# 2024年医院网络安全管理制度(十三篇)

来源：网络 作者：梦里花落 更新时间：2024-09-21

*人的记忆力会随着岁月的流逝而衰退，写作可以弥补记忆的不足，将曾经的人生经历和感悟记录下来，也便于保存一份美好的回忆。范文怎么写才能发挥它最大的作用呢？下面我给大家整理了一些优秀范文，希望能够帮助到大家，我们一起来看一看吧。医院网络安全管理制...*

人的记忆力会随着岁月的流逝而衰退，写作可以弥补记忆的不足，将曾经的人生经历和感悟记录下来，也便于保存一份美好的回忆。范文怎么写才能发挥它最大的作用呢？下面我给大家整理了一些优秀范文，希望能够帮助到大家，我们一起来看一看吧。

**医院网络安全管理制度篇一**

1、未经相关部门批准，任何人不得改变网络(内部信息平台)拓扑结构、网络(内部信息平台)设备布置、服务器、路由器配置和网络(内部信息平台)参数。任何人不得进入未经许可的计算机系统更改系统信息和用户数据。

3、机关局域网上任何人不得利用计算机技术侵占用户合法利益，不得制作、复制和传播妨害单位稳定的有关信息。

4、网络(内部信息平台)帐号采用分组管理。并详细登记：用户姓名、部门名称、口令，存取权限，开通时间，网络(内部信息平台)资源分配情况等。

5、网络(内部信息平台)管理员必须严守职业道德和职业纪律，不得将任何用户的密码、帐号等保密信息等泄露出去。网络管理员协助制定网络(内部信息平台)建设方案，确定网络(内部信息平台)安全及资源共享策略。

6、严格遵守国家、自治区、自治州制定的相关法律、行政法规，严格执行《网络安全工作制度》，以人为本，依法管理，确保网络(内部信息平台)安全有序。

7、所有用户有责任对所发现或发生的违反有关法律，法规和规章制度的人或事予以制止或向我部信息安全协调科反映、举报，协助有关部门或管理人员对上述人或事进行调查、取证、处理，应该向调查人员如实提供所需证据。

8、在发生网络(内部信息平台)重大突发事件时，应立即报告，采取应急措施，尽快恢复网络(内部信息平台)正常运行。

9、充分利用现有的安全设备设施、软件，最大限度地防止计算机病毒入侵和黑客攻击。14、经常检查网络(内部信息平台)工作环境的防火、防盗工作。

10、单位应定期查毒，(周期为一周或者10天)管理员应及时升级病毒库，并提示各部门对杀毒软件进行在线升级。 密码安全保密制度

11、涉密移动存储介质未经批准不得擅自带离本单位，确因工作需要携带外出的，须履行登记备案手续，并经领导批准。严禁将涉密移动存储介质借给外单位或他人使用。

12、涉密移动存储介质需维修的，由单位技术人员送至有保密资质的单位现场监修，严禁维修人员擅自读取和拷贝其存储的国家秘密信息。如涉密移动存储介质无法修复，必须按涉密载体予以销毁。

13、要定期对网站进行网络(内部信息平台)数据包的监控，及时发现和网络(内部信息平台)运行情况，全面监视对公开服务器的访问，及时发现和拒绝不安全的`操作和黑客攻击行为，阻止网络(内部信息平台)内外的入侵。

14、网络(内部信息平台)信息安全员履行对所有上网信息进行审查的职责，根据需要采取措施，监视、记录、检测、制止、查处、防范针对内部信息平台或入网计算机的人或事。

**医院网络安全管理制度篇二**

为加强我市校园网络安全管理，确保校园网络安全稳定运行，依据教育部《关于加强教育行业网络与信息安全工作的指导意见》，制订本制度。

一、学校成立网络信息安全领导小组，组长由学校校长担任，负责校园内网络安全和信息安全管理工作，学校网络管理员负责全校网络及信息具体安全工作，对校园网和上网信息进行审查和监控。

二、校园网用户必须严格遵守国家法律、法规及学校规章制度，不得利用计算机联网从事危害国家安全、泄露秘密等犯罪活动，不得制作、查阅、传播违法内容。严禁制造和输入计算机病毒。

三、学校要对教师和网络用户定期进行信息安全和网络安全相关教育，增强防范意识。

四、校园网要有防火墙和防病毒软件。学校网管员对校园网设备和线路，进行统一管理，其它个人禁止擅自打开计算机主机机箱，禁止擅自移动计算机、线路及附属设备，禁止擅自将计算机设备外借。任何人不得更改ip及网络设置。

五、校园网设备，要按分配的使用权限来使用，遵循谁使用，谁负责的原则进行管理。对服务器、路由器、交换机等重要网络设备，要由网管员进行管理。

六、严格遵守网络保密制度，不得将已知的用户名、密码、口令、地址外泄。对于有版权保护的\'计算机软件禁止任何科室和个人擅自对外提供。

七、网络管理员定期汇报及网络事故随时报告制度，及时解决突发事件和问题。校园网服务器发生案件、遭到黑客攻击后，网管员必须及时处理，必要时通过学校领导向公安机关报告。

八、做好设备的日常维护、保养工作。机房及各功能室设施应符合国家有关规定，认真做好电源防护、防盗、防火、防水、防尘、防震、防静电等工作，必须安装防盗门窗和报警装置，人离关窗锁门。

**医院网络安全管理制度篇三**

学校校园网是为教学及学校管理而建立的计算机信息网络，为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，更好的为教育教学服务，特制定本制度：

1、学校成立信息安全领导小组，组长由学校法人担任，负责校园内的网络安全和信息安全管理工作，定期对学校网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

2、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

3、网络管理员负责全校网络及信息的安全工作，建立定期汇报及网络事故随时报告制度，及时解决突发事件和问题。校园网服务器发生案件、遭到黑客攻击后，网络中心必须及时备案并通过学校领导向公安机关报告。

4、计算机防病毒软件由网络中心统一安装，用户要切实做好防病毒措施，及时在线升级杀毒软件，严禁在校园网内使用来历不明、引发病毒传染的软件或文件;对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、消毒。及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

5、校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

6、校园网中对外发布信息的网站必须按有关规定办理icp备案。发布信息必须经审核程序，由负责人签署意见后再由信息员发布。

7、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。

8、校园网的系统软件、应用软件及信息数据要实施保护措施。未经校园网络中心同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。装有涉密资料、重要数据、财务数据的`电脑要与网络实行物理隔离。

9、保护校园网的设备和线路。不准擅自打开计算机主机的机箱，不准擅自移动计算机、线路及附属设备，不准擅自把计算机设备外借。任何人不得更改ip及网络设置。禁止私自安装、卸载程序，禁止使用盗版软件，禁止任意修改和删除服务器、计算机的系统文件和系统设置。

10、校园网用户不得利用计算机联网从事危害国家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有敏感信息、政治问题和淫秽色情内容的信息。严禁制造和输入计算机病毒。对利用网络从事违法行为者，应立即送交公安机关处理。

11、校园网用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把户名借给他人使用，增强自我保护意识，经常更换口令，保护好户名和ip地址。不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动。

**医院网络安全管理制度篇四**

所有网络设备（包括光纤、路由器、交换机、集线器等）均归现代教育技术中心所管辖，其安装、维护等操作由现代教育技术中心工作人员进行。其他任何人不得破坏或擅自维修。

所有学校内计算机网络部分的扩展必须经过现代教育技术中心实施或批准实施，未经许可任何部门不得私自连接交换机、集线器等网络设备，不得私自接入网络。现代教育技术中心有权拆除用户私自接入的网络线路并进行处罚措施。

各部门的联网工作必须事先报现代教育技术中心，由现代教育技术中心做网络实施方案。

学校局域网的网络配置由现代教育技术中心统一规划管理，其他任何人不得私自更改网络配置。

接入学校局域网的客户端计算机的网络配置由现代教育技术中心部署的dhcp服务器统一管理分配，包括：用户计算机的ip地址、网关、dns和wins服务器地址等信息。未经许可，任何人不得使用静态网络配置。

任何接入学校局域网的客户端计算机不得安装配置dhcp服务。一经发现，将给予通报并交有关部门严肃处理。

网络安全：严格执行国家《网络安全管理制度》。对在学校局域网上从事任何有悖网络法规活动者，将视其情节轻重交有关部门或公安机关处理。

教职工具有信息保密的义务。任何人不得利用计算机网络泄漏公司机密、技术资料和其它保密资料。

任何人不得在局域网络和互联网上发布有损学校形象和教工声誉的信息。

任何人不得扫描、攻击学校计算机网络。

任何人不得扫描、攻击他人计算机，不得盗用、窃取他人资料、信息等。

为了避免或减少计算机病毒对系统、数据造成的影响，接入学校局域网的所有用户必须遵循以下规定：

1.任何单位和个人不得制作计算机病毒；不得故意传播计算机病毒，危害计算机信息系统安全；不得向他人提供含有计算机病毒的文件、软件、媒体。

2.采取有效的计算机病毒安全技术防治措施。建议客户端计算机安装使用现代教育技术中心部署发布的瑞星杀毒软件和360安全卫士对病毒和木马进行查杀。

3.定期或及时更新用更新后的新版本的杀病毒软件检测、清除计算机中的病毒。

学校的互联网连接只允许教职工为了工作、学习和工余的休闲使用，使用时必须遵守有关的国家、企业的法律和规程，严禁传播淫秽、反动等违犯国家法律和中国道德与风俗的内容。学校有权撤消违法犯纪者互联网的使用。使用者必须严格遵循以下内容：

1.从中国境内向外传输技术性资料时必须符合中国有关法规。

2.遵守所有使用互联网的网络协议、规定和程序。

3.不能利用邮件服务作连锁邮件、垃圾邮件或分发给任何未经允许接收信件的人。

4.任何人不得在网上制作、查阅和传播宣扬反动、淫秽、封建迷信等违犯国家法律和中国道德与风俗的内容。

5.不得传输任何非法的、骚扰性的、中伤他人的、辱骂性的、恐吓性的.、伤害性的等信息资料。

6.不得传输任何教唆他人构成犯罪行为的资料，不能传输助长国内不利条件和涉国家安全的资料。

7.不能传输任何不符合当地法规、国家法律和国际法律的资料。

各部门人员每日上班及时打开计算机，进入学校办公系统、浏览相关文件信息、学习有关文件资料。如有自己业务相关的工作信息，要及时处理，处理结果及时回馈有关责任人员。

充分利用办公系统的优势信息处理平台，浏览的相关情况由办公系统后台数据库自动生成详细记录，以便领导检查相关登陆信息提供记录参考。

各部门人员必须及时做好各种数据资料的录入、修改、备份和数据保密工作，保证数据资料的完整准确和安全性。

严禁外来人员对计算机数据和文件进行拷贝或抄写以免泄漏学校机密，对学校办公系统或其它学校内部平台帐号不得相互知晓，每个人必须保证自己帐号的唯一登陆性负责，否则由此产生的数据安全问题由其本人负全部责任。

**医院网络安全管理制度篇五**

学校校园网是为教学及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理条例。

1、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

2、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

3、我校成立了网络安全领导小组，组长由学校法人担任，从事校园网络管理的人员要具有相应的法律意识和计算机网络管理水平，必须成立校园网络安全管理机构，负责校园内的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

4、任何单位和个人，未经学校法人或校园网络中心同意，不得擅自安装、拆卸或改变网络设备。

5、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

6、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络中心进行的网络系统及信息系统的安全检查。

7、使用校园网的全体师生有义务向学校法人、网络中心和有关部门报告违法行为和有害信息。

1、校园网由学校统一管理及维护。接入校园网的各部门、处室、教室和个人使用者必须严格使用自己的用户名和密码上网。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作，要及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。网络教室未经允许不准对社会开放。

5、校园网中对外发布信息的\'web服务器中的内容必须经领导审核，由负责人审核通过后再进行发布。新闻公布、公文发布权限要经过对应部门领导的批准。对网站内容要进行定期更新、备份。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监督：

（1）校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志同时上报县教育局电教室。

（2）加强对学生开放互联网以及全校教职工上网的监管。

（3）专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

8、校园网络内的每台计算机上必须安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

9、禁止私自安装、卸载程序，在校园网上，禁止使用盗版软件，不允许玩网络游戏，不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

10、严禁在校园网内使用来历不明、引发病毒传染的软件或文件；对于外来光盘、优盘上的文件应使用合格的杀毒软件进行检查、杀毒。

11、任何单位和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

12、未经校园网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

13、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的c盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

14、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线路设备及附属设备，不准擅自把计算机设备外借。

15、各处室部门和教研组必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通过校园办公系统上报。

16、各处室部门和教研组应认真做好本单位计算机的维护和清洁卫生工作。

1、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有敏感信息和有害信息。

2、除校园网负责人员外，其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施。

3、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把户名借给他人使用，增强自我保护意识，经常更换口令，保护好用户名和密码。严禁用各种手段破解他人口令、盗用户名和密码。

4、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动。

5、使用校园网的全体师生有义务向网络中心报告违法行为和有害的、不健康的信息。

违反本制度规定，有下列行为之一的，学校可根据情节提出警告、停止其上网，情节严重者给予行政处分，或交公安机关处理。

1、查阅、复制或传播下列信息

（1）煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度；

（2）煽动抗拒、破坏宪法和国家法律、行政法规的实施；

（3）捏造或者歪曲事实，故意散布谣言，扰乱社会秩序；

（4）公然侮辱他人或者捏造事实诽谤他人；

（5）宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

2、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

3、盗用他人帐号或私自转借、转让用户帐号造成危害者；

4、故意制作、传播计算机病毒等破坏性程序者。

5、上网信息审查不严，造成严重后果者。

6、使用任何工具破坏网络正常运行或窃取他人信息者。

7、有盗用用户名和口令、破解用户口令等危及网络安全运行与管理的恶劣行径者。

**医院网络安全管理制度篇六**

学校校园网是为教学及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理条例。

1、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

2、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

3、教技领导小组下的网络管理组负责相应的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

4、任何单位和个人，未经管理组同意，不得擅自安装、拆卸或改变网络设备。

5、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

6、进入校园网的\'全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络管理组进行的网络系统及信息系统的安全检查。

7、使用校园网的全体师生有义务向网络管理组和有关部门报告违法行为和有害信息。

1、校园网由学校网络管理小组统一管理及维护。连入校园网的各部门、教室和个人使用者必须严格使用由网络中心分配的ip地址。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用ip地址及用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作，建立网络事故报告制度并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络管理组必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。校园网络不准对社会开放。

5、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络管理组对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监督：

（1）校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

（2）加强对学生开放互联网以及全校教职工上网的监管。

（3）专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

8、网络管理小组统一在每台计算机上安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络管理组报告陌生、可疑邮件和计算机非正常运行等情况。

**医院网络安全管理制度篇七**

为加强我委计算机信息网络安全管理，确保信息网络安全、高效、正常运行，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》和柳保(20xx)9号《关于在全市开展保密计算机违规联接互联网监管工作的通知》和有关规定，制定本规定。

第一条全委干部职工必须严格遵守国家保密法和计算机网络信息安全管理法规及本规定。

第二条任何单位和个人不得利用本委计算机信息网络从事危害国家安全、泄露国家秘密等非法活动，不得利用本委计算机信息网络制作、查阅、复制和传播妨碍社会治安和淫秽色情等有害信息。

第三条涉密计算机信息系统的研制、安装和使用，必须符合保密要求，并采取有效的措施，配置合格的保密专用设备，防泄密、防窃密。

第四条涉密计算机信息系统必须与互联网实行物理隔离，严禁用处理国家秘密信息的计算机(包括便携式计算机)上互联网。

第五条装有国家秘密信息的便携式计算机原则上只能在委机关内使用，确因工作需要携带外出，必须将涉密信息全部转出便携式存储设备存放在机关。

第六条上互联网的计算机必须与处理涉密信息的计算机严格区分，专机专用，不得既用于上互联网又用于处理国家秘密信息。

第七条计算机网络插头和接口，必须标明字样，严格区分，按规范安装，其他人员不得擅自删除或更改与网络系统有关的设置，严防由于误操作造成泄密。

第八条涉密信息和数据必须按照保密规定进行采集、存储、处理、传递、使用和销毁。使用计算机起草、存储、处理、传递涉密文件、材料，必须在涉密计算机上进行。

第九条建立上网信息保密审查制度，坚持“谁上网谁负责\'的原则，信息上网必须经过严格审查和批准，确保国家秘密不上网，上网信息不涉密。

第十条各科室，应当造册登记，切实加强软盘、磁带、光盘、移动硬盘等信息媒体管理。存储有国家秘密信息的信息媒体，按所存储信息的最高密级标明密级，并按相应密级文件的保密规定进行管理，不得降低密级使用。不再使用的信息媒体应及时销毁。

第十一条报废、维修存储过国家秘密信息的计算机和信息媒体，须交委办公室按保密规定统一处理，保证所存储的国家秘密信息不被泄露。

第十二条做好计算机信息系统数据备份。根据需要与存贮环境，重要信息要定期(半年至二年)进行循环复制三份分处存放，并注意防止因静电、电磁干扰等原因导致信息丢失。

第十三条做好计算机日常维护工作，严格查毒杀毒，发现病毒及时清除，确保信息系统安全运行。

第十四条妥善保管和使用计算机ca认证系统密钥，保守计算机信息系统用户口令秘密。密钥被盗或遗失，应及时作废，重新分配。

第十五条文印室计算机管理。文印室的计算机由打字员负责管理，任何人不得擅自使用文印室的计算机，如需用扫描仪应自带u盘在外网计算机上操作直接将文件存入自带盘中，严禁扫描、传输有密级的文件。严禁外单位人员进入文印室。

第十六条本委计算机信息网络安全工作由委信息安全领导小组负责。委主要负责人担任领导小组组长，成员由各科室负责人组成。领导小组职责是：

(一)根据国家有关计算机信息网络安全的法规和政策，审定本委计算机信息网络安全工作计划和管理制度;

(二)指导和检查本委计算机信息网络安全工作;

(三)定期对计算机信息系统的\'系统安全保密管理人员进行上岗前保密培训，严格审查和考核。

(四)研究、解决本委计算机信息网络安全重大问题。

第十七条委信息安全领导小组下设办公室，由委办公室和相关人员组成，在领导小组领导下，负责本委计算机信息网络安全管理的日常工作。

第十八条各科室负责人是本科室计算机信息网络安全工作的第一责任人，对本科室信息安全工作负责。

第十九条各科室切实加强对本科室的保密知识教育，提高工作人员信息安全保密意识，自觉遵守保密纪律和有关保密规定，发现有违反规定的行为，立即纠正，发现国家秘密泄露或可能泄露情况时，应当立即报告委信息安全领导小组。

第二十条违反本规定造成泄密的，将按有关法律和规定，追究当事人和责任人的责任，依法依纪进行处理。

第二十一条本规定自发布之日起执行。

**医院网络安全管理制度篇八**

智慧校园校园网是为教学工作及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理制度。

一、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

二、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

三、校园网实行统一管理、分级负责制。网络中心负责对校园网资源进行管理，负责全校的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控；各处室及办公室负责对本部门资源进行管理；各部门计算机责任人负责对本部门计算机系统的管理。有关校园网上进行学校信息发布、新闻宣传系统、管理信息系统等方面的信息服务，归口学校办公室负责。

四、任何单位和个人，未经校园网网络中心同意，不得擅自安装、拆卸或改变网络设备。

五、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

六、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络中心进行的网络系统及信息系统的安全检查。

七、使用校园网的全体师生有义务向网络中心和有关部门报告违法行为和有害信息。

一、校园网由学校网络中心统一管理及维护。连入校园网的各部门、处室、教室和个人使用者必须严格使用由网络中心分配的ip地址。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用ip地址及用户帐号。

二、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

三、网络管理员负责全校网络及信息的安全工作，建立网络事故报告并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

四、对所有联网计算机要及时、准确登记备案。网络教室不准对社会开放。

五、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

六、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的`系统软件、应用软件及信息数据要实施保密措施。

七、加强对师生用户上网安全教育指导和监督：

1、校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

2、加强对学生开放互联网以及全校教职工上网的监管。

3、专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

八、网络中心统一在每台计算机上安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

九、禁止私自安装、卸载程序；在校园网上，禁止使用盗版软件，不允许玩计算机游戏，不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

十、严禁在校园网内使用来历不明、引发病毒传染的软件或文件；对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、消毒。

十一、任何单位和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

十二、未经校园网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

十三、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的c盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

十四、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线路设备及附属设备，不准擅自把计算机设备外借。

十五、各处室部门和教研组必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通知网络中心处理。

十六、各处室部门和教研组应认真做好本单位计算机的养护和清洁卫生工作。

一、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害国家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有碍社会治安和有伤风化的信息。

二、除校园网负责人员外，其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对校园网安全运行的破坏行为。

三、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把帐号借给他人使用，增强自我保护意识，经常更换口令，保护好帐号和ip地址。严禁用各种手段破解他人口令、盗用帐号和ip地址。

四、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动，该活动被认为是对网络用户权益的侵犯。

五、使用校园网的全体师生有义务向网络中心报告违法行为和有害的、不健康的信息。

违反本制度规定，有下列行为之一者，学校可提出警告、停止其上网，情节严重者给予行政处分，或提交司法部门处理。

一、查阅、复制或传播下列信息者：

1、煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度。

2、煽动抗拒、破坏宪法和国家法律、行政法规的实施。

3、捏造或者歪曲事实，故意散布谣言，扰乱社会秩序。

4、公然侮辱他人或者捏造事实诽谤他人。

5、宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

二、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

三、盗用他人帐号或私自转借、转让用户帐号造成危害者。

四、故意制作、传播计算机病毒等破坏性程序者。

五、上网信息审查不严，造成严重后果者。

六、使用任何工具破坏网络正常运行或窃取他人信息者。

七、有盗用ip地址、盗用帐号和口令、破解用户口令等危及网络安全运行与管理的恶劣行径者。

**医院网络安全管理制度篇九**

一、校园网的安全运行和所有网络设备的管理维护工作由学校网络管理中心负责。

二、网络管理中心机房要装置调温、调湿、稳压、接地、防雷、防火、防盗等设备，保证网络设备的安全运行，要建立完整、规范的校园网设备运行情况档案及网络设备帐目，认真做好各项资料(软件)的记录、分类和妥善保存工作。

三、除网络管理中心外，其他单位或个人不得以任何方式试图登陆校园网后台管理端，不得对服务器等设备进行修改、设置、删除等操作。

四、校园网对外发布信息的web服务器中的内容，必须经发布信息的学校部门负责人审核并签署意见后，交校办公室审核备案，由网络管理中心从技术上开通其对外的信息服务。

五、网络使用者不得利用各种网络设备或软件技术从事用户账户及口令的侦听、盗用活动，该活动被认为是对校园网网络用户权益的侵犯。

六、为防范黑客攻击，校园网出口处应设置硬件防火墙。若遭到黑客攻击，网络管理中心必须在二十四小时内向当地县以上公安机关报告。

七、严禁在校园网上使用来历不明及可能引发计算机病毒的软件。外来软件应使用经公安部门颁发了《计算机信息系统安全专用产品销售许可证》的杀毒软件检查、杀毒。

八、不得在校园网及其联网计算机上传送危害国家安全的信息(包括多媒体信息)、录阅传送淫秽、色情资料。

九、校园网的.系统软件、应用软件及信息数据要实施保密措施。信息资源分不同的保密等级对学校各部门开放。

十、对校园网站内各交互栏目实现管理员24小时巡查制度，双休日、节假日，要有专人检查网络运行情况。

十一、学校网络管理中心必须遵守国家公安部及省公安厅关于网络管理的各项法律、法规和有关技术规范。合理对系统进行安全配置，落实各项网络安全技术防护措施，完善系统定期维护更新措施，落实垃圾邮件、有害信息过滤、封堵技术措施，严格防范病毒、木马、黑客等网络攻击。

十二、服务器系统及各类网络服务系统的系统日志、网络运行日志、用户使用日志等均应严格按照保留60天的要求设置，邮件服务器系统严禁使用匿名转发功能。

**医院网络安全管理制度篇十**

一、严格执行国家及地方制定的信息安全条例。

二、上网用户必须严格遵循网络安全保密制度。

三、提供的上网信息,必须经过办公主的审核后方可上网,并及时予以登记。

四、用户必须配合有关部门依法进行信息安全检查。

五、建立健全网络安全管理制度,采取安全技术措施,落实安全管理责任,加强对bbs等交互式栏目信息发布的审核,网络运行日志的管理,并将系统运行日志完整仅用3个月以上,以备公安机关的监督检查。

六、\"安全专管员\"要加强网络信息、监测,定期检查安全情况、计算机是否感染病毒并及时清除,同时应配合网络管理员对各开通服务器的\'系统日志进行不定期检查,及时发现隐患及时汇报与处理。

七、对网络上有害信息及时控制并删除。严防非法用户侵入我方网络从事非法活动,一经发现及时进行相应的技术处理,如及时清除有需信息的传播途径、关闭相应的服务器等,并且保护好相关日志等数据,及时向有关部门报告。

八、出现有关网络安全隐患及时上报办公室,及时处理并作日志。

九、加强对用户数据的管理,发现异常用户,及时处理并上报办公室备案。

十、定期组织网络管理人员进行安全管理学习和培训。

**医院网络安全管理制度篇十一**

1、学校成立网络管理领导小组和网络维护小组。维护小组由管理员和信息技术教师组成，负责在网络管理领导小组指导下进行日常维护。

2、网络用户是指使用网络的各部门及个人。

3、学校鼓励各部门、各科室、各学科组和全体师生使用网络资源。

4、网络维护小组根据教育网信息管理中心要求为每科室、学科组、个人统一分配ip地址，其他人不得随意更改，如有需要报维护小组进行修改。

5、各科室、学科组和个人在使用网络过程中必须遵守国家有关法律、法规和信息中心的有关规定。

6、用户在使用网络时违反国家法律和行政法规的\'，学校将视情节轻重给予警告、通报批评，情节特别严重构成犯罪的，报有关部门依法追究刑事责任。

7、禁止各用户上不良网站。通过聊天、邮件而传播网络病毒的，维护小组要及时提醒，要求该用户改正，如果是故意行为，将报学校网络管理领导小组进行严肃处理。

8、网络的主干通信设备、主干网络线路、服务器、网络交换机及其它公共设备由维护小组负责管理维护。

9、维护小组对各用户计算机进行对入网设备、安装的软件实行

规范管理，不定期进行检查。对安装不健康内容、危害网络安全和一些游戏软件进行及时清除

10、网络信息是指通过网络发布、传递及存储在网络设备中的信息。学校鼓励教师使用网络上有用资源。

11、任何人不得利用学校网络提供的各种信息服务从事危害国家安全、泄露国家机密等犯罪活动，不得制作、查阅、复制和传播危害国家安全、妨碍社会治安和淫秽色情的信息。

12、发生重大突发事件期间，学校网络安全管理领导小组要加强网络监控，及时、果断地处置网上突发事件。

**医院网络安全管理制度篇十二**

为了加强局计算机及网络安全的管理，确保网络安全稳定的运行，切实提高工作效率，促进信息化建设的健康发展，现结合实际情况，制定本管理规定。

局信息化领导小组办公室是计算机及网络系统的管理部门，履行管理职能。局信息中心具体负责局计算机(包括外部设备)及网络设备的选型、安装、维修;应用系统及软件的安装、维护;负责局计算机网络系统的安全保密工作。

计算机使用管理

第一条各科室、局属各单位对所使用的计算机及其软硬件设施，享有日常使用的权利，负有保管的义务。

第二条计算机开启关闭应按规定步骤进行，工作人员应规范使用计算机设备。如因操作不当等原因导致设备损坏，将视情节处理。

第三条各科室计算机实行专人专用，使用统一分配的口令进入局域网，发现不能进入局域网须及时报告网管人员,不得擅自修改计算机的ip地址和cmos设置参数。

第四条各科室、各单位确需增加计算机设备或网络终端接口，应向局信息中心提出申请，经批准后，由网管人员负责接入。

第五条工作人员使用计算机时，不得关闭杀毒软件和网络防火墙，应确保防火墙处于激活状态。防病毒软件要定期进行更新升级，定期和及时对电脑进行杀毒，清洁，除尘，保证电脑能安全运行。工作人员发现计算机病毒应及时清除并报告网管人员备案。

第六条禁止私自拆卸和擅自修理计算机，禁止私自更换计算机硬件设备。如需修理或更换，应先报局信息中心经审批后由网管人员或计算机公司专业人员负责修理或更换。

第七条为保证业务系统安全工作，软盘、光盘等存储设备必须经病毒检查后方可使用。

第八条严格遵守信息传递操作流程。各终端计算机可根据工作需要设立共享硬盘或文件夹，设立的共享硬盘或文件夹使用完毕后应立即取消共享设置。

第九条网络用户密码及共享权限密码严禁外泄。严禁擅自查看、修改、拷贝其局域网内其他计算机的程序及内容。

第十条不浏览和发布反动、黄色、邪教，反动言论等信息，一经发现，严肃查处，停止使用互联网权限。严禁在线播放或下载电影、电视剧等，禁止擅自安装使用游戏。

第十一条局信息中心网管人员要定期检查各计算机终端运行情况，发现问题，及时排除。

第十二条非因工作需要，不得将机关计算机设备和存储涉密信息的软件、磁盘、光盘及其他存储介质带离机关。因工作需要带出工作区域的，须经批准后登记备案才能带出。严禁将与工作无关的存储介质在单位的计算机上使用。严禁存储介质在内外网计算机，以及在涉密与非涉密计算机间互用。

第十三条建立、健全计算机病毒的预防、发现、报告、消除管理制度及计算机设备的使用、维护制度,对机关的计算机信息网络系统进行经常性的病毒检测。

第十四条未经允许，禁止开设文件服务器、共享服务器、下载服务器、ftp服务器、web服务器、e-mail服务器、游戏服务器、媒体服务器、网络磁盘、聊天服务器等各种对外服务器。

第十五条禁止使用各类群发、抢占网络带宽、强迫他人下网的软件;局域网内的计算机禁止使用多线程下载文件而造成网络拥堵、系统瘫痪、影响别人正常使用。随着信息化工作的深入开展，不同格式、不同内容的数据库也将越来越多，市局数据中心涉及20多种不同类型的数据库系统，因此对于数据库系统的管理也应进一步规范。

第十六条网络系统用户，须做好自身用户密码和权限的`保密工作，新用户系统启用后两天内必须更改初始密码，不得将密码随意告诉他人。

第十七条数据库管理员不得将数据库管理员密码随意透露给他人;不得将数据库一般用户密码泄漏或随意修改其用户权限;不能向任何人泄露数据库存储的内容。

第十八条若因用户名和密码泄露造成数据库信息被更改或流失的，由泄密者承担责任，情节严重者递交局党组处理。

第十九条数据库管理员随时做好数据库的备份，核心数据库的进入必须设置准入的用户名和密码，只有用户名和密码同时输入正确时才能更改、导出数据库信息;数据库管理员对不正当的数据库信息更改行为做好记录，并由提出更改要求的人员签字。

第二十条任何人不得随意向外单位或个人提供纸质或电子版的数据库信息，如确须提供的，需经相关业务分管领导审核、审批同意，并经相关业务科室负责人签字确认后方可提供。

**医院网络安全管理制度篇十三**

为确保我单位计算机信息网络的安全，根据《中华人民共和国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》的有关规定,结合我单位计算机信息网络使用情况，特制定本办法。

一、计算机信息安全及工作，实行责任制和责任追究制。各部门主要负责人为本部门信息网络安全责任人，负责本单位网络信息安全及保密管理工作。

二、网络中心必须由专人负责，各种设备的技术参数由中心负责，以确保信息网络的安全运行。其他任何人不得随意移动网络设备，不得擅自修改设备技术参数。

三、网络中心负责单位局域网的规划、建设、运行维护及用户管理。计算机ip地址采取与网卡物理地址绑定，由中心统一管理并登记备案，严禁外单位或个人联入中心局域网。

四、入网部门和个人必须接受职能部门的监督检查，并对采取的.必要措施给予配合。单位网页内容和新闻动态等信息服务由指定的职能部门负责维护和服务，未被授权的任何部门或个人不能更改其内容。

五、所有部门和个人在网络上都应自觉遵守计算机信息网络安全的有关规定。不允许出现任何方式干扰网络用户、破坏网络服务和网络设备安全的活动；不允许进入未经授权使用的计算机服务器和网络系统；不允许以不真实身份使用网络资源；不允许窃取他人账号、口令；不允许盗用未经合法申请的ip地址入网；任何人不得擅自改动ip地址设置。

六、禁止下载互联网上任何未经确认其安全性的软件，严禁使用盗版软件及游戏软件。任何单位和个人不得利用单位分配的个人电子邮箱上公网注册信息，不得访问恶意网站和不健康网站，不要随意打开陌生邮件。

七、所有账号、口令等密码3个月更改一次，数据库、重要文件等每天备份一次，网络系统的所有软件均不准私自拷贝出来赠送其它单位或个人，违者将严肃处理。

八、严禁随意使用u盘、光盘等存储介质，如工作需要，外来u盘、光盘须在没联网的单机上检查病毒，确认无毒后方可上网使用。私自使用造成病毒侵害要追究当事人责任。

十、严禁以任何途径和媒体传播计算机病毒，对于传播计算机病毒者视情节轻重，给予处分。制造病毒或修改病毒程序者，要给予严肃处理。

十一、发现病毒，应及时对感染病毒的设备进行隔离，情况严重时报相关部门并及时妥善处理。实时进行防病毒监控，做好防病毒软件和病毒库的智能升级。

十二、应当注意保护网络数据信息的安全，对于存储在数据库中的关键数据，以及关键的应用系统进行及时数据备份，及时更新数据库和防病毒软件病毒库，定期对所有数据库进行漏洞扫描、补丁修复，保证重要数据的安全。

十三、任何人不得利用网络从事危害国家安全，泄露国家秘密的活动。任何人不得查阅、复制和传播有碍社会治安和伤风败俗的信息。违反本管理规定，且有下列行为之一者，中心可提出警告、停止其使用网络，情节严重者，提交行政部门或有关司法部门处理。

十四、在我单位的计算机网络发生安全事件或者事故的情况下，网络中心积极处置，跟进、快速地协调、处理各种事件或者事故；及时响应、处置上级网监部门的预警和问题通报。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找