# 最新医院网络安全管理制度 建立网络安全管理制度(11篇)

来源：网络 作者：风月无边 更新时间：2024-09-21

*无论是身处学校还是步入社会，大家都尝试过写作吧，借助写作也可以提高我们的语言组织能力。相信许多人会觉得范文很难写？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 建立网络安全管理制度篇一二、学校...*

无论是身处学校还是步入社会，大家都尝试过写作吧，借助写作也可以提高我们的语言组织能力。相信许多人会觉得范文很难写？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 建立网络安全管理制度篇一**

二、学校网络中心必须采取各种技术及行政手段保证网络安全和信息安全。

三、网络中心的工作人员和用户必须对所提供的信息负责。不得利用计算机联网从事危害国家安全，泄露国家秘密等违法活动，不得制作、查阅、复制和传播有碍社会治安和有伤风俗文化的信息。

四、不允许进行任何干扰网络用户、破坏网络服务和破坏网络设备的活动。包括不许在网络上发布不真实的信息，不许散布计算机病毒，不许使用网络进入未经授权使用的计算机等。

五、学校应设立网络安全员，负责网络安全和信息安全工作。

六、网络中心应按照《计算机信息网络国际联网安全保护管理办法》定期对相应的网络用户进行有关的`网络安全和信息安全教育。

七、网络中心应根据国家有关规定对上网用户进行审查。凡违反国家有关规定的信息严禁上网。

八、所有用户有义务向网络安全员和有关部门报告违法犯罪行为和有害信息。

九、网络中心和用户必须接受上级有关部门依法进行的监督检查。对违反本管理办法的个人，将对其进行警告，停止网络连接、上报学校等处理。

十、安装正版杀毒软件、防火墙，按时更新杀毒软件、防火墙，定期杀毒，防范非法用户入侵，防止计算机病毒入侵。

**医院网络安全管理制度 建立网络安全管理制度篇二**

计算机网络为学校局域网提供网络基础平台服务和互联网接入服务，由网络维护中心负责计算机连网和网络管理工作。为保证集团局域网能够安全可靠地运行，充分发挥信息服务方面的重要作用，更好地为学校员工提供服务。

第一条

所有网络设备（包括路由器、交换机、集线器、光纤、网线等）均归网络维护中心所管辖，其安装、维护等操作由网络维护中心工作人员进行，其他任何人不得破坏或擅自维修。

第二条

所有学校内计算机网络部分的扩展必须经过网络维护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。网络维护中心有权拆除用户私自接入的网络线路并报告上级领导。

第三条

各分校、处（室）的联网工作必须事先报经网络维护中心，由网络维护中心做网络实施方案。

第四条

学校局域网的网络配置由网络维护中心统一规划管理，其他任何人不得私自更改网络配置。

第五条

接入学校局域网的客户端计算机的网络配置由网络维护中心部署的`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，任何人不得更改网络配置。

第六条

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。

第七条

学校员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。

第八条

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，保证数据资料的完整准确和安全性。

第九条

任何人不得在局域网络和互联网上发布有损学校形象和职工声誉的信息。

第十条

任何人不得扫描、攻击学校计算机网络和他人计算机。不得盗用、窃取他人资料、信息等。

第十一条

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.任何部门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网络维护中心部署发布的相关杀毒软件和360安全卫士对病毒和木马进行查杀。

3.定期或及时用更新后的新版杀病毒软件检测、清除计算机中的病毒。

第十二条

学校的互联网连接只允许员工为了工作、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。一经发现学校网络维护中心有权撤消违纪者互联网的使用权。

第十三条

为了发挥好网站的形象宣传作用，各分校、处（室）要及时向网络维护中心提供有关资料，以便充实网站内容，加大宣传影响。由网络维护中心统一整理、编辑上传及内容更新。

第十四条

各分校、处（室）人员在下班离开前必须关闭计算机和电源插座，避免浪费电能和发生消防隐患，违纪者通报批评并进行相应的处罚。有加班需要的工作人员必须提前通知网络维护中心。

**医院网络安全管理制度 建立网络安全管理制度篇三**

1、具体负责校园网网络安全的管理，协调各部门实施校园网网络安全的有关管理措施。

2、维护和管理学院网络版杀毒软件，监控网络病毒，并对用户的网络版杀毒软件使用提供技术支持。

3、负责校园网网络安全的管理，做好各服务器的.防病毒和防篡改工作，对服务器进行定期查毒、杀毒，及时下载并安装系统漏洞补丁，采取各种有效措施防止黑客攻击和破坏。

4、对网络的系统及环境进行安全维护，随时监督网络情况，防止黑客入侵、病毒侵害及网络安全，配合有关部门进行相应管理。

5、网络安全人员要协助信息管理中心技术人员定期检查有关网络和服务器系统的运行日志，定期和不定期地进行对全校校园网进行网络安全检查。

6、对校园网上的信息进行管理，随时更新并查看www、ftp信息内容，删除、屏蔽有害信息，为用户提供内容丰富健康的信息服务。

7、定期检查有关网络和服务器系统的运行日志，定期和不定期对校园网进行安全检查。

8、负责与省公安厅、市公安局等有关计算机安全监察部门的联系及有关材料的组织、汇总和上报工作。

9、网络安全员根据国家、地方和学校的有关文件精神，根据校园网的工作需要，提出并组织制定和修订校园网的有关网络安全管理的各项规定并监督实施。

10、网络安全员须积极配合公安等安全和保密的有关执法部门，对网络违法案件进行调查和取证等工作。

11、做好校园网及学校各计算机的安全涉密工作。

**医院网络安全管理制度 建立网络安全管理制度篇四**

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账目，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、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，监控、封堵、清除网上有害信息。为了有效地防范网上非法活动，校园网要统一出口管理、统一用户管理，进出校园网访问信息的所有用户必须使用网络管理中心负责设立的代理服务器、email服务器。

十二、服务器必须保持日志记录功能，历史记录保持时间不得低于2个月。

**医院网络安全管理制度 建立网络安全管理制度篇五**

校园网是学校重要的基础设施之一，为全体师生提供先进、可靠、安全的\'计算机网络环境，支持学校的教学、科研、管理工作。为充分发挥校园网的作用，特制订本条例，希望广大师生共同遵守。

1、校园网使用者必须遵守国家有关法律、法规，必须认真学习遵守《中华人民共和国保守国家秘密法》和国家保密局《计算机信息系统国际互联网保密管理规定》。

2、学校各部门要加强对校园网新闻传播和信息内容的安全管理，对上网信息要进行审查，严格把关，落实防范措施。

3、校园网的所有用户必须接受学校依法进行监督检查和采取的必要措施。对校园网的所有设备要精心使用，如有损坏要按价赔偿。

4、学生上网必须有老师的具体指导，教师要引导学生正确、安全、健康地使用网络进行查阅资料、收集资料、利用资料等教育教学活动。

5、为了使学校的网络畅通无阻，发挥网络的积极作用，具有下列行为之一，对网络使用者的任何部门、任何人，一旦发现，经教育仍不改正者，将对该使用者取消上网资格，对部门将采取切断网络等相关措施。

（1）查阅、复制或传播下列信息的\'：

a、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；

b、煽动抗拒、破坏宪法和国家法律、行政法规的实施；

c、捏造或者歪曲事实，故意散布谣言，扰乱社会秩序；

d、公然侮辱他人或者捏造事实诽谤他人；

e、宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等；

f、破坏、盗用计算机网络中的信息资源和危害计算机网络安全活动；

g、故意制作、传播计算机病毒等破坏性程序。

（2）访问国家命令禁止的非法网站、国内外的反动、迷信、暴力、色情等不健康的网站。

（3）下载游戏等与教育教学无关的内容、下载并传播一些迷信、暴力、色情等不健康的内容。

**医院网络安全管理制度 建立网络安全管理制度篇六**

对于网络公司而言，做好网络安全管理工作非常重要，这时候，需要制订一套完善的网络安全管理制度。以下是关于安全管理规章制度范文，供各位参考。

1. 建立健全计算机信息网络电子公告系统的用户登记和信息管理制度；

2. 组织网络管理员学习《计算机信息网络国际联网安全保护管理办法》，提高网络安全员的警惕性。

3. 负责对本网络用户进行安全教育和培训。

4. 建立电子公告系统的网络安全管理制度和考核制度，加强对电子公告系统的审核管理工作，杜绝bbs上出现违犯《计算机信息网络国际联网安全保护管理办法》的内容。

1. 对版主的`聘用本着认真慎重的态度、认真核实版主身份，做好版主聘用记录。

2. 对各版聘用版主实行有针对性的网络安全教育，落实版主职责，提高版主的责任感。

3. 版主负责检查各版信息内容，如发现违反《计算机信息网络国际互联网安全保护管理办法》即时予以删除，情节严重者，做好原始记录，络管理员解决，由管理员向公安机关计算机管理监察机构报告。

4. 网络管理员负责对各版版主进行绩效管理考核，如发现不能正常履行版主职责者，将予以警告，严重者予以解聘。

5. 在版主负责栏目中发现重大问题未得到及时解决者，即时对版主予以解聘。

6. 加强网络管理员职责，配合各版版主的工作，共同维护电子公告板的信息安全。

1. 检查时严格按照《计算机信息网络国际互联网安全保护管理办法》、《网络安全管理制度》及《信息审核管理制度》（见附页）的标准执行。

2. 如发现违犯《计算机信息网络国际互联网安全保护管理办法》（见附页）的言论及信息，即时予以删除，情节严重者保留有关原始记录，并在二十四小时内向当地公安机关报告。

3. 负责对本网络用户进行安全教育和培训，网络管理员加强对《计算机信息网络国际互联网安全保护管理办法》的学习，进一步提高对网络信息安全维护的警惕性。

**医院网络安全管理制度 建立网络安全管理制度篇七**

计算机网络为集团局域网提供网络基础平台服务和互联网接入服务，由信息部负责计算机连网和网络管理工作。为保证集团局域网能够安全可靠地运行，充分发挥信息服务方面的重要作用，更好地为集团员工提供服务。现制定并发布《网络及网络安全管理制度》。

第一条 所有网络设备（包括光纤、路由器、交换机、集线器等）均归信息部所管辖，其安装、维护等操作由信息部工作人员进行。其他任何人不得破坏或擅自维修。

第二条 所有集团内计算机网络部分的扩展必须经过信息部实施或批准实施，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。信息部有权拆除用户私自接入的网络线路并进行处罚措施。

第三条 各部门的联网工作必须事先报经信息部，由信息部做网络实施方案。

第四条 集团局域网的网络配置由信息部统一规划管理，其他任何人不得私自更改网络配置。

第五条 接入集团局域网的客户端计算机的网络配置由信息部部署的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。

第六条 任何接入集团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。

第七条网络安全：严格执行国家《网络安全管理制度》。对在集团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。

第八条 集团员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。

第九条 任何人不得在局域网络和互联网上发布有损集团形象和职工声誉的信息。

第十条 任何人不得扫描、攻击集团计算机网络。

第十一条 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。

第十二条 为了避免或减少计算机病毒对系统、数据造成的影响，接入集团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信息部部署发布的`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。

第十三条 集团的互联网连接只允许员工为了工作、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。集团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。

第十四条 集团门户网即将改版成功，为了发挥好网站的形象宣传作用，各部室要及时向信息部提供有关资料，以便充实网站内容，加大宣传影响。由信息部统一整理、编辑上传及内容更新。

第十五条 各部门人员每日上班及时打开计算机，进入集团办公系统、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。

第十六条 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。

第十七条 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。

第十八条 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集团机密，对集团办公系统或其它集团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 建立网络安全管理制度篇八**

一、校园网络设施系学校贵重财产和精密设备，学校师生应严格执行有关规定。

二、校园网络要有完备的防火、防潮、防盗、防磁、防雷、防触电、防病毒和防黑客侵入等设备和措施。中心机房应安装空调，保持室温、温度稳定。

三、学校应制定《网络事故安全预案》，全校师生应掌握其相关内容。当发生紧急事件时按照《网络事故安全预案》进行处理。

四、校园网络管理人员负责监控校园网络的运行状态，随时了解网络运行情况，如有异常，应及时处理，保证学校的教育教学和各项管理正常进行。

五、校园网络管理人员应随时查看网络日志，屏蔽含有有害数据的网页。

六、全校师生不得在网络上发布不真实的.信息、散布有害信息（包括计算机病毒、反动信息等）、进入未经授权使用的计算机和不以真实身份使用网络资源，禁止访问不明网站。

七、学校师生不得在网络上发布不真实的信息、散布计算机病毒、进入未经授权使用的计算机和不以真实身份使用网络资源。

八、学校师生在发现有害信息或数据时，应及时向校园网络管理人员报告，并保护现场及相关资料。

九、全校教职工应对所使用的数据做好定期备份，在紧急时刻应立即备份。

**医院网络安全管理制度 建立网络安全管理制度篇九**

为了保护学校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，制定本安全管理制度：

1、校园网络使用者必须遵守国家有关法律、法规，必须遵守《中华人民共和国保守国家秘密法》和国家保密局《计算机信息系统国际互联网保密管理规定》。

2、校园网络的所有用户必须接受学校依法进行监督检查和采取的必要措施。遵守学校的管理制度，爱护网络设备，正确使用网络设备，保证网络设备的正常运行。

3、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账目，认真做好各项资料（软件）的记录、分类和妥善保存工作。

4、除信息处外，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。

5、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，交校办公室审核备案，由信息处从技术上开通其对外的信息服务。

6、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。

7、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。

8、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。

9、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。

10、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。

11、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。

12、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。

13、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 建立网络安全管理制度篇十**

为保证我公司网的.正常运行，防止各类病毒、黑客软件对公司内网主机构成的威胁，最大限度地减少此类损失，特制定本制度：

1、各接入部门计算机内应安装防病毒软件、防黑客软件及垃圾邮件消除软件，并对软件定期升级。

2、各接入单位计算机内严禁安装病毒软件、黑客软件，严禁攻击其它联网主机，严禁散布黑客软件和病毒。

3、信息中心应定期检测公司网内病毒和安全漏洞，并采取必要措施加以防治。

4、公司网内主要服务器应当安装防火墙系统，加强网络安全管理。

5、信息中心定期对网络安全和病毒检测进行检查，发现问题及时处理。

**医院网络安全管理制度 建立网络安全管理制度篇十一**

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。

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