# 最新医保网络安全管理制度(12篇)

来源：网络 作者：风华正茂 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。大家想知道怎么样才能写一篇比较优质的范文吗？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。医保网络安全管理制度篇一1、校园网络使...*

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。大家想知道怎么样才能写一篇比较优质的范文吗？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。

**医保网络安全管理制度篇一**

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、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。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。

(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。

6、计算机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。

7、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。

8、认真做好本单位计算机的养护和清洁卫生工作。

9、全体师生有义务向学校网络管理员报告违法行为和有害的、不健康的信息。

**医保网络安全管理制度篇二**

为确保单位网络安全、高效运行和网络设备运行处于良好状态，正确使用和维护网络设备安全，特制定本制度。

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。

**医保网络安全管理制度篇三**

1、机房设备是国土资源广域网、局域网和门户网站赖以运行的载体。隐患险于明火，防范胜于救灾，责任重于泰山。信息中心工作人员要以高度的责任心确保机房设备的安全、正常运行。

2、非信息中心工作人员严禁出入机房。除信息中心人员外，任何人不得接触和使用服务器、路由器、交换机、防火墙等网络设备。网络管理人员必须遵守安全操作程序，不得安装与工作无关的软件系统。

3、网络设备参数为局内部工作秘密，任何人不得向外泄露。系统管理员须定期更换服务器登陆密码，并做好记录。

4、凡在服务器上开通ftp的\'，须报信息中心和局领导同意后方可实施。所有工作人员使用的计算机拟接入互联网，须经局领导同意，信息中心人员不得擅自实施。

5、机房所有设备仅为全局工作服务，禁止利用机房设备对外承接业务，严禁将机房设备带出机房使用。

6、加强机房消防安全管理。定期对机房供电线路及照明器具等进行检查，防止因线路老化等原因造成火灾。定期检查更换消防用品。

7、保持机房的温湿度，特别防止温度过高对设备造成损害。

8、严禁易燃易爆和强磁物品及其它与机房工作无关的物品进入机房。

9、机房内禁止吸烟、用餐、吃零食、打牌下棋、嬉戏喧哗等行为。

10、进入机房必须换拖鞋或用鞋套。机房设备、桌椅等确保没有积尘和污迹，地面无尘，保持机房整洁。

11、建立机房人员值班制度。值班人要对当日值班期间网络运行情况、温湿度情况等做好详细记录。交接班时须履行相关手续，注明交接时间。

12、建立运转灵活、反应灵敏的网络应急处理协调机制，确保发生突发网络安全紧急事件时，能够准确判断、快速反应，尽可能避免、减少突发事件给广域网和局域网运行带来的影响。

13、建立机房管理责任人制度。责任人要加强管理和监督，落实以上制度，建好网络设备及线路端口分布(变动)、设备故障排除等台账。机房管理责任人必须于周一上午上班后和周五下午下班前，对所有设备运行状况和运行环境进行全面检查并做好记录，发现问题及时处理，重大情况及时报告。网络发生故障或隐患时，须对所发生的故障现象、处理过程和结果等做好详细记录。

14、中心机房是局重点防盗、防火部门。大楼值班人员必须重点关注。非正常上班期间，如遇长时间停电，须提前告知信息中心，以便及时采取应急措施。

15、违反以上规定者，视情节轻重对当事人进行严肃处理，造成损失的，由当事人赔偿，并追究相关责任。

**医保网络安全管理制度篇四**

1、采取严密的安全措施防止无关用户进入系统；

2、数据库管理系统的口令必须由电脑中心专人掌管，并要求定期更换。禁止同一人掌管操作系统口令和数据库管理系统口令；

3、操作人员应有互不相同的用户名，定期更换操作口令。

4、严禁操作人员泄露自己的`操作口令；

5、各岗位操作权限要严格按岗位职责设置。应定期检查操作员的权限；

6、重要岗位的登录过程应增加必要的限制措施；

**医保网络安全管理制度篇五**

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。

**医保网络安全管理制度篇六**

1、目的

维护公司计算机网络安全、正常运行，确保服务器及各个终端正常使用。使网络资源充分安全共享，为业务经营活动提供安全的网络环境。

2、适用范围

适用于公司内部办公局域网络，业务局域网络、国大药房、国瑞药业、国药物流的网络。

3、职责

3.1 信息部

3.1.1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。

3.1.2系统管理岗负责公司网络系统数据的安全备份。

3.1.3其它岗位协助系统管理岗进行公司网络的安全管理。

3.2 各部门

3.2.1负责各自部门使用的计算机网络设备的安全管理。

3.2.2负责各自部门数据的安全备份。

3.2.3负责及时通知信息部有关各自部门使用的计算机病毒发生情况及其它安全隐患情况。

4、工作程序

4.1 公司整体网络安全的规划、管理。

4.2 网络安全信息的追踪，黑客、病毒的\'日常防护工作。

4.2.1 每天至少一次上网浏览相关网站，下载最新病毒代码

4.2.2 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。

4.2.3及时跟踪防火墙的软硬件升级信息。

4.3 负责公司本部办公网网络安全防护工作。

4.3.1 及时升级本公司网络的最新病毒代码。

4.3.2 实时对各个工作终端进行病毒监测。

4.3.3 及时将染病毒的工作终端逐一脱离网络。

4.3.4 对染毒终端逐一进行全面查杀毒。

4.3.5 及时对防火墙软硬件进行升级。

4.3.6 建立日常病毒记录日志，记录病毒代码。（参见《病毒记录日志》）

4.4 监督、检查、落实公司本部业务、国大药房、国瑞药业、国药物流的网络安全防护措施等工作。

4.5 协助本部相关部门进行重要数据的定期备份。

4.6 业务、办公网数据的交换和相关数据输入输出的管理。

5、相关文件

《计算机及相关设备管理办法》

《计算机机房管理制度》

6、记录

《病毒记录日志》

**医保网络安全管理制度篇七**

第一条 所有接入网络的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连网计算机从事危害城域网及校园网防火墙、路由器、交换机、服务器等网络设备的活动。不得在网络上制作、发布、传播下列有害内容：

（一）泄露国家秘密，危害国家安全的；

（二）违反国家民族、宗教与教育政策的；

（三）煽动暴力，宣扬封建迷信、邪教、黄色淫秽，违反社会公德，以及赌博、诈骗和教唆犯罪的；

（四）公然侮辱他人或者捏造事实诽谤他人的，暴露个人隐私和攻击他人与损害他人合法权益的；

（五）散布谣言，扰乱社会秩序，鼓励聚众滋事的；

（六）损害社会公共利益的；

（七）计算机病毒；

（八）法律和法规禁止的其他有害信息。

如发现上述有害信息内容，应及时向三门县教育局现代教育中心或上级主管部门报告，并采取有效措施制止其扩散。

第二条 在网站上发现大量有害信息，以及遭到黑客攻击后，必须在12 小时内向三门县教育局现代教育中心及公安机关报告，并协助查处。在保留有关上网信息和日志记录的前题下，及时删除有关信息。问题严重、情况紧急时，应关闭交换机或相关服务器。

第三条 任何单位和个人不得在校园网及其连网的计算机上收阅下载传递有政治问题和淫秽色情内容的信息。

第四条 所有接入网络的用户必须对提供的信息负责，网络上信息、资源、软件等的使用应遵守知识产权的有关法律法规。对于运行无合法版权的网络软件而引起的\'版权纠纷由使用部门（ 个人） 承担全部责任。

第五条 严禁在网络上使用来历不明、引发病毒传染的软件，对于来历不明的可能引发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。

第六条 认真执行各项管理制度和技术规范，监控、封堵、清除网上有害信息。为有效地防范网上非法活动、各子网站要加强出口管理和用户管理。重要网络设备必须保持日志记录，时间不少于180 天。

第七条 上网信息管理坚持“ 谁上网谁负责、谁发布谁负责” 的原则。对外发布信息，必须经局机关或各单位负责人审核批准后，才可发布（具体操作方法可参考“ 网络信息发布管理制度” ）。

第八条 各单位和学校要确定一名行政人员为本单位（学校）网络安全责任人，领导网管员（网管机构）做好本单位和学校的网络和信息安全工作。建立岗位责任制和机房管理制度。网络管理人员应加强责任心，保证现有各种网络设备良好运行，充分发挥效率。

第九条 单位和学校各信息终端用户必须受网络管理员监督管理。整个单位和校园要统一出口、统一用户管理。建立帐号登记管理制度，用户帐号只能专人专用，方便日后的检查和监督工作。

第十条 与城域网及单位和学校网络相连的机房建设，应当符合国家的有关标准和规定，在电源防护、防盗、防火、防水、防尘、防雷等方面，采取规范的技术保护措施。

第十一条 城域网及校园网站的系统软件、应用软件及信息数据要实施保密措施。接入互联网网的计算机必须与本部门的涉密计算机信息系统实行物理隔离。涉密信息不得在上网设备上操作或存储。信息资源保密等级可分为：

（一）可向internet 公开的；

（二）可向本城域网公开的；

（三）可向有关单位或个人公开的；

（四）可向本单位公开的；

（五）仅限于个人使用的。

第十二条 任何单位和个人不得利用联网计算机从事下列活动：

（一）未经允许，非法访问教育城域网及校园网上网络服务器、工作站、交换机、路由器及其它相关设备；对教育城域网上所具有的功能、程序、数据进行删除、修改和增加；

（二）未经允许，擅自提供与教育无关的网络服务；

（三）故意制作、传播计算机病毒与破坏性程序；

（四）其他危害教育城域网络安全的行为。

第十三条 违反本管理制度，将提请有关部门视情节给予相应的批评教育、通报批评或行政处分、处以警告或停机整顿。触犯国家有关法律、行政法规的，依照有关法律、行政法规的规定予以处罚；构成犯罪的，依法追究刑事责任。

第十四条故意输入计算机病毒，造成危害城域网及子网站网络安全的，按《中华人民共和国计算机信息系统安全保护条例》中第二十三条的规定予以处罚。

**医保网络安全管理制度篇八**

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。

**医保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。

**医保网络安全管理制度篇十**

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！

**医保网络安全管理制度篇十一**

第一条为维护公司计算机网络安全、正常运行,确保服务器及各个终端正常使用。使网络资源充分安全共享,为业务经营活动提供安全的网络环境。

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。

**医保网络安全管理制度篇十二**

一、严格遵守国家有关涉及互联网方面的法律法规；

二、坚决封堵互联网上不良和有害信息的\'侵入；

三、积极配合公安机关的网络信息安全部门检查；

四、按照备案要求，及时备案本单位在互联网应用方面的变更信息；

五、在本单位建立网络信息安全保护小组，并报公安机关的网络安全部门备案；

六、根据本单位在互联网应用的实际情况，在安全员、安全教育和培训、机房管理、安全保护技术措施、巡视上报、用户登记、帐号使用和操作权限管理等方面制定以下细则制度。

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