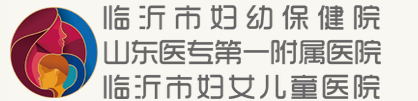
临沂市妇幼保健院

信息安全管理制度汇编



2017年6月

目录

[临沂市妇幼保健院 信息安全工作总体规定 1](#_Toc529970737)

[第一章 总则 1](#_Toc529970738)

[第二章 方针、目标和原则 1](#_Toc529970739)

[第三章 总体安全策略 3](#_Toc529970740)

[第四章 信息安全总体框架 9](#_Toc529970741)

[第五章 附则 11](#_Toc529970742)

[临沂市妇幼保健院 信息安全制度管理规定 12](#_Toc529970743)

[第一章 总则 12](#_Toc529970744)

[第二章 制度建设组织管理 13](#_Toc529970745)

[第三章 制度建设规划与年度计划 13](#_Toc529970746)

[第四章 制度起草 13](#_Toc529970747)

[第五章 审查、论证与批准 15](#_Toc529970748)

[第六章 修订与废止 16](#_Toc529970749)

[第七章 附则 17](#_Toc529970750)

[临沂市妇幼保健院 信息化工作规则 22](#_Toc529970751)

[第一章 总则 22](#_Toc529970752)

[第二章 机构与职责 22](#_Toc529970753)

[第三章 项目和实施 24](#_Toc529970754)

[第四章 资金和资产 24](#_Toc529970755)

[第五章 附则 25](#_Toc529970756)

[临沂市妇幼保健院 信息系统“三员”管理规定 26](#_Toc529970757)

[第一章 总则 26](#_Toc529970758)

[第二章 系统管理员职责 26](#_Toc529970759)

[第三章 安全管理员职责 27](#_Toc529970760)

[第四章 安全审计员职责 28](#_Toc529970761)

[第五章 附则 28](#_Toc529970762)

[临沂市妇幼保健院 信息系统安全检查规定 29](#_Toc529970763)

[第一章 总则 29](#_Toc529970764)

[第二章 实施细则 29](#_Toc529970765)

[第三章 附则 30](#_Toc529970766)

[临沂市妇幼保健院 人员信息安全管理规定 38](#_Toc529970767)

[第一章 总则 38](#_Toc529970768)

[第二章 内部工作人员管理 38](#_Toc529970769)

[第三章 外部相关人员管理 39](#_Toc529970770)

[第四章 附则 39](#_Toc529970771)

[临沂市妇幼保健院 信息安全教育和培训管理规定 43](#_Toc529970772)

[第一章 总则 43](#_Toc529970773)

[第二章 信息安全教育、培训、考核 43](#_Toc529970774)

[第三章 附则 44](#_Toc529970775)

[临沂市妇幼保健院 机房管理规定 45](#_Toc529970776)

[第一章 总则 45](#_Toc529970777)

[第二章 机房管理 45](#_Toc529970778)

[第三章 附则 46](#_Toc529970779)

[临沂市妇幼保健院 门户网站管理办法 47](#_Toc529970780)

[第一章 总则 47](#_Toc529970781)

[第二章 信息采集与报送 47](#_Toc529970782)

[第三章 信息审核与发布 48](#_Toc529970783)

[第四章 信息管理 48](#_Toc529970784)

[第五章 安全管理 49](#_Toc529970785)

[第六章 附则 49](#_Toc529970786)

[临沂市妇幼保健院 信息系统运行维护管理办法 51](#_Toc529970787)

[第一章 总则 51](#_Toc529970788)

[第二章 信息化办公设备运维管理 51](#_Toc529970789)

[第三章 网络系统运维管理 52](#_Toc529970790)

[第四章 主机、存储系统运维管理 52](#_Toc529970791)

[第五章 应用系统、数据运维管理 53](#_Toc529970792)

[第六章 驻场运维人员管理 54](#_Toc529970793)

[临沂市妇幼保健院 信息系统设备管理规定 55](#_Toc529970794)

[第一章 总则 55](#_Toc529970795)

[第二章 设备选型、购置与安装 55](#_Toc529970796)

[第三章 设备登记与使用 56](#_Toc529970797)

[第四章 设备维修、报废与销毁管理 57](#_Toc529970798)

[第五章 附则 57](#_Toc529970799)

[临沂市妇幼保健院 移动存储介质管理规定 59](#_Toc529970800)

[第一章 总则 59](#_Toc529970801)

[第二章 存储介质使用 59](#_Toc529970802)

[第三章 介质保存 60](#_Toc529970803)

[第四章 介质接入 60](#_Toc529970804)

[第五章 介质维修、报废和销毁管理 61](#_Toc529970805)

[第六章 附则 61](#_Toc529970806)

[临沂市妇幼保健院信息系统 恶意代码防范与软件补丁分发管理规定 65](#_Toc529970807)

[第一章 总则 65](#_Toc529970808)

[第二章 恶意代码防范管理 65](#_Toc529970809)

[第三章 安全漏洞与补丁安全管理 66](#_Toc529970810)

[第四章 附则 67](#_Toc529970811)

[临沂市妇幼保健院 信息系统安全审计管理规定 69](#_Toc529970812)

[第一章 总则 69](#_Toc529970813)

[第二章 审计管理 69](#_Toc529970814)

[第三章 附则 70](#_Toc529970815)

[临沂市妇幼保健院 信息系统数据备份与恢复管理规定 71](#_Toc529970816)

[第一章 总则 71](#_Toc529970817)

[第二章 职责与分工 71](#_Toc529970818)

[第三章 数据备份方式 71](#_Toc529970819)

[第四章 数据备份与恢复的管理 72](#_Toc529970820)

[第五章 附则 73](#_Toc529970821)

[临沂市妇幼保健院 信息系统密码管理规定 74](#_Toc529970822)

[第一章 总则 74](#_Toc529970823)

[第二章 密码管理 74](#_Toc529970824)

[第三章 附则 75](#_Toc529970825)

[临沂市妇幼保健院 76](#_Toc529970826)

[软件正版化管理规定 76](#_Toc529970827)

[第一章 总则 76](#_Toc529970828)

[第二章 职责与权限 76](#_Toc529970829)

[第三章 正版软件的管理 77](#_Toc529970830)

[第四章 其他规定 78](#_Toc529970831)

[第五章 附 则 79](#_Toc529970832)

# 临沂市妇幼保健院 信息安全工作总体规定

## 总则

1. 为加强和规范临沂市妇幼保健院信息系统安全工作，提高信息系统整体安全防护水平，实现信息安全的可控、能控、在控，依据国家有关法律法规规定，结合我单位工作实际，制定本规定。
2. 本规定适用于临沂市妇幼保健院信息系统的安全保护总体方针、策略制定和规划方面的工作。

## 方针、目标和原则

1. 临沂市妇幼保健院信息安全工作应坚持“积极预防、全面保障、动态管理、持续改进”的总体方针，实现信息系统安全可控、能控、在控。依照“分区、分级、分域”总体安全防护策略，执行信息系统安全等级保护制度。
2. 临沂市妇幼保健院信息安全工作的总体目标是确保信息系统持续、稳定、可靠运行和确保信息内容的机密性、完整性、可用性，防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃，抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏，防止数据丢失，防止系统对外服务中断和由此造成的系统运行事故。
3. 信息安全工作的总体原则

（一）需求导向原则

根据其信息系统承载的业务，信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，平衡安全投入与效果。

（二）领导负责原则

一把手负总责，分管领导在职责范围内各负其责的信息安全管理。

（三）全员参与原则

信息系统所有相关人员须参与信息系统的安全管理，共同保障信息系统安全。

（四）标准化原则

按照信息安全等级保护相关标准的要求，采用管理和技术结合的方法，实现信息安全目标。

（五）同步实施原则

新建信息系统时，应充分考虑信息化发展趋势，遵循信息化建设与信息安全建设同步规划、同步建设、同步实施的原则，确保信息化建设与信息安全建设同步进行。

（六）管理与技术并重原则

坚持积极防御和综合防范，全面提高信息系统安全防护能力，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

## 总体安全策略

1. 物理安全策略

（一）机房和办公场地选择在具有防震、防风和防雨等能力的建筑内，机房场地避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

（二）机房出入口安排专人值守，重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

（三）需进入机房的来访人员经过申请和审批流程，并限制和监控其活动范围。

（四）对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

（五）机房内部署基础防护系统和设备，如电子门禁系统、监控报警系统、防雷设备、消防系统、防水监控系统、温湿度控制系统和UPS供电系统。

1. 网络安全策略

（一）保证主要网络设备的业务处理能力具备冗余空间，保证网络各个部分的带宽，以满足业务高峰期需要。

（二）根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

（三）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。

（四）应在网络边界部署访问控制设备，根据实际安全需求设置访问控制策略启用访问控制功能。

（五）对网络系统中的网络设备运行状况、网络流量、用户行为等进行审计，并对审计记录数据进行分析，生成审计报表，且保护审计数据。

（六）能够对非授权联接行为进行检查，准确定出位置，并对其进行有效阻断。

（七）在网络边界处监视攻击行为，记录发生的攻击行为。

（八）在网络边界处监视，并维护恶意代码库的升级和检测系统的更新。

（九）对登录网络设备的用户进行身份标识和鉴别，并设置身份标识和鉴别方式。

1. 主机安全策略

（一）对登录操作系统和数据库系统的用户进行身份标识和鉴别，并设置身份标识和鉴别方式。

（二）启用访问控制功能，设置访问控制策略，依据安全策略控制用户对资源的访问。

（三）对服务器和重要客户端的重要用户行为、系统资源的异常使用和重要系统命令的使用等内容进行安全审计，并对审计记录数据进行分析，生成审计报表，且保护审计数据。

（四）确保操作系统和数据库系统用户的鉴别信息，系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

（五）能够对重要服务器进行入侵的行为和对重要程序的完整性进行检测。

（六）安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库，并支持恶意代码库的统一管理。

1. 应用安全策略

（一）提供专用的登录控制模块对登录用户进行身份标识和鉴别，并设置身份标识和鉴别方式。

（二）提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。

（三）提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计，形成审计记录，并对审计记录数据进行分析，生成审计报表，且保护审计数据。

（四）确保应用系统用户的鉴别信息，系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

（五）具有在请求的情况下为数据原发者或接收者提供数据原发、接收证据的功能。

（六）应用系统须具有软件容错功能，提供数据有效性检验功能和自动保护功能。

1. 数据安全策略

（一）能够检测到系统管理数据、鉴别信息和重要业务数据在传输和存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

（二）采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输和存储保密性。

（三）应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放。

1. 安全管理制度

（一）制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等。

（二）组织相关人员对制定的安全管理制度进行论证和审定。

（三）定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。

1. 安全管理机构

（一）设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。

（二）配备一定数量的系统管理员、网络管理员、安全管理员等。

（三）针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。

（四）加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题。

（五）制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

1. 人员安全管理

（一）严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核。

（二）严格规范人员离岗过程，及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

（三）定期对各个岗位的人员进行安全技能及安全认知的考核，对关键岗位的人员进行全面、严格的安全审查和技能考核。

（四）对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训。

（五）确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。

1. 系统建设管理

（一）明确信息系统的边界和安全保护等级，并组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定。

（二）根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件

（三）制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。

（四）在测试验收前根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

（五）对已定级系统的相关备案材料报相应公安机关备案。

（六）三级及三级以上信息系统运行过程中，至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。

1. 系统运维管理

（一）指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理。

（二）建立资产安全管理制度，对介质和设备的选型、采购、发放、领用、使用、维修、报废等方面规定，并严格执行制度规定。

（三）建立监控和安全管理中心，对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理，形成记录并妥善保存。

（四）建立网络、系统安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期、系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定，并严格执行相关规定。

（五）建立恶意代码防范管理制度，对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定，并严格执行相关规定。

（六）建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。

（七）在统一的应急预案框架下制定不同事件的应急预案，并定期对应急预案进行演练。

## 信息安全总体框架

1. 应在信息安全策略的指导下，通过构建安全管理、安全技术和安全运维三大体系，在既定方针目标的指引下，相互支撑，相互促进，构成实时、动态和持续改进的全生命周期防护体系。
2. 信息安全管理体系应参照《信息安全技术信息系统安全管理要求》（GB/T 20269—2006）、《信息安全技术信息系统安全工程管理要求》（GB/T 20282-2006）和《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2006）等标准规范，建立健全我单位信息安全管理制度体系。
3. 信息安全技术体系应参照《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2006）、《信息安全技术信息系统等级保护安全设计技术要求》（GB/T 25070-2010）等标准规范，在云安全、物理安全、网络安全、主机安全、应用安全和数据安全方面，同步建设和优化信息安全设施，完善我单位信息安全技术体系。
4. 信息安全运维体系应根据《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2006）、《信息技术安全技术信息安全事件管理指南》（GB/Z 20985—2007）和《信息安全技术信息系统灾难恢复规范》（GBT 20988-2007）等标准规范，在信息化办公设备、网络系统、应用系统、主机系统、存储系统等方面完善我单位信息安全运维体系。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

# 临沂市妇幼保健院 信息安全制度管理规定

## 总则

1. 为促进临沂市妇幼保健院信息系统安全制度的制定与管理工作规范化、程序化，提高建章立制质量，结合我单位实际情况，制定本规定。
2. 本规定适用于临沂市妇幼保健院各项信息安全制度的规划、起草、审核、发布、修订和废止等相关活动。
3. 制度制定应当遵循下列原则：

（一）依照法定权限和程序制定原则，法律、法规已经明确规定的原则上不作重复规定。

（二）全面性原则，既包括制度范围的全面性，也包含制度本身的全面性。

（三）准确性原则，规章制度用语准确、简洁，条文内容明确、具体。

（四）可操作性原则，切合我单位信息安全管理的实际需求，制定操作的相关流程，明确相关工作的负责部门和责任岗位。

（五）适度超前原则，推动信息安全管理制度的建设和创新。

（六）协调性原则，避免各项制度相互重复、冲突和遗漏。

## 制度建设组织管理

1. 临沂市妇幼保健院网络安全和信息化领导小组分别依照国家法律法规及单位相关规定、实际情况对所制定的安全管理制度进行论证。
2. 网络安全和信息化领导小组对所提交的安全管理制度进行审核、修订。
3. 临沂市妇幼保健院网络安全和信息化领导小组 负责审批安全管理制度，经审批后方可发布。
4. 网络安全和信息化领导小组负责起草、编写安全管理制度，并收集制度执行中存在的问题，提出完善、修改和废止有关规章制度的建议。

## 制度建设规划与年度计划

1. 信息委制定管理体系的整体规划，根据信息安全需要进行调整。
2. 各部门可临时提议并由网络安全和信息化领导小组决定将某些重要规章制度的制定列入调整计划。

## 制度起草

1. 起草信息安全制度应注意制度之间的协调和衔接，并就制度之间对同一事项的不同具体规定在上报时做出说明。
2. 信息安全制度的起草，按下列步骤进行：

（一）收集资料，掌握有关法律、法规以及其他信息安全的相关规定。

（二）调查研究，提出符合实际情况的制度框架。

（三）撰写草案。

（四）将草案送相关部门征求意见。被征求意见部门或个人应认真填写《信息安全制度征求意见表》。

（五）汇总意见，修改草案，填写《信息安全制度审查表》，提交至网络安全和信息化领导小组

1. 信息安全制度一般应包括下列内容：

（一）目的：清晰简洁说明本制度控制的活动和内容。

（二）适用范围：明确制度所涉及的有关部门（单位）、人员、事项和活动。

（三）职责：规定实施本制度的部门（单位）或人员的责任和权限。

（四）制度规范的内容、要求与程序，对相应安全活动的约束与要求。

（五）相应活动、事项的详细流程。

（六）支持性文件和相关记录、图表，包括与本制度相关的支持性文件、规定，各种应保留的相关记录、表格、单据等。

（七）违反规定的相关责任。

（八）制度的实行时间及有效期限。

1. 信息安全制度结构排列可根据内容多少分为章、条、款、项、目的结构表达，内容简单的也可直接以条的方式表达。章、条的序号用中文数字依次表述；款不编序号；项的序号用中文数字加括号依次表述；目的序号用阿拉伯数字依次表述。

## 审查、论证与批准

1. 网络安全和信息化领导小组对信息安全制度草案进行下列审查：

（一）与我单位现行规章制度是否协调。

（二）草案结构、条款是否符合规章制度的要求和技术规范。

（三）是否切合我单位实际情况，是否体现权责对等原则。

1. 经审查符合要求的，提交信息科进行论证，通过论证后填写《信息安全制度审批表》，提交至网络安全和信息化领导小组进行审批，通过审批后下发实行。
2. 制度采取试行办法，首次颁布的制度试行期为一年，试行期后经修订审批为正式制度，正式制度如需修订则按照修订与废止的相关程序办理。
3. 信息安全制度一经发布生效，相关人员必须严格遵守。

## 修订与废止

1. 为加强信息安全制度管理，制度实施过程中，信息科向各相关部门征求制度执行意见，搜集执行过程中存在的问题，以便修订。
2. 各相关部门在执行信息安全制度过程中，对制度存在的问题应及时记录，填写《信息安全制度修订、废止建议表》提交给信息委。
3. 信息安全制度的修订和废止应由信息委提出，信息委办公会审定。
4. 信息安全制度符合下列情形之一的，应进行修订。

（一）规定事项不能切合现行信息安全方针或实际需要。

（二）规定事项局部已不适用。

（三）制度的局部与国家有关政策法规相抵触。

（四）所涉及的部门名称，与现实不符，或原规定事项主管或执行部门已经变更。

1. 信息安全制度符合下列情形之一者，应予以废止。

（一）规定事项与现行信息安全方针相悖或不符。

（二）与实际情况完全不相切合。

（三）其他项已有新规定并已公布实行。

（四）规定事项已执行完毕，或因情势变迁，已无继续施行必要。

（五）其它情形下，无保留或继续适用必要。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

附件：1.信息安全制度征求意见表

2.信息安全制度审查表

3.安全管理制度审批表

4.安全管理制度修改、废止建议表

附件1

**信息安全制度征求意见表**

|  |  |
| --- | --- |
| 拟定制度名称 |  |
| 拟颁定时间 |  |
| 起草部门 |  |
| 拟实行范围 |  |
| 部门意见或建议 | 部门负责人： |

附件2

**信息安全制度审查表**

|  |  |  |  |
| --- | --- | --- | --- |
| 拟定制度名称 |  | | |
| 起草部门 |  | | |
| 拟稿人 |  | | |
| 审查部门 |  | | |
| 审查部门  修改意见和建议 |  |  |  |
| 审查人 |  | 审查部门负责人 |  |

附件3

**安全管理制度审批表**

|  |  |  |  |
| --- | --- | --- | --- |
| 拟定制度名称 |  | | |
| 起草部门 |  | | |
| 拟稿人 |  | 核稿人 |  |
| 审批部门 |  | | |
| 审批部门意见 |  |  |  |
| 审批人 |  | 审批部门负责人 |  |

附件4

**安全管理制度修改、废止建议表**

|  |  |  |  |
| --- | --- | --- | --- |
| 制度名称 |  | | |
| 印发时间 |  | 印发文号 |  |
| 提请人 |  | 部门负责人 |  |
| 建议内容 |  | | |

# 临沂市妇幼保健院 信息化工作规则

## 总则

1. 为进一步加强临沂市妇幼保健院信息化建设，确保工作协调有序开展，提高建设水平和应用效能，根据我单位信息化建设工作要求，结合实际情况，制定本规则。
2. 本规则所称信息化建设是指以应用现代信息技术为主要手段而进行的信息化建设。主要包括：临沂市妇幼保健院应用系统建设项目，网络、安全、数据库等信息基础设施建设项目，运行维护建设项目以及其他信息化建设项目等。
3. 本规则适用于全系统开展的信息化建设。
4. 信息化建设应坚持统筹规划、统一标准，突出重点、分步实施，整合资源、讲求效益，加强管理、确保安全的原则，坚持需求主导，强化顶层设计，加强基础建设，提升应用效能，实现管理、业务、技术一体化。

## 机构与职责

1. 临沂市妇幼保健院信息化建设工作领导小组办公室是临沂市妇幼保健院信息化建设的领导机构。主要职责是：

（一）贯彻落实政府和上级部门的工作部署，审定信息化建设发展规划和实施方案；

（二）审定我单位重大信息化建设项目并监督实施；

（三）研究解决我单位信息化建设中的重大问题；

（四）指导和协调我单位系统信息化建设工作。

1. 信息科是信息化建设的工作机构。主要职责是：

（一）组织开展信息化建设调研，提出相关措施建议；

（二）组织起草信息化建设总体规划，制订建设计划，提出重点建设项目和专项经费使用建议；

（三）组织实施已确定的重点信息化建设项目；

（四）组织建立信息化建设评价体系，开展绩效考评；

（五）贯彻落实信息标准和技术规范；

（六）负责主管部门及相关单位的日常联系；

（七）承办信息委交办的其他事项。

1. 信息办负责信息化建设业务需求的总体协调，负责信息化建设技术协调和运行维护工作，参与拟订信息化建设规划和标准、规范，参与编制项目建议书，督导项目实施和组织项目验收等。
2. 财务科负责信息化建设项目经费管理和审计，会同信息科组织进行采购。

## 项目和实施

1. 信息科根据信息化建设总体规划，结合各部门提出的信息化建设需求组织立项，经由专家论证后报网络安全和信息化领导小组审批。
2. 信息科根据网络安全和信息化领导小组审定的建设项目，按程序上报有关部门立项、申请经费预算，并组织进行项目采购，确定项目承建单位，签订合同等。
3. 各部门要积极开展信息化需求调研，参与编制项目建设方案，并全程参与项目建设。
4. 项目实施按照国家有关规定，通过招标确定具有相应资质的工程监理单位，全程进行监理。
5. 项目建成后由信息科组织专家及有关部门按照国家法律法规规定的方法及程序进行验收。未经验收或验收不合格的项目，不得交付使用。
6. 各部门负责项目建成后的推广应用。信息科负责协调信息化软、硬件的运行维护工作，细化完善各项管理制度，制定应急预警方案，确保应用系统和网络安全稳定运行。

## 资金和资产

1. 信息化项目建设和运行维护经费列入部门预算，并且专款专用，不得挤占挪用。
2. 项目建设形成的国有资产，要及时办理资产登记相关手续，纳入临沂市妇幼保健院国有资产统一管理。
3. 项目完成后形成的全部工作成果及相关知识产权，除有合同约定外，归临沂市妇幼保健院所有。

## 附则

1. 本办法由临沂市妇幼保健院负责解释，信息化工作中其他重大问题，由临沂市妇幼保健院网络安全和信息化领导小组研究确定。
2. 本规定自发布之日起施行。

# 临沂市妇幼保健院 信息系统“三员”管理规定

## 总则

1. 为加强和规范临沂市妇幼保健院信息系统管理，依据国家安全有关规定和技术要求，制定本规定。
2. 本规定所称“三员”指系统管理员、安全管理员、安全审计员，分别负责系统运行、系统安全和安全审计工作：

（一）系统管理员主要负责系统日常运行维护工作；

（二）安全管理员主要负责系统日常安全管理工作；

（三）安全审计员主要负责对系统管理员、安全管理员的操作行为进行审计跟踪和监督检查，以及发现违规行为，并定期向系统安全管理机构汇报相关情况。

## 系统管理员职责

1. 系统管理员分为网络管理员、应用系统管理员、终端设备管理员。

网络管理员职责：

（一）合理规划网络、主机、存储架构，并部署。

（二）服务器、网络设备等日常管理和维护。

（三）定期搜集、统计、报送网络运行和管理情况。

（四）接受网络和主机事件报告，并及时处理。

应用系统管理员职责：

（一）应用系统结构和性能优化，消除性能瓶颈；

（二）应用系统日常管理和维护，故障处理。

（三）定期搜集、统计、报送应用系统安全管理情况。

（四）定期备份应用系统数据，并在事件发生时及时恢复。

（五）接受软件和系统事件报告，并及时处理。

终端设备管理员职责：

（一）终端计算机设备配置、维护、管理。

（二）终端操作系统及应用系统客户端状态监控。

（三）定期对系统终端进行病毒扫描和病毒库更新。

（四）终端操作系统及应用系统客户端软件升级、补丁安装等。

（五）定期报送终端使用管理情况和异常事件统计信息。

（六）受理来自终端设备用户的故障报告，并及时处理。

（七）其他信息化办公设备的配置、维护、管理。

## 安全管理员职责

1. 制定并实施信息系统安全策略。
2. 安全设备和安全软件日常管理和维护，包括升级更新、故障处理。
3. 监控安全设备和安全软件运行状态，定期审查、维护权限列表，并对日志进行分析，及时发现安全隐患并妥善处理。
4. 系统管理员账户、权限管理，应用系统管理员权限管理，定期审查、维护权限列表，并对日志进行分析，及时发现安全隐患并妥善处理。
5. 定期报送安全管理情况和异常事件统计信息。
6. 信息系统安全事件处理。

## 安全审计员职责

1. 对系统各用户名和口令管理与变更记录进行审计。
2. 对系统安全策略执行情况进行审计。
3. 定期备份安全审计日志。
4. 监督系统管理员和安全管理员对事件（包括报送事件）处理过程。
5. 定期对系统管理员和安全管理员工作和相关文档进行检查，形成审计记录，并向主管领导报送，发现异常情况及时报告。
6. 对审计的安全事件进行及时处理，并对处理结果进行记录。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

# 临沂市妇幼保健院 信息系统安全检查规定

## 总则

1. 为加强和规范临沂市妇幼保健院信息系统安全监督检查工作，保障信息系统安全稳定运行，根据国家信息安全等级保护有关规定和我单位信息系统安全有关管理规定制定本规定。
2. 本规定适用于我单位信息系统建设、使用和运维管理中安全监督检查工作。
3. 网络安全和信息化领导小组办公室负责组织监督检查工作：人员管理、教育培训等相关检查由信息科具体执行；安全技术相关检查由信息科具体执行。

## 实施细则

1. 检查内容主要包括信息系统安全技术措施有效性和安全管理制度执行情况。
2. 专项检查应填写检查登记表，检查结果汇总后报信息科，发现问题及时整改。
3. 定期对系统进行安全性能检测，确保系统安全稳定运行。
4. 系统安全性能检测由系统管理员、安全管理员和安全审计员共同完成。
5. 检查人员应利用漏洞扫描等工具对整个系统进行安全检查，对网络系统、应用系统、主机系统、用户终端进行安全分析，发现漏洞或安全隐患及时整改。
6. 及时记录安全检查和整改操作情况。

（一）网络设备、服务器安全性能检查由网络管理员负责，安全设备安全性能检查由安全管理员负责，并根据检查情况填写《网络系统安全性能检测表》、《系统安全漏洞检测记录表》、《主机和存储安全性能检查表》。

（二）应用系统安全性能检测由应用系统管理员负责，并根据检测情况填写《应用系统安全性能检测表》。

（三）用户终端安全检测由终端设备管理员负责，并根据检测情况填写《终端安全性能检测表》。

1. 安全管理员定期汇总各类安全性能检测表和整改情况，形成《系统安全性能检测汇总表》后上报我单位领导。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

附件：1.系统安全漏洞检测记录表

2.网络系统安全性能检测表

3.应用系统安全性能检测表

4.主机和存储安全性能检测表

5.终端安全性能检测表

6.系统安全性能检测汇总表

附件1

**系统安全漏洞检测记录表**

|  |  |  |  |
| --- | --- | --- | --- |
| 扫描日期 |  | 操作人员 |  |
| 扫描部门 | 漏洞主机IP | 漏洞类型 | 备注 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：“漏洞类型”填写漏洞的具体类型，例如：冲击波漏洞、空连接漏洞、数据库漏洞、弱口令等。

附件2

**网络系统安全性能检测表**

|  |  |  |  |
| --- | --- | --- | --- |
| 检测人 |  | 检测时间 |  |
| 设备类型 | 检测内容 | 检测结果 | 备注 |
| 网络设备 | 1. 运行状态是否正常 |  |  |
| 1. 管理员口令是否满足要求 |  |  |
| 1. 不必要端口是否已关闭 |  |  |
| 1. Vlan划分是否合理有效 |  |  |
| 1. ACL是否合理有效 |  |  |
| 1. 是否设置流量控制策略 |  |  |
| 1. 是否保存日志并定期审查 |  |  |
| 1. 是否有未处理报警日志 |  |  |
| 安全设备 | 1. 运行状态是否正常 |  |  |
| 1. 管理员口令是否满足要求 |  |  |
| 1. 特征库是否及时更新 |  |  |
| 1. 访问控制策略是否合理有效 |  |  |
| 1. 安全策略是否合理有效 |  |  |
| 1. 是否保存日志并定期审查 |  |  |
| 1. 是否有未处理报警日志 |  |  |

附件3

**应用系统安全性能检测表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 检测人 |  | 系统名称 |  | 检测时间 |  |
| 设备类型 | 检测内容 | | | 检测结果 | 备注 |
| 应用系统 | 1. 运行状态是否正常 | | |  |  |
| 1. 用户口令是否有效 | | |  |  |
| 1. 是否划分三员 | | |  |  |
| 1. 用户权限划分是否符合最小授权原则 | | |  |  |
| 1. 访问控制策略是否有效 | | |  |  |
| 1. 非合规用户是否及时注销 | | |  |  |
| 1. 用户增加、删除是否有记录 | | |  |  |
| 1. 用户重鉴别策略是否有效 | | |  |  |
| 1. 是否有未处理报警日志 | | |  |  |

附件4

**主机和存储安全性能检测表**

|  |  |  |  |
| --- | --- | --- | --- |
| 检测人 |  | 检测时间 |  |
| 设备类型 | 检测内容 | 检测结果 | 备注 |
| 主机和存储 | 1. 运行状态是否正常 |  |  |
| 1. 登陆口令是否满足要求 |  |  |
| 1. 是否设置登录失败处理策略 |  |  |
| 1. 系统补丁是否更新 |  |  |
| 1. 防病毒软件是否更新 |  |  |
| 1. 是否有隐藏进程、异常监听等 |  |  |
| 1. 无用服务端口是否已关闭 |  |  |
| 1. 是否存在多余账户 |  |  |
| 1. 是否保存日志并定期审查 |  |  |
| 1. 是否有未处理报警日志 |  |  |

附件5

**终端安全性能检测表**

|  |  |  |  |
| --- | --- | --- | --- |
| 检测人 |  | 检测时间 |  |
| 设备类型 | 检测内容 | 检测结果 | 备注 |
| 终端 | 1. 是否有非法外联痕迹（内网） |  |  |
| 1. 是否有敏感信息（外网） |  |  |
| 1. 是否设置登录失败处理策略 |  |  |
| 1. 是否有恶意软件或病毒 |  |  |
| 1. 操作系统口令是否满足要求 |  |  |
| 1. 操作系统补丁是否更新 |  |  |
| 1. 重要终端是否设置审计策略 |  |  |
| 1. 防病毒软件是否更新 |  |  |
| 1. 是否有隐藏进程、异常监听等 |  |  |
| 1. 是否有未处理报警日志 |  |  |

附件6

**系统安全性能检测汇总表**

|  |  |
| --- | --- |
| 检测内容  （可附表） |  |
| 检测情况 | 检查人签字：  年月日 |
| 信息科意见 | 领导签字  年月日 |
| 整改情况 | 签字  时间 |
| 备注： | |

# 临沂市妇幼保健院 人员信息安全管理规定

## 总则

1. 为加强临沂市妇幼保健院人员安全管理，按照国家信息安全等级保护相关制度和标准要求，结合工作实际，制定本规定。
2. 本规定适用于临沂市妇幼保健院内部工作人员和外部相关人员的管理。
3. 临沂市妇幼保健院工作人员有维护我单位信息安全的责任和保守工作秘密的义务，应自觉遵守信息安全相关的法规和制度，接受安全教育和监督。

## 内部工作人员管理

1. 任用信息化管理人员，要依据信息安全相关标准要求，进行严格审查，包括录用人员的身份、背景、专业资格和资质等进行审查和核实。
2. 关键岗位的人员应从内部人员中选拔，并签署岗位安全协议，不符合要求的人员应及时调离岗位。
3. 内部工作人员工作活动场所和工作信息接触范围应当被限制在完成本职工作所需的最小范围内。
4. 信息科应定期组织对内部工作人员进行信息安全教育、培训和考核。
5. 内部工作人员办理离岗离职手续时，须承诺保密义务后方可离岗。即时取消其一切授权，注销用户账号，收回机构提供的各种身份证件、钥匙、软硬件设备等。

## 外部相关人员管理

1. 须向外部人员明确本单位的相关规定，使其清楚自身的责任和安全违规的后果。
2. 对重要安全区域采取隔离控制，禁止未授权的外部人员出入。
3. 禁止外部人员携带与工作无关的具有录音、录像、拍照、信息存储等功能的设备进入重要安全区域。
4. 对所有进入重要安全区域进行维修、服务、参观等的外部人员进行全程旁站陪同。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

附件：

**员工保密协议**

甲方：临沂市妇幼保健院

乙方： 身份证号码：

鉴于乙方在甲方任职，工作中将接触并知悉甲方工作秘密。为了有效保护甲方的工作秘密，明确乙方的保密义务，根据有关法律法规，甲、乙双方本着平等、自愿、公平和诚实信用的原则签订本保密协议。

**第一条**本协议提及的“工作秘密”指，除国家秘密以外的，在工作中不得公开扩散的事项；一旦泄露，会给本单位的工作带来被动和损害。

**第二条**按照法律规定，乙方在甲方任职期间，因履行职务、承担甲方交给的任务或者主要是利用甲方的物质技术条件、业务信息等产生的工作秘密归甲方所有。

一切记录着甲方工作秘密的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、仪器以及其他任何形式的载体，属甲方资产，均归甲方所有。

**第三条**乙方在甲方任职期间，由于工作关系，知悉甲方的工作秘密，因此乙方应履行以下义务：

（1）遵守甲方制定的任何成文的和其他形式的保密规章、制度，履行与其工作岗位相应的保密职责。甲方的保密规章、制度没有规定或者规定不明确之处，乙方亦应本着谨慎、诚实的态度，采取必要、合理的措施，保护甲方工作秘密。

（2）未经甲方同意，不以泄露、告知、公布、发布、出版、传授或者其他方式使任何第三方（包括按照保密规章、制度规定不得知悉该项秘密的甲方其他职员）知悉甲方的工作秘密，也不在履行职务之外使用、许可或转让上述工作秘密；不非法使用任何属于他人的工作秘密。

（3）离职时，应将本协议第三条所述的甲方资产归还甲方，并将记载于自有载体上的工作秘密立即删除；不能删除的，应当立即销毁或无条件移交给甲方，同时向甲方书面保证已经全部归还或销毁上述资料及其他载体。

**第四条**无论乙方因何种原因离职，乙方离职之后仍对其在甲方任职期间接触、知悉的甲方工作秘密承担如同任职期间一样的保密义务。

**第五条**乙方离职后承担保密义务的期限为下列第种（没有做出选择的，视为无限期保密）：

（A）无限期保密，直至甲方宣布解密或者秘密信息实际上已经公开；

（B）有限期保密，保密期限自离职之日起，至 年 月 日止。

**第六条**乙方若违反本协议约定保密义务，甲方有权采取以下措施：

1.根据乙方所造成的后果轻重分别采取调离岗位、解除劳动关系等处置措施。

2.乙方违约行为构成犯罪的，提请有关机关依法追究乙方刑事责任。

3.乙方违约行为造成甲方经济损失的，甲方在采取上述处理措施的同时，有权要求乙方对实际损失进行赔偿。

**第七条** 双方因履行本协议发生争议的，可向甲方所在地劳动仲裁机构申请仲裁或向人民法院提起诉讼。

**第八条** 双方一致同意对本协议补充、修改时，以书面方式签订补充或变更协议。

**第九条** 双方确认，在签署本协议前已仔细审阅过协议的内容，并完全了解协议各条款的法律含义。

**第十条** 本协议一式两份，甲乙双方各执一份，具有同等法律效力，自甲方签字盖章、乙方签字后生效。

甲方（盖章）： 乙方（签名）：

年　　月　　日 年　　月　　日

# 临沂市妇幼保健院 信息安全教育和培训管理规定

## 总则

1. 为加强临沂市妇幼保健院信息安全管理，切实提高相关人员对信息安全的认识和岗位安全技能，制定本规定。
2. 本规定适用于临沂市妇幼保健院所有人员信息安全教育和培训管理工作。

## 信息安全教育、培训、考核

1. 信息安全教育应坚持以人为本、预防为主的原则，结合实际工作，分层次、有重点、有针对性地进行。
2. 信息科组织、实施关于全员的信息安全培训，特别是信息安全意识、政策和基本知识普及方面的培训；信息科组织、实施关于技术人员及信息安全分管领导的信息安全培训，主要包括信息安全技术方面的培训。
3. 信息安全培训内容应包括信息安全政策法规、意识、岗位职责、基础知识、操作规程等。
4. 信息安全教育培训应包括以下三个环节：

1.上岗前安全教育；

2.在岗安全教育；

3.离岗前安全教育。

1. 信息安全教育所采用的形式包括举办安全知识讲座、报告会、座谈会，观看安全教育片，参观安全教育展览，以及参加信息安全演练等。
2. 临时工作人员、聘用人员、借用人员，以及实习人员等，都应在工作前接受信息安全教育培训。
3. 我单位对信息安全教育培训情况进行详细记录，包括人员、时间、内容、考核等。
4. 培训组织机构应对培训对象进行考核，考核内容包括信息安全知识、安全技能、操作行为等。
5. 我单位各部门工作人员应自觉接受安全教育和安全监督检查。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

# 临沂市妇幼保健院 机房管理规定

## 总则

1. 本规定主要用于信息化管理人员开展机房内主机、存储、网络设备管理工作。

## 机房管理

1. 进入机房人员严禁携带影响和威胁机房正常运行的物品，包括易燃易爆物品、强磁物品、放射性物品、食品、饮料。
2. 为保持机房环境整洁，进入机房须更换拖鞋或戴上鞋套。严禁乱扔废弃物、严禁吸烟、喧哗。
3. 操作人员严禁在主机和监控终端上进行工作范围以外的操作，如学习、娱乐、上网等。
4. 严禁携带与工作无关的具有录音、录像、拍照、信息存储等功能的设备进入机房，以防拷贝、传输、泄露机房内数据。
5. 外来人员因参观或设备检修、维护需进出机房内相关设备时，须经信息科领导批准，并由信息科相关人员全程陪同，无特殊情况不得进入机房。
6. 信息科相关人员收到机房管理人员协助需求信息时，应协助机房管理人员尽快排除故障。
7. 网络管理员应定期对机房内本局设备进行维护。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

# 临沂市妇幼保健院 门户网站管理办法

## 总则

1. 为充分发挥临沂市妇幼保健院门户网站的作用，建立规范的信息采集、报送、审核、发布、更新机制，保证信息发布的准确、及时、有效，依据有关规定，结合我单位实际情况，制订本办法。
2. 本办法所称信息是指在门户网站上对外发布的文字、数据、图片、音像、链接以及其他形式的信息。
3. 信息科是门户网站的综合管理机构，负责门户网站工作的指导、协调和监管。
4. 信息科是门户网站的运维机构，具体负责技术支持、运行环境维护管理和网站安全等工作。
5. 各部门分别负责与其工作职责相关的信息采集、报送、审核和发布。

## 信息采集与报送

1. 门户网站设置了主要栏目,分别是新闻、医院介绍、咨询等。
2. 宣传科负责门户网站新闻信息采集及上传，按门户网站所设栏目要求，通过门户网站信息发布管理平台及时准确地报送、发布和管理信息。

## 信息审核与发布

1. 宣传科建立信息发布审核制度，拟发布的信息经宣传科部门负责人及分管领导审核确认后报送或发布。
2. 信息审核要点：

（一）是否属于涉密信息；

（二）是否属于敏感信息；

（三）信息中的统计数据是否准确、及时；

（四）发布的信息是否与承担的职责相符。

1. “在线培训”、“公众留言”、“在线上报”、“举报投诉”等互动类栏目信息，按照职责分工由各相关部门及时处理和反馈。
2. 各科室如需利用门户网站发布其他类信息（如新闻信息等），须经宣传科审核并报领导审批后处理。
3. 各科室如需变更门户网站栏目，须经宣传科审核并报领导审批后处理。

## 信息管理

1. 不得发布违反国家法律法规的信息，不得发布与党的路线、方针、政策相违背的信息。不得在网上从事危害国家安全等犯罪活动。
2. 严禁发布涉密信息。
3. 不得制作、复制和传播各类不健康信息，不得发布虚假信息。
4. 信息内容必须真实、准确、完整。发布前必须认真校对，发现问题应及时更正。
5. 信息发布单位应加强本单位信息动态的日常管理，一旦发现有超时、过期、失效的网上信息，应及时调整、更新、撤销。

## 安全管理

1. 宣传科门户网站信息发布管理平台账号密码应定期或根据情况及时更新，避免泄露，确保门户网站安全。
2. 信息科负责网站安全工作，要加强安全技术和手段的应用，完善安全基础设施，制定完备的安全策略和应急策略，提高应对网络攻击、病毒入侵、系统故障等风险的安全防范和应急处置能力，确保及时解决突发情况。

## 附则

1. 对违反本办法导致信息发布工作出现失误的部门或个人，给予批评教育。对造成严重不良后果的，要追究相关责任。
2. 本办法由临沂市妇幼保健院负责解释。
3. 本办法自印发之日起施行。

# 临沂市妇幼保健院 信息系统运行维护管理办法

## 总则

1. 为进一步加强和深化临沂市妇幼保健院信息系统运行维护管理工作，明确工作内容，强化工作职责，提高工作效率，确保我单位各类信息系统稳定、安全、高效运行，根据国家和行业有关技术标准，结合我单位实际工作情况，制定本办法。
2. 运维管理工作的主要管理对象是信息化办公设备、网络系统、主机、存储、应用系统和数据等。
3. 信息科作为运行维护体系的管理部门，负责运行维护体系的规划、建设和管理。

## 信息化办公设备运维管理

1. 该项工作由信息科硬件组负责，运维内容包括：

（一）终端操作系统安装、升级、故障诊断和处理等。

（二）信息科提供的或授权的应用软件、防病毒软件等安装、配置和升级等。

（三）终端、打印机、扫描仪等硬件设备的安装、配置、网络调试、维修等。

## 网络系统运维管理

1. 该项工作由网络管理员负责，运维内容包括：

（一）广域网、局域网、通讯线路管理，布线系统的正常使用和维护。

（二）网络设备的配置，并对网络设备的配置进行维护管理和日志管理。

（三）网管系统的运维管理，利用网管软件对网络流量和网络性能进行监控、分析和管理。

（四）对网络运行过程中出现的故障和性能问题进行监控和解决。

## 主机、存储系统运维管理

1. 该项工作由系统管理员负责，运维内容包括：

（一）主机运行情况监控分析及故障处理。

（二）主机操作系统的安装、升级和维护。

（三）主机操作系统相关配置策略的制定、部署和备份等。

（三）存储系统运行情况监控分析及故障处理。

（四）存储系统软件的安装、升级和维护。

（五）存储系统相关配置策略的制定、部署和备份等。

## 应用系统、数据运维管理

1. 应用系统运维。该工作由应用系统管理员和安全管理员负责，运维内容包括：

（一）应用系统管理员负责应用系统软件的安装、升级、维护。

（二）应用系统管理员负责应用系统状态检查和日志检查。

（三）应用系统管理员负责应用系统的参数配置、变更及配置备份。

（四）应用系统管理员负责应用程序的数据和代码调整。

（五）应用系统管理员负责应用系统的用户的增加、删除和修改工作。

（六）应用系统管理员负责制定和实施应用系统备份和恢复策略。

（七）安全管理员负责管理员用户权限管理。

1. 数据运维。该项工作由应用系统管理员负责，运维内容包括：

（一）数据库的安装、升级和维护，负责数据库的参数调整。

（二）数据库的存储空间分配、备份、用户管理和日志检查等工作。

（三）数据库系统的性能监控，配合各应用系统管理员做好系统优化。

（四）对数据库系统制定和实施备份与恢复策略。

（五）对数据库系统运行过程中发生的问题进行及时处理和解决。

（六）负责对其他类型数据（包括文本、图片、视频、音频等）进行监控、备份恢复、问题处理。

## 驻场运维人员管理

1. 该项工作由信息科负责，现驻场人员为佳和电子工作人员，负责打印机维护，内容包括：

（一）负责培训运维人员工作区域的安全管理规定。

（二）负责对运维人员进行信息安全管理制度培训，使其明确重要操作、重要变更等相关流程，并监督执行。

（三）负责与运维人员签署保密协议。

（四）负责运维人员日常管理，如考勤、工作完成情况等。

# 临沂市妇幼保健院 信息系统设备管理规定

## 总则

1. 为更好的利用临沂市妇幼保健院信息系统设备，实行设备统一管理，根据国家有关安全管理规定和技术要求，结合我单位工作实际，制定本制度。
2. 本制度中规定的信息系统设备主要指与临沂市妇幼保健院信息系统相关的软、硬件设备，本制度适用于临沂市妇幼保健院信息系统设备的使用和管理工作，包括设备的购置、安装、使用、维修、报废等设备管理的各个环节。
3. 临沂市妇幼保健院配合办公室对信息系统设备进行管理。

## 设备选型、购置与安装

1. 信息系统设备的选择应该优先选择国产设备，信息安全类产品的选择应符合[信息安全等级保护管理办法(公通字[2007]43号)](http://www.baidu.com/link?url=rJyLxXeYvLA0cfktQSEXy8__1EkzwUsKFO07oCFyratfAnWO40FjcdI94tisSlcH0DgmaYAcp9g34tkcN5iKIX3pia_TL5oj0sNTp8ik1e7" \t "_blank)等相关要求，密码产品采购和使用应符合国家密码主管部门的要求。
2. 信息系统设备的购置应符合临沂市妇幼保健院固定资产管理办法相关规定。
3. 所购信息系统设备由信息科归口管理，统一标识、统一安装。
4. 软、硬件设备安装配置完毕后先进入试运行阶段，试运行时间的长短可根据需要自行确定，软、硬件设备通过试运行后，方可投入正式运行。

## 设备登记与使用

1. 对所有信息系统设备的购置、移交、使用、维护、维修、报废等进行登记，根据所承载的信息和软件的重要程度对信息系统设备进行标识和分类,并认真做好登记的检查工作，规范信息系统设备管理工作。所购信息系统设备交付时，应按照相关规定对信息系统设备进行验收。
2. 信息科负责信息系统设备的使用和维护，信息系统设备操作和使用过程中应严格遵守操作规程和相关安全规定。
3. 信息系统设备须指定安全责任人，落实安全责任，明确责任主体。
4. 信息科应对信息系统设备的基本信息、领用归还、运行起止时间及运行状况进行登记，建立设备管理台账。
5. 因工作需要携带重要信息系统设备外出的，应填报《携带重要信息系统设备外出登记表》，经审批后方可带出。因工作需要携带重要信息系统设备出境的，应当按照有关安全规定办理批准和携带手续。
6. 信息系统设备使用者负责进行信息系统设备的日常保洁和维护，保证信息系统设备处于最佳状态。一旦出现故障，信息系统设备使用者无法及时解决时，应立即联系信息科处理。

## 设备维修、报废与销毁管理

1. 信息系统设备出现故障需进行维修时，原则上由信息科进行维修。确需外来维修人员上门维修，应与维修单位签定安全承诺书，由信息科安排专人陪同。
2. 信息系统设备送外维修须经我单位领导审批同意，并采取数据保护措施，如加密、备份等措施。
3. 维修过程中需更换重要存储部件的，必须将替换下的旧件带回统一销毁，严禁将旧件抵价或随意丢弃。
4. 重要信息系统设备到达使用期限或因故障不能恢复，应对设备现状进行详细登记，提出处理意见，经信息科审核后报财务科作报废处理。
5. 需销毁的重要存储部件应按照国家相关规定进行处置。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

附件一

**携带重要信息系统设备外出申请表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 注意事项 | 1. 要采取可靠的安全措施，确保信息系统资产的安全。 2. 信息系统资产始终处于携带人的有效控制之下，做到不离人。 3. 两人以上信息系统资产要明确主次责任。 4. 禁止将信息系统资产带到不具有安全条件的公共场所（如医院、火车、飞机、轮船等地）阅办。 5. 禁止携带信息系统资产外出旅游、探亲访友、参加外事活动。  携带人签字：日期： | | | | | | |
| 携带人 |  | 职务 | |  | 部门 | |  |
| 携带设备名称 |  | | 设备编号 | | |  | |
| 携带外出时间 | 年月日至年月日 | | | | | | |
| 携带外出原因 |  | | | | | | |
| 携带设备内重要  文件名称 |  | | | | | | |
| 信息科签字 | 年月日 | | | | | | |
| 归还人 |  | | | 归还时间 |  | | |

# 临沂市妇幼保健院 移动存储介质管理规定

## 总则

1. 为确保临沂市妇幼保健院信息安全，加强和规范我单位移动存储介质的管理，根据有关安全规定和技术要求，结合工作实际，特制定本规定。
2. 本规定适用于临沂市妇幼保健院对移动存储介质的购买、配发、使用、维修、报废和销毁等各环节的管理。
3. 本规定所称的移动存储介质是指U盘、移动硬盘、光盘、软盘、磁带、存储卡、录音笔等可与计算机交互信息的便携式电、磁、光信息载体。
4. 移动存储介质实行统一管理，安全使用管理由临沂市妇幼保健院具体负责。

## 存储介质使用

1. 我单位现移动存储介质策略为内网电脑禁止插入，通过联软内网管理软件实行管控。
2. 特殊情况如心电图机器、检验科仪器数据备份、CT室数据备份所用移动存储需提交内网存储介质开通申请，且需专用，并填写存储介质安全保证书。
3. 报废处理的存储介质在其他信息系统内重新使用前，应进行信息消除处理，信息消除处理时所采取的信息消除技术、设备和措施应符合国家相关规定。
4. 携带重要存储介质外出应进行必要的信息消除处理，以保证介质上只存有与本次外出相关的资料。
5. 移动存储介质使用人应严格遵守移动存储介质管理规定，由个人原因造成的移动存储介质丢失、信息泄漏等事件应由使用人承担相应责任。

## 介质保存

1. 移动存储介质保存必须符合防火、防水、防震、防潮、防腐蚀、防鼠害、防虫蛀、防静电、防电磁辐射的安全要求。
2. 重要移动存储介质应备份，保存应当选择安全级别高的场所；需要归档的存储介质，应当按照有关规定归档。
3. 临沂市妇幼保健院定期对存储介质进行清查、核对，发现问题及时向相关领导报告。
4. 移动存储介质的使用人员离岗、离职前，应当将所使用的存储介质全部清退，并办理移交手续。

## 介质接入

1. 工作移动存储介质只能在工作计算机上使用，禁止在非工作计算机上使用。
2. 私人使用的存储介质未经我单位检查核准，禁止在工作计算机等设备上使用。私人使用的存储介质禁止存储工作信息。

## 介质维修、报废和销毁管理

1. 移动存储介质的维修、维护，由临沂市妇幼保健院统一管理。
2. 当移动存储介质需要报废时，由信息科按照相关规定进行销毁。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施。

附件：

1.介质维修记录表

2.介质报废记录表

3.携带介质外出登记表

附件2

**介质维修记录表**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **介质**  **名称** | **介质**  **编号** | **申请**  **部门** | **申请人** | **维修**  **时间** | **维修**  **地点** | **维修人** | **陪同人** | **故障**  **原因** | **排除**  **方法** | **返回**  **情况** | **经办人** | **审批人** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

附件3

**介质报废记录表**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **介质名称** | **介质编号** | **申请部门** | **申请人** | **报废时间** | **最终去向** | **信息处理**  **情况** | **报废过程** | **经办人** | **审批人** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

附件4

**携带介质外出登记表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 携带人 |  | 携带人职位 |  | 部门 |  | |
| 携带外出原因及文件去向 |  | | | | | |
| 携带介质名称 |  | 介质编号 |  | | | |
| 携带外出时间 | 年月日至年月日 | | | | | |
| 介质内文件名称 |  | | | 文件重要性 | |  |
| 部门负责人签字 | 年月日 | | | | | |
| 审核人签字 | 年月日 | | | | | |
| 带回文件名称 |  | 带回文件重要性 |  | 带回文件去向 |  | |
| 信息消除情况 |  | | | | | |
| 经办人签字 | 年月日 | | | | | |

# 临沂市妇幼保健院信息系统 恶意代码防范与软件补丁分发管理规定

## 总则

1. 为进一步加强和规范临沂市妇幼保健院信息系统恶意代码防范与软件补丁分发管理工作，防范安全风险，保障系统安全稳定运行，根据信息系统安全有关管理规定，制定本规定。
2. 本规定适用于临沂市妇幼保健院信息系统的病毒、木马等恶意代码的防范，以及软件的补丁分发管理工作。
3. 临沂市妇幼保健院负责信息系统恶意代码防范与软件补丁分发的相关管理工作。

## 恶意代码防范管理

1. 临沂市妇幼保健院安全管理员和系统管理员共同负责信息系统恶意代码防范工作：规划防范策略，经审定后组织实施；及时关注恶意代码预警信息，妥善调整防护策略；检测、记录所采取的防范操作。
2. 所购买和使用的恶意代码防范产品必须是经过国家相关主管部门认可、认证的产品。
3. 临沂市妇幼保健院所有计算机必须安装信息科指定的杀毒软件，不得私自卸载。
4. 定期对恶意代码库进行升级，恶意代码库加载工作由安全管理员负责。
5. 临沂市妇幼保健院工作人员遇到恶意代码发作，应立即断开网络连接，及时清除恶意代码；无法清除的由临沂市妇幼保健院辅助处理。彻底解决后，方可重新入网。
6. 所有移动存储介质在使用前，都必须进行恶意代码查杀工作，确保其无恶意代码。需使用的各种软件，安装前应进行恶意代码查杀。
7. 重要资料除在非系统盘存储外，还应利用移动存储介质备份，以防遭恶意代码破坏而遗失。信息的备份及其介质管理按有关规定执行。
8. 临沂市妇幼保健院安全审计员负责对恶意代码防范措施的落实情况进行监督检查。

## 安全漏洞与补丁安全管理

1. 临沂市妇幼保健院系统管理员和安全管理员应及时掌握信息系统安全漏洞预警信息，并采取加载相关补丁、关闭系统端口、调整防火墙防护策略等措施提高系统安全防护能力。
2. 紧急补丁必须在一天内、重要补丁必须在一周内、一般补丁必须在两周内完成补丁的测试、发布和加载工作。
3. 补丁加载之前必须经过恶意代码查杀和测试，做好应用系统和关键数据的备份工作。
4. 补丁加载工作由系统管理员负责操作，遵守补丁加载流程。
5. 建立健全补丁分发管理机制，对我单位信息系统补丁使用情况进行实时监管。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

附件：

1.软件安装记录表

附件一

**软件安装记录表**

|  |  |  |  |
| --- | --- | --- | --- |
| 软件类别 |  | 软件提供单位 |  |
| 软件名称 |  | 软件使用单位 |  |
| 安装时间 |  | 安装人员 |  |
| 安装位置 |  | 使用范围 |  |
| 基本功能 |  | | |
| 临沂市妇幼保健院测试意见 | 签字（盖章）：  年月日 | | |
| 审批意见 | 签字（盖章）：  年月日 | | |
| 备注 |  | | |

注：信息系统中未安装使用过的软件，需要信息科进行测试并且提供测试意见。

# 临沂市妇幼保健院 信息系统安全审计管理规定

## 总则

1. 为进一步加强和规范临沂市妇幼保健院信息系统安全审计管理工作，特制定本规定。
2. 本规定适用于临沂市妇幼保健院信息系统的安全审计管理。
3. 安全审计主要指记录和跟踪信息系统状态变化，监控、记录对程序和文件的使用以及对文件的处理过程等。
4. 安全审计管理指利用信息系统审计方法，对信息系统进行详尽审计，对于发现的安全问题，及时通知安全管理员调整安全策略，从而达到降低安全风险的目的。

## 审计管理

1. 由安全审计员定期对信息系统的服务器、网络设备、安全设备、存储设备、应用系统进行安全审计，并形成审计记录。
2. 信息系统日志内容应提供足够的信息，以便确定事件的来源和结果，日志包括以下内容：事件发生的时间、地点、类型、主体、客体和结果（成功或失败）等。
3. 信息系统日志存储：

（一）有充足的日志存储空间，防止由于存储空间不足造成日志丢失。

（二）具有存储空间阀值设置功能，当存储空间达到阀值时及时进行告警。

（三）审计系统出现异常时，保证存储的日志不被破坏。

（四）日志至少保存一年。

（五）日志存储空间将满时，覆盖最早存储的日志数据或转存日志数据。

1. 信息系统日志的查阅及保护：

（一）安全审计员定期对日志进行审查或分析，发现可疑行为及违规操作后采取相应的措施，并及时报告。

（二）提供对日志的统计、查询功能，包括按时间范围、主客体身份、行为类型等条件进行检索查询。

（三）安全审计员调阅、备份、删除日志，必须进行记录。

（四）对审计系统和审计信息进行访问控制，保证日志不被篡改、伪造和非授权删除。

## 附则

1. 本规定由临沂市妇幼保健院负责解释。
2. 本规定自发布之日起施行。

# 临沂市妇幼保健院 信息系统数据备份与恢复管理规定

## 总则

第一条 为加强临沂市妇幼保健院信息系统的数据备份与恢复管理工作，防止信息数据丢失，确保应用系统的安全稳定运行和历史数据的保存，特制定本规定。

第二条 本规定适用于临沂市妇幼保健院数据管理。

## 职责与分工

第三条 数据库管理员负责临沂市妇幼保健院信息系统的数据备份与恢复管理工作。

## 数据备份方式

第四条 数据备份根据系统情况和备份内容，采用不同的备份方式：

1、完全备份：对备份的内容进行整体备份。

2、增量备份：仅备份相对于上一次备份后新增加和修改过的数据。

3、差分备份：仅备份相对于上一次完全备份之后新增加和修改过的数据。

4、按需备份：仅备份应用系统需要的部分数据。

第五条 我院现主要采用完全备份方式，具体备份方式为数据库同时写两份数据至双活存储，另异地机房有一份数据备份，另每日上班后，数据库操作员手动检查备份数据完成情况，并将所备份数据转移至专用存储，专用存储存放在远离磁性、辐射性的安全环境。

## 数据备份与恢复的管理

第六条 应建立健全数据备份与恢复的管理制度，明确备份与恢复的工作流程，完善数据备份与恢复的技术措施，采取有效的安全运行技术方案，保证数据安全。

第七条 应根据各种数据的重要性及其容量，制订数据备份与恢复策略：确定应用系统的备份内容、备份的方式、备份存储介质、备份周期和保留周期等内容。

第八条 各办公终端数据备份由该办公终端使用者负责，定期使用备份介质或者FTP服务器进行数据备份。

第九条 建立备份文件档案及档案库，详细记录备份数据的信息。要做好数据备份的管理，所有备份应有明确标识。

第十条 定期对长期保存的备份进行校验，以防止在需要时备份不可用的情况发生，校验应使用专业的校验工具进行。

第十一条 若出现数据丢失事件，应做到认真分析事件发生的原因，形成事件分析报告；依据分析报告，制订恢复计划；对现有的数据作相应的备份，以防止在恢复的过程中发生更进一步的错误；同时与有关部门进行沟通和通知有关部门进行恢复前的准备工作。

第十二条 恢复计划应包括恢复的内容、恢复的时间、恢复的操作步骤、恢复对应用造成的影响等因素。此计划应报上级领导批准。

第十三条 进行恢复操作前，数据库管理者应再次确认恢复计划的可行性及造成的后果，确认无误后进入到实际的恢复操作。进行恢复操作时应将每一步的执行过程记录下来。恢复操作后，必须测试数据恢复的结果；对恢复后的系统进行相应备份；将执行恢复操作的操作及管理者、恢复操作的时间、过程、完成的状况等情况形成恢复操作报告；同时通知相应部门恢复有关的应用。

第十四条 事件分析报告、恢复计划、恢复操作报告应编号存档。

## 附则

第十五条 本规定由临沂市妇幼保健院负责解释。

第十六条 本规定自发布之日起施行。

# 临沂市妇幼保健院 信息系统密码管理规定

## 总则

第一条 为加强临沂市妇幼保健院网络信息系统安全管理，促进临沂市妇幼保健院信息技术资源有效、可靠利用，根据国家有关信息化管理规定，制定本规定。

第二条 本规定所指的信息网络系统密码管理，是指临沂市妇幼保健院非涉密信息系统，包括计算机（含各类型主机、PC机及相关和配套设备）的系统登录密码，各应用系统的管理密码（如数据库、中间件管理密码），各应用系统的终端用户登录密码，各网络、安全设备的管理密码及各存储介质的访问许可密码等的管理。

1. 本规定适用于临沂市妇幼保健院各级临沂市

妇女儿童医院机关所属的计算机系统、应用系统、网络安全系统等信息网络系统。

## 密码管理

第四条 各岗位操作权限要严格按岗位职责设置，各岗位操作必须使用密码对用户的身份进行验证，防止对系统资源的未经授权的存取访问。

1. 主机系统、存储系统、数据库系统、核心应用中

间件系统和关键网络及安全设备（如路由器、防火墙等）的口令必须由专人掌管，并要求定期更换。按分别管理、共同负责的原则，由不同人员掌握服务器操作系统、数据库管理系统、中间件系统和关键网络、安全管理系统密码。

1. 在线运行的系统或设备，不允许使用初始密码或

默认密码。一般系统密码长度不得小于6位，重要系统密码不得少于8位，并且必须由字母、数字和特殊符号组成，具有一定的复杂性。

1. 定期更换口令。口令的最长使用时间不能超过半

年，人员复杂、保密条件较差的应尽可能缩短口令的使用时间。当口令使用期满时，应更换新的口令。

1. 用户应记住自己的口令，不应把它记载在不保密

的媒介物上或告知他人，严禁将口令贴在终端上。

1. 如因密码管理不善造成严重后果，将依照相关规

定追究当事人责任。

## 附则

第十条 本规定由临沂市妇幼保健院负责解释。

第十一条 本规定自发布之日起执行。

# 临沂市妇幼保健院

# 软件正版化管理规定

## 第一章 总则

第一条 为维护临沂市妇幼保健院良好形象，营造良好的舆论环境，切实增强尊重和保护知识产权的意识，根据《中华人民共和国计算机软件保护条例》等文件规定，并结合单位实际情况，特制定本规定。

第二条 本规定适用于单位软件的使用管理。

第三条 软件正版化的管理应遵循按需申请、专人安装、合理分配、科学使用、安全管理的原则。

## 第二章 职责与权限

第四条 信息科工作的任务是管理、监督软件终端用户使用正版软件，并保证所使用软件的品质和必要的升级维护。

第五条 信息科负责公司软件正版化标准的制定和软件的选型。

（一）负责贯彻落实国家有关软件正版化工作的政策和法规；遵守软件有关版权等规定。

（二）负责单位正版软件的安装、使用、保管、升级、版权保护及软件资产的管理。

（三）负责监督检查软件正版化工作的开展情况、执行情况和软件资产管理情况。

第六条 各科室主要负责人为软件正版化工作的第一责任人。

第七条 用户是软件需求的发起人。正版付费类软件需经过请示，待单位相关部门及领导同意后，方可申请购买和安装。

## 第三章 正版软件的管理

第八条 采购的管理

（一）根据需求指定正版软件采购计划，并将软件采购费用纳入年度预算，确保软件正版化工作资金到位、措施到位、管理到位。

（二）按照国家有关要求和本规定，加强软件资产管理，规范正版软件采购。

第九条 安装的管理

（一）信息科负责正版软件的安装调试。

（二）在购买计算机等相关设备时，不得要求或允许销售商安装任何非正版软件包括操作系统。

（三）不得要求扩大安装范围，严禁超越使用许可授权。

第十条 使用的管理

（一）加强软件正版化培训工作，进一步提高员工操作、使用软件的能力和水平，提高员工的法律意识，使正版软件更好地服务于公司的各项工作。

（二）不得擅自复制和销售公司计算机软件产品的复制品。

（三）要按照国家有关要求和本规定，确保正版软件在使用周期内的有效性。

（四）未经授权禁止擅自将计算机软件放在网上供他人下载。

（五）未经审批同意，禁止使用和下载未经授权的计算机软件。

（六）不得故意规避或者破坏软件著作权人为保护其著作权而采用的技术措施。

（七）不得故意删除或者改变计算机软件权限等管理信息。

（八）未经审批同意，禁止安装任何软件。

## 第四章 其他规定

第十一条 各部门在年度计划上报时，要将年度软件正版化工作情况总结同时上报，并组织进行考评。

第十二条 建立规范的正版软件管理台账，对各类正版软件进行登记。同时对有关的软件介质、说明书、使用许可证（或合同）等相关资料要由专人妥善保存。

第十三条 对于使用非法软件给公司声誉造成重大影响的，除追究相关责任人的法律责任外，公司还将追究相关部门、机构以及负责人的行政责任。

## 第五章 附 则

第十四条 本规定由临沂市妇幼保健院负责解释和修改。

第十五条 本规定自发布之日起施行。