正常时。

1、原则：对于门诊患者，登记前核查患者是否已经缴费；对于住院患者，采用脱机版程序进行通费。

2、方法：

（1）有病历号的门诊病人，放射科登记处在登记的时候，在电脑上采用手工登记，输入患者的病历号、姓名、性别、床位号、年龄等信息，选择检查类型、检查部位，进行登记。在后续的检查步骤中，摄片、胶片打印、报告书写等和网络正常时一样操作。

（2）没有病历号的门诊病人，则由放射登记处、CT登记处参照附件中的手工登记表格进行登记，将临时流水号抄在申请单上，技师在摄片的时候在机器上手工输入临时流水号和患者姓名的拼音，进行检查。等到故障排除，患者拿到病历号之后再使用电脑进行登记，到机器上修改流水号等信息，再传往RIS/PACS，继续后面的报告书写等流程。

（3）住院病人，放射科登记处在登记的时候在电脑上采用手工登记，输入患者的病历号、姓名、性别、床位号、年龄等信息，选择检查类型、检查部位，进行登记。后面的检查步骤中，摄片、胶片打印、报告书写等和网络正常时一样操作。

（五）放射科内部系统出现故障。

1、原则：对于门诊患者，登记前核查患者是否已经缴费；对于住院患者，采用脱机版程序进行通费。

2、方法：

（1）有病历号的门诊病人，放射科登记处在登记的时候，参照附件中的手工登记表格进行登记，将临时流水号抄在申请单上，技师在摄片的时候在机器上手工输入临时流水号和患者姓名的拼音，进行检查。病人检查完毕后，先将胶片打印之后给病人，报告如需要，手写后由医生签名后给病人。等到故障排除，系统恢复正常之后再使用电脑进行登记，到机器上修改流水号等信息，再传往PACS。

（2）没有病历号的病人，则由放射登记处和CT登记处参照附件中的手工登记表格进行登记，将临时流水号抄在申请单上，技师在摄片的时候在机器上手工输入临时流水号和患者姓名的拼音，进行检查。病人检查完毕后，先将胶片打印之后给病人，报告如需要，手写后由医生签名后给病人。等到网络正常，患者拿到病历号之后再使用电脑进行登记，到机器上修改流水号等信息，再传往PACS。再补报告书写等后续流程。

（3）住院病人，放射科登记处在登记的时候参照下面的手工登记表格进行登记，将临时流水号抄在申请单上，技师在摄片的时候在机器上手工输入临时流水号和患者姓名的拼音，进行检查。对于危重和紧急的病人，检查完毕后，先将胶片打印之后给病人，报告如需要，手写后由医生签名后给病人，并等到网络正常时补收费。待网络正常，患者拿到病历号之后再使用电脑进行登记，到机器上修改流水号等信息，再传往PACS。

（六）放射科手工登记表格，其中临时流水号一项，放射登记处从700001开始计数，CT登记处从800001开始计数。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 | 病历号 | 性别 | 年龄 | 检查类型 | 就诊类别 | 检查部位 | 临时流水号 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### 附件8：信息科机房故障应急预案

为科学应对网络与信息安全突发事件，提高信息中心机房处理突发信息网络事件的能力，建立健全信息安全应急机制，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，特制订信息中心机房故障应急预案。

本预案坚持“统一领导、协调配合、明确责任、依法规范、条块结合、整合资源、防范为主、加强监控”的原则。适用于信息中心机房可能发生的网络与信息安全突发事件。

**一、机房漏水防治应急预案**

（1） 发生机房漏水后，第一目击者应立即通知网络与信息安全领导小组。

（2）若空调系统出现渗漏水，应立即停止故障空调,将机房内的积水清除干净，并及时联系设备供应方进行处理，必要情况下可以临时用电扇对服务器进行降温。

（3）若为墙体或窗户渗漏水，应立即通知行总务科，及时清除积水，进行墙体或窗户维修，避免不必要的损失。

**二、设备发生被盗或人为损害事件应急预案**

（1）发生设备被盗或有人为损害设备情况时，使用者或管理者应立即报告网络与信息安全领导小组，同时保护好现场。

（2）网络与信息安全领导小组接报后，通知安全保卫部门及公安部门，一同核实审定现场情况，清点被盗物资或盘查人为损害情况，做好必要的影像记录和文字记录。

（3）事件当事人应当积极配合公安部门进行调查，并将有关情况向网络与信息安全领导小组汇报。

（4）网络与信息安全领导小组召开会议研讨，事态严重时，应向局网络与信息安全领导小组办公室报告，请示进一步处理的决策。

**三、机房长时间停电应急预案**

接到长时间停电通知后，应及时通过内网发布或电话通知停电通告，要求网内用户在停电前停止办公、保存数据并正常关机。

**四、通信网络故障应急预案**

（1）发生通信网络故障后，计算机操作员应及时将信息告知网络与信息安全小组。

（2）网络与信息安全小组及时查清通信网络故障位置，或告知相关通信网络运营商，请求协助查清原因，同时，隔离故障区域，切断故障区与服务器的网络联接。

（3）系统管理员会同电信技术人员或医院技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

（4）相关责任人负责写出故障分析报告，上报网络与信息安全小组备查。

**五、不良信息和网络病毒事件应急预案**

（1）当发现不良信息或网络病毒时，网络管理员应立即断开网线，终止不良信息或网络病毒传播，并告知网络与信息安全小组。

（2）接到报告后，网络与信息安全小组应立即通告局域网内所有计算机用户防病毒方法，隔离网络，指导各计算机操作人员进行杀毒处理，直至网络处于安全状态。

（3）对不良信息要进一步追查来源，对未经相关领导同意，擅自发布信息，造成不良影响且触犯法律者，移交执法部门追究法律责任。

（4）情况严重时，应立即向市局网络与信息安全应急领导小组报告，请求支援，作好应对措施。

**六、计算机软件系统故障应急预案**

（1）发生计算机软件系统故障后，计算机操作人员立即保存数据，并停止该计算机使用应用。

（2）由部门负责人将情况报告网络与信息安全小组，不得擅自进行处理。

（3）网络与信息安全领导小组迅速派出技术人员进行处理，必要情况下，应对硬盘进行备份。

（4）在保持原始数据安全的情况下，对计算机系统进行修复；修复系统成功，则检查数据丢失情况，利用备份数据恢复；若修复失败，立即联系相关厂商和市局信息中心请求支援。

**七、黑客攻击事件应急预案**

（1）当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告网络与信息安全小组。

（2）接到报告后，网络与信息安全小组应立即关闭网络，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

（3）及时清理系统、恢复数据、程序，尽力将系统和网络恢复正常；情况严重时，应立即向市局网络与信息安全应急领导小组报告，请求支援，作好应对措施。

**八、机房设备硬件故障应急预案**

（1）发生机房设备硬件故障后，网络与信息安全领导小组应立即确定故障设备及故障原因，并进行先期处置。

（2）若故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（3）故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商，并认真填写设备故障报告单备查。

**九、应急处置**

发生信息网络突发事件后，相关人员应在5分钟内向网络与信息安全小组报告，应急小组组织人员开展先期处置。发生重大事件应向市局网络与信息安全应急领导小组报告。

**十、善后处置**

应急处置工作结束后，网络与信息安全小组组织有关人员及邀请上级信息中心技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，总结经验教训，整改存在隐患组织，恢复正常工作秩序。

**十一、应急通讯保障**

网络与信息安全小组全体人员保证全天24小时通讯畅通。

**十二、装备保障**

应预留一定数量的信息网络硬件和软件设备，指定专人保管和维护。

**十三、数据保障**

重要信息系统均应建立备份系统，保证重要数据在受到破坏后可紧急恢复。

**十四、队伍保障**

选择熟悉本单位软硬件系统的抚州市易通科技有限医院作为突发信息网络突发事件的社会应急支援单位，提供技术支持与服务。

**十五、宣传、培训和演习**

宣传

网络与信息安全小组每年至少开展一次范围内的信息网络安全教育，提高信息安全防范意识和能力。

**十六、培训**

网络与信息安全领导小组每年至少开展一次信息网络安全培训，提高信息网络事件的应急能力。

**十七、预案演习**

网络与信息安全小组每年至少安排一次演练，通过演练发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处理能力。



5771001803090012095 579036822859633082

5771001803090012386 576137399735760696

5771001803090013594 578077579902515512

5771001803090012387 577164982601818051

5771001803090012138 572131192158918326

5771001803090012359 579036822361076053

5771001803090012356 576135286143791742

5771001803090012355 575087869704693279

17088100343355274 101229944325833379

17088100343355275 101866732938832008

17088100343356107 101581152501500522

17088100343356108 101000180059871732

17088100343354295 101074194142687017

17088100343356184 101878660869628802

17088100343356185 101775831174086674

17088100343356109 101086014373572846

17088100343356110 101152207216014916

17088100343355237 101027041605702709

17088100343355238 101229364861425414

17088100343356169 101862204402635718

17088100343354928 101760654089788804