# 最新单位网络安全管理制度(11篇)

来源：网络 作者：风吟鸟唱 更新时间：2024-09-21

*范文为教学中作为模范的文章，也常常用来指写作的模板。常常用于文秘写作的参考，也可以作为演讲材料编写前的参考。范文书写有哪些要求呢？我们怎样才能写好一篇范文呢？下面是小编帮大家整理的优质范文，仅供参考，大家一起来看看吧。单位网络安全管理制度篇...*

范文为教学中作为模范的文章，也常常用来指写作的模板。常常用于文秘写作的参考，也可以作为演讲材料编写前的参考。范文书写有哪些要求呢？我们怎样才能写好一篇范文呢？下面是小编帮大家整理的优质范文，仅供参考，大家一起来看看吧。

**单位网络安全管理制度篇一**

第二条本制度适用于公司内部办公局域网络和业务局域网络。

第三条职责。

(1)信息部。

①系统管理岗负责公司整体网络安全的规划、管理及其相关的技术支持。

②系统管理岗负责公司网络系统数据的安全备份。

③其他岗位协助系统管理岗进行公司网络的安全管理。

(2)各部门。

①负责各自部门使用的计算机网络设备的`安全管理。

②负责各自部门数据的安全备份。

③负责及时通知信息部有关计算机病毒发生情况及其他安全隐患情况。

第四条系统管理岗工作程序。

(1)公司整体网络安全的规划、管理。

(2)网络安全信息的追踪,黑客、病毒的日常防护工作。

①每天至少一次上网浏览相关网站,下载最新病毒代码。

②跟踪最新防病毒信息及其防杀方法,将其及时发布在公司内部网络上。

③及时跟踪防火墙的软硬件升级信息。

(3)负责公司本部办公网络安全防护工作。

①及时升级本公司网络的最新病毒代码。

②实时对各个工作终端进行病毒监测。

③及时将染病毒的工作终端逐一脱离网络。

④对染毒终端逐一进行全面查杀毒。

⑤及时对防火墙软、硬件进行升级。

⑥建立日常病毒记录日志,记录病毒代码。

(4)监督、检查、落实公司本部业务的网络安全防护措施等工作。

(5)协助本部相关部门进行重要数据的定期备份。

(6)业务、办公网数据的交换和相关数据输入、输出的管理。

第五条相关文件有《计算机及相关设备管理办法》和《计算机机房管理制度》。

第六条在《病毒记录日志》上做好记录。

**单位网络安全管理制度篇二**

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。

**单位网络安全管理制度篇三**

为了避免公司网络资源被滥用，提高工作效率，特别制定本规范，希望公司全体人员遵守规则，共同创造高效有序的网络环境。

适用于所有办公计算机及其使用者

1、p2p软件对网络资源的消耗极大，上班时间内严禁使用pps网络电视、酷狗音乐、qq网络音乐电视、bt电驴等p2p软件，以免影响他人工作正常上网，工作时间，不得下载、上传任何与工作无关的文件。

2、不滥用网络资源浏览无关网页、娱乐网站、购物网站、股票交易、bbs、blog等，禁止在工作时间登录qq、蚂蚁旺旺等聊天工具，如有特殊情况，必须填写计算机系统的使用申请书，所属部门一级部门长签字审查后，人事部人事审查通过未通过申请开通者，不得擅自在电脑上登录qq等聊天工具。

允许使用msn、qq等及时聊天工具的员工不使用qq/msn进行与工作无关的聊天，禁止访问土豆网、优酷网等所有流媒体网站。

3、所有工作人员应加强网络安全知识的学习，严禁故意输入计算机病毒及其他有害数据，危害公司网络系统安全，增强信息安全和保密意识，不能识别的信息不能下载，不能确定是否安全操作，慎重进行，以免被病毒侵入危害公司和自身。

4、所有网络工作人员禁止擅自建立个人wifi，目前个人wifi对公司局域网络有很大影响，给公司服务器和公司局域网环境带来巨大压力。

5、禁止利用互联网从事国家法律法规禁止的所有活动。

6、禁止通过互联网查看和下载国家法律法规禁止传播的所有信息。

7、未经单位领导批准，禁止在网上布与单位相关的所有信息。

8、不得在公司的局域网上发送与工作无关的信息和邮件。

9、不得在公司的计算机硬盘中保管与工作无关的资料、录像、mp3等文件。

10、禁止下载、安装与工作无关的程序或文件，未经信息化管理人员允许，不得擅自更改电脑网络设置、擅自安装或拆卸公司的it网络设备。

11、不得利用互联网泄露公司战略规划、经营数据、财务数据、业务资料、技术资料以及被公司列为保密范围内的信息和资料，严禁利用公司网络资源从事违反公司制度的活动。

12、信息化管理者负责审计和监视公司所有网络行为。

1、中层干部以上：正常登录qq，浏览正常网页，登录外部邮箱，下载文件。

2、员工水平：浏览通常的网页，登录外部邮箱。

3、工作单位的文士、各部门的资料员，不能问互联网。如果需要外部交流，可以申请开通qq。

因为员工需要工作，所以有必要申请开设网络权限的人，必须在所属部门的一级部门长签字审查后提交人事部人事审查通过后提交给信息化管理者。一级部门长要严格审查网络权限，网络权限大致分为五类

视频音乐类（包括优酷、马铃薯、qq音乐、酷等流媒体音乐网站）

新闻类（网络及时发布的新闻）

即时通信类（qq、蚂蚁旺旺等聊天软件）

消费类（淘宝、京东等购物网站）

网络游戏类（魔兽世界、炫耀舞蹈、qq游戏等流行的主流网络游戏）

员工开设的网络权限默认不能使用以上5种网络权限。如果需要开设权限，请在计算机系统中使用申请书，详细说明原因。如果没有详细说明，信息管理者有权禁止开通。

4、公司客户的网络使用公司建立的wifi网络，各专家室的wifi密码由制造部项目经理管理，如客户需要连接wifi使用网络，项目经理通知客户使用网络。

附件：如果员工的个人电脑需要在办公室通过互联网的话，默认的互联网权限不能使用5种。

1、公司的所有计算机和周边设备都是公司的固定资产，必须根据实际工作需要配备给各部门的人员，各部门的人员必须保护整理，保证良好的使用环境。

2、信息化管理人员对公司的.所有计算机设备进行统一编号，建立计算机硬件明细户，定期维护和检查硬件各部门的使用情况。

3、硬件故障：各部门使用者发现硬件时，应立即向信息管理者说明情况，由信息管理者确定及时处理，各部门人员不得擅自更换硬件设备。

4、设备追加、更换、升级各部门根据实际工作需要提出申请，填写固定资产购买申请书，经相关负责人批准后，由信息管理者确定具体配置，通知购买部购买。

5、部门需要接受消耗品（如键盘鼠标、键盘等）时，需要向信息化管理员填写消耗品申请签字确认，申请必须明确记载消耗品申请的原因。申请一级部门长或主管批准后，由信息管理员发行（原则上更换）。

6、电脑使用者是该设备的负责人，使用部门是负责部门。未经责任部门长批准，任何人都不得使用其他部门或其他人的电脑。各部门查阅互联网数据的公共电脑由各组长管理和监督。

7、信息管理员负责审计和监控公司所有计算机硬件的使用。

1、设计软件和应用软件的使用、安装：各部门和人员使用的软件（办公软件）可以自己安装，如果不安装，信息管理者可以负责安装。

2、软件故障：各部门使用者发现软件故障时，应立即向信息管理者说明情况，由信息管理者确定并立即处理。

3、员工不得擅自在工作机上安装与工作无关的程序，mp3、视频文件播放程序、聊天工具、游戏等。

4、公司所有计算机（包括个人计算机办公室）必须设置企业版360（禁止使用其他杀菌软件），企业版360设置地址http：//192.168.1.48：8080/

5、公司计算机名称统一由信息化管理者制作，局域网ip地址统一由信息化管理者分配，不得擅自变更，擅自变更计算机名称和mac地址的通报批评。

6、信息化管理负责审计和监控公司所有计算机软件的使用。

1、故意更换、破坏计算机和周边硬件设备的人，以成本的2倍的价格赔偿，公开通报。

2、上班时间利用电脑玩游戏、炒股、网上购物、看电影、听音乐等与工作无关的人，给予50―200元的处罚。

3、网络违规处理方法：如违反上述规定，发现一次罚款100元，重复发生的双倍处罚

本规定自发布之日起生效！

**单位网络安全管理制度篇四**

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。

**单位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。

**单位网络安全管理制度篇六**

第一条目的为维护公司网络安全，保障信息安全，保证公司网络系统的畅通，有效防止病毒入侵，特制定本制度。

第二条适用范围本制度适用于公司网络系统管理。

第三条职责

1、集团业务处负责公司网络系统的安全管理和日常系统维护，制定相关制度并参加检查。

2、集团办公室会同相关部门不定期抽查网络内设备安全状态，发现隐患及时予以纠正。

3、各部门负责落实网络安全的各项规定。

第四条网络安全管理范围网络安全管理须从以下几个方面进行规范：物理层、网络层、平台安全，物理层包括环境安全和设备安全、网络层安全包含网络边界安全、平台安全包括系统层安全和应用层安全。

第五条机房安全

1、公司网络机房是网络系统的\'核心。除管理人员外，其他人员未经允许不得入内。

2、管理人员不准在主机房内会客或带无关人员进入。

3、未经许可，不得动用机房内设施。

第六条机房工作人员进入机房必须遵守相关工作制度和条例，不得从事与本职工作无关的事宜，每天上、下班前须检查设备电源情况，在确保安全的情况下，方可离开。

第七条为防止磁化记录的破坏，机房内不准使用磁化杯、收音机等产生磁场的物体。

第八条机房工作人员要严格按照设备操作规程进行操作，保证设备处于良好的运行状态。

**单位网络安全管理制度篇七**

为加强公司网络系统的安全管理,防止因偶发性事件、网络病毒等造成系统故障,妨碍正常的工作秩序,特制定本管理办法。

一、网络系统的安全运行,是公司网络安全的一个重要内容,有司专人负责网络系统的安全运行工作。

二、网络系统的安全运行包括四个方面:一是网络系统数据资源的安全保护,二是网络硬件设备及机房的安全运行,三是网络病毒的防治管理,四是上网信息的安全。

(一)数据资源的安全保护。网络系统中存贮的`各种数据信息,是生产和管理所必须的重要数据,数据资源的破坏将严重影响生产与管理工作的正常运行。数据资源安全保护的主要手段是数据备份,规定如下:

1、办公室要做到数据必须每周一备份。

2、财务部要做到数据必须每日一备份

3、一般用机部门要做到数据必须每周一备份。

4、系统软件和各种应用软件要采用光盘及时备份。

5、数据备份时必须登记以备检查,数据备份必须正确、可靠。

6、严格网络用户权限及用户名口令管理。

(二)硬件设备及机房的安全运行

1、硬件设备的供电电源必须保证电压及频率质量,一般应同时配有不间断供电电源,避免因市电不稳定造成硬件设备损坏。

2、安装有保护接地线,必须保证接地电阻符合技术要求(接地电阻≤2ω,零地电压≤2v),避免因接地安装不良损坏设备。

3、设备的检修或维护、操作必须严格按要求办理,杜绝因人为因素破坏硬件设备。

4、网络机房必须有防盗及防火措施。

5、保证网络运行环境的清洁,避免因集灰影响设备正常运行。

(三)网络病毒的防治

1、各服务器必须安装防病毒软件,上网电脑必须保证每台电脑要安装防病毒软件。

2、定期对网络系统进行病毒检查及清理。

3、所有u盘须检查确认无病毒后,方能上机使用。

4、严格控制外来u盘的使用,各部门使用外来u盘须经检验认可,私自使用造成病毒侵害要追究当事人责任。

5、加强上网人员的职业道德教育,严禁在网上玩游戏,看于工作无关的网站,下载歌曲图片游戏等软件,一经发现将严肃处理。

(四)上网信息及安全

1、网络管理员必须定期对网信息检查,发现有关泄漏企业机密及不健康信息要及时删除,并记录,随时上报主管领导。

2、要严格执行国家相关法律法规,防止发生窃密、泄密事件。外来人员未经单位主管领导批准同意,任何人不得私自让外来人员使用我公司的网络系统作任何用途。

3、要加强对各网络安全的管理、检查、监督,一旦发现问题及时上报公司负责人。公司计算机安全负责人分析并指导有关部门作好善后处理,对造成事故的责任人要依据情节给予必要的经济及行政处理。

五、未经公司负责人批准,联结在公司网络上的所有用户,严禁在同过其它入口上因太网或公司外单位网络.

**单位网络安全管理制度篇八**

1、学校计算机网络系统的安全运行和系统设备管理维护工作由信息中心负责，任何部门和个人未经同意，不得擅自安装、拆卸或改变网络设备。

2、不准通过学校内部网络发布和工作无关的信息；不准通过电子邮件、bbs、chat等方式发布不健康的、xxx的、或者和工作无关的信息。任何部门和个人不得在学校计算机网络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。

3、任何部门和个人不得利用联网计算机从事危害计算机网络系统的活动，不得危害或侵入未授权的服务器或工作站。不准通过内部网络从事和工作无关的\'活动，包括：不准攻击内部或者外部的任何机器。不得以任何方式对服务器、工作站进行修改、设置、删除等操作。不得以任何借口盗窃、破坏网络设施，这些行为视为对学校计算机网络安全运行的破坏行为。

4、不准将工作用机交给非校内人员使用。不准擅自使用他人的机器；不准通过他人的机器从事违反规定的活动。

5、任何部门不得在学校计算机网络上从事对用户帐户及口令的侦听、盗用活动，对其他网站的恶意攻击或黑客攻击行动。

6、严禁在计算机上安装游戏软件，严禁使用来历不明，易引发病毒传染的软件。对来历不明的可能引起计算机病毒的软件应使用公安部门推荐的杀毒软件检查、杀毒。

7、各处室、教研组对上网计算机的使用要严格管理，部门负责人为网络安全责任人。公共机房不准对社会开放。

8、所有教师必须认真保管自己的机器账号和网管部授权使用的账号；所有账号至少要每个季度更新一次。

9、网管部门要加强监控和管理；在学校网关上要配置防火墙和监控服务器；对外部ip加强管理，落实到人头；服务器账号要加强管理，落实责任人。

10、以上规定，请大家自觉遵守。如有违背，学校将酌情处理；必要的时候，交由公安机关处理。

**单位网络安全管理制度篇九**

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、网络中心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，未经校园网网络中心同意，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、校园网由学校电教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。

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。

4、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。

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。

9、禁止私自安装、卸载程序，在校园网上，禁止使用盗版软件，不允许玩电子游戏，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、软盘上的文件应使用合格的杀毒软件进行检查、消毒。

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，发现故障及时通知网络中心处理。

16、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。

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、复制和传播有碍社会治安和有伤风化的信息。

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，这些行为被视为对校园网安全运行的破坏行为。

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，不随意把户头借给他人使用，增强自我保护意识，经常更换口令，保护好户头和ip地址。严禁用各种手段破解他人口令、盗用户头和ip地址。

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，该活动被认为是对网络用户权益的侵犯。

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。

1、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。

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。

**单位网络安全管理制度篇十**

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。

**单位网络安全管理制度篇十一**

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。

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