# 2024网络安全管理制度完整版

作者：夜幕降临 更新时间：2025-03-06

*20\_网络安全管理制度完整版6篇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。多多范文网小编：夜幕降临 小编为大家整理了2024网络安全管理制度完整版，分享给有需要的朋友...*

20\_网络安全管理制度完整版6篇

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。多多范文网小编：夜幕降临 小编为大家整理了2024网络安全管理制度完整版，分享给有需要的朋友。!

**20\_网络安全管理制度完整版 【篇1】**

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。

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，现制定并发布《文山中学网络安全管理制度》。

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、备份和数据工作，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。

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。

为了认真贯彻落实公安部《关于开展重要信息系统和重点网站网络安全保护状况自检自查工作的通知》文件精神，为进一步做好我院网络与信息系统安全自查工作，提高安全防护能力和水平，预防和减少重大信息安全事件的发生，切实加强网络与信息系统安全防范工作，创造良好的网络信息环境。近期，我院进行了信息系统和网站网络安全自查，现就我院网络与信息系统安全自查工作情况汇报如下：

一、网络与信息安全自查工作组织开展情况

(一)自查的总体评价

我院严格按照公安部对网络与信息系统安全检查工作的要求，积极加强组织领导，落实工作责任，完善各项信息系统安全制度，强化日常监督检查，全面落实信息系统安全防范工作。今年着重抓了以下排查工作：一是硬件安全，包括防雷、防火和电源连接等;二是网络安全，包括网络结构、互联网行为管理等;三是应用安全，公文传输系统、软件管理等，形成了良好稳定的安全保密网络环境。

(二)积极组织部署网络与信息安全自查工作

1、专门成立网络与信息安全自查协调领导机构

成立了由分管领导、分管部门、网络管理组成的信息安全协调领导小组，确保信息系统高效运行、理顺信息安全管理、规范信息化安全等级建设。

2、明确网络与信息安全自查责任部门和工作岗位

我院领导非常注重信息系统建设，多次开会明确信息化建设责任部门，做到分工明确，责任具体到人。

3、贯彻落实网络与信息安全自查各项工作文件或方案

信息系统责任部门和工作人员认真贯彻落实市工业和信息化委员会各项工作文件或方案，根据网络与信息安全检查工作的特点，制定出一系列规章制度，落实网络与信息安全工作。

4、召开工作动员会议，组织人员培训，专门部署网络与信息安全自查工作

我院每季度召开一次工作动员会议，定期、不定期对技术人员进行培训，并开展考核。技术人员认真学习贯彻有关文件精神，把信息安全工作提升到重要位置，常抓不懈。

二、信息安全主要工作情况

(一)网络安全管理情况

1、认真落实信息安全责任制

我院制定出相应信息安全责任追究制度，定岗到人，明确责任分工，把信息安全责任事故降低到最低。

2、积极推进信息安全制度建设

(1)加强人员安全管理制度建设

我院建立了人员录用、离岗、考核、安全保密、教育培训、外来人员管理等安全管理制度，对新进人员进行培训，加强人员安全管理，不定期开展考核。

(2)严格执行机房安全管理制度

我院制定出《机房管理制度》，加强机房进出人员管理和日常监控制度，严格实施机房安全管理条例，做好防火防盗，保证机房安全。

(二)技术安全防范和措施落实情况

1、网络安全方面

我院配备了防病毒软件、网络隔离卡，采用了强口令密码、数据库存储备份、移动存储设备管理、数据加密等安全防护措施，明确了网络安全责任，强化了网络安全工作。计算机及网络配置安装了专业杀毒软件，加强了在防病毒、防攻击、防泄密等方面的有效性。并按照保密规定，在重要的涉密计算机上实行了开机密码管理，专人专用，杜绝涉密和非涉密计算机之间的混用。

2、信息系统安全方面

涉密计算机没有违规上国际互联网及其他的信息网的情况，未发生过失密、泄密现象。实行领导审查签字制度凡上传网站的信息，须经有关领导审查签字后方可上传;二是开展经常性安全检查，主要对SQL注入攻击、跨站脚本攻击、弱口令、操作系统补丁安装、应用程序补丁安装、防病毒软件安装与升级、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监管，认真做好系统安全日记。

(三)应急工作情况

1、开展日常信息安全监测和预警

我院建立日常信息安全监测和预警机制，提高处置网络与信息安全突发公共能力事件，加强网络信息安全保障工作，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网站网络与信息安全突发公共事件的危害。

2、建立安全事件报告和响应处理程序

我院建立健全分级负责的应急管理体制，完善日常安全管理责任制。相关部门各司其职，做好日常管理和应急处置工作。设立安全事件报告和相应处理程序，根据安全事件分类和分级，进行不同的上报程序，开展不同的响应处理。

3、制定应急处置预案，定期演练并不断完善

我院制定了安全应急预案，根据预警信息，启动相应应急程序，加强值班值守工作，做好应急处理各项准备工作。定期演练预警方案，不断完善预警方案可行性、可操作性。

(四)安全教育培训情况

为保证我院网络安全有效地运行，减少病毒侵入，我院就网络安全及系统安全的有关知识进行了培训。期间，大家对实际工作中遇到的计算机方面的有关问题进行了详细的咨询，并得到了满意的答复。

三、网络与信息安全存在的问题

经过安全检查，我单位信息系统安全总体情况良好，但也存在了一些不足：

1、信息安全意识不够。员工的信息安全教育还不够，缺乏维护信息安全主动性和自觉性。

2、设备维护、更新还不够及时。

3、专业技术人员少，信息系统安全力量有限，信息系统安全技术水平还有待提高。

4、信息系统安全工作机制有待进一步完善。

四、网络与信息安全改进措施

根据自查过程中发现的不足，同时结合我院实际，将着重以下几个方面进行整改：

一是要继续加强对全员的信息安全教育，提高做好安全工作的主动性和自觉性。

二是要切实增强信息安全制度的落实工作，不定期的对安全制度执行情况进行检查，对于导致不良后果的责任人，要严肃追进责任，从而提高人员安全防范意识。

三是要加强专业信息技术人员的培养，进一步提高信息安全工作技术水平，便于我们进一步加强计算机信息系统安全防范和工作。

四是要加大对线路、系统、网络设备的维护和保养，同时，针对信息技术发展迅速的特点，要加大系统设备更新力度。

五是要创新完善信息安全工作机制，进一步规范办公秩序，提高信息工作安全性。

五、关于加强信息安全工作的意见和建议

我们在管理过程中发现了一些管理方面存在的薄弱环节，今后我们还要在以下几个方面进行改进：

一是对于线路不整齐、暴露的，立即对线路进行限期整改，并做好防鼠、防火安全工作。

二是加强设备维护，及时更换和维护好故障设备。

三是自查中发现个别人员计算机安全意识不强。在以后的工作中，我们将继续加强计算机安全意识教育和防范技能训练，让员工充分认识到计算机案件的严重性。人防与技防结合，确实做好单位的网络安全工作。

按照汉区宣字〔20\_\_〕17号《关于在全区开展关键信息基础设施网络安全检查的通知》文件精神要求，我镇高度重视，立即对网络安全工作进行了全面检查，现将自查情况报告如下：

一、网络安全情况

吉河镇网络建设运行以来，一直对安全工作十分重视，成立了专门的网络安全领导小组，积极完善各项安全制度，严格落实有关网络安全的各项管理规定，采取了多种措施防范网络安全事件的发生，近年来未发生安全事故，保障了网络安全、稳定、高效运行，为全镇各项工作的开展奠定了坚实基础。

1、组织管理

我镇高度重视网络安全工作，成立了由主要领导任组长，分管领导任副组长，站所办负责人为成员的网络安全领导小组，领导小组下设办公室，抽调具体工作人员负责办公。召开了由分管领导、网络安全职能部门和重点部门负责人参加的会议，对上级文件进行了认真学习，对自查工作做了周密部署，确定了自查任务和人员分工，真正做到了领导到位、机构到位、人员到位、责任到位。为确保网络安全工作顺利开展，要求镇全体干部充分认识网络安全工作的重要性，认真学习网络安全知识，都能按照网络安全的各种规定，正确使用计算机网络和各类信息系统。

2、日常管理

针对网络安全工作的特点，结合我镇实际，制定了《网络安全管理办法》、《视频会议管理制度》、《电子政务平台操作系统操作指南》等一系列网络安全制度和规定。网站信息发布由专人负责，并进行登记;杀毒软件和防火墙均为国内产品;网站上传信息前均在本地进行病毒检测;禁止携带移动存储介质进入电子政务平台专用计算机。

3、防护管理

全镇网络设备、服务器等均运转正常。所有网络设备、信息系统等按规定设置高强度密码并定期进行更换;开展经常性安全检查，主要对SQL注入攻击、跨站脚本攻击、弱口令、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监控，认真检查保管系统安全。

4、应急管理

进一步完善了网络安全应急预案，明确了应急处理流程，落实了应急技术支持队伍;对重要文件、数据进行定期自动备份。

5、安全检查

对系统和软件等及时更新补丁;对防病毒软件和防火墙升级病毒代码特征库;定期对网站进行查杀、漏洞扫描、检测和修复。

二、20\_\_年网络安全工作情况

成立了吉河镇网络安全工作领导小组，全面负责网络安全工作;修订完善了《网络安全管理规定》等一系列制度;新增了2名网络工作人员，充实了技术队伍;开展了网络安全应急处理培训;让网络工作人员定期在网上收听信息安全教育讲座。

三、检查发现的主要问题及整改情况

通过这次自查，我们也发现了当前存在的一些问题：

1、部分干部网络安全意识不强，日常运维缺乏主动性和自觉性。

2、专业技术人员较少，网络安全知识、技术、经验欠缺。

3、网络安全经费投入不足，软、硬件设备需要进行改善。

4、规章制度尚不完善，未能涉及到网络安全的所有方面。

针对自查过程中发现的问题，结合我镇实际情况，将在以下几个方面进行整改：

1、进一步加强对全镇干部和网络工作人员的安全意识教育，提高做好安全工作的主动性和自觉性，增强对网络安全的防范意识。

2、多参加市区和专业机构举办的网络安全技术培训，增强安全防范意识和应对能力，提高工作人员的水平和能力，提高网络安全管理水平。

3、完善网络安全制度，同时安排专人，密切监测，及时发现网络安全隐患。

4、加大投入，继续完善网络安全设施，从边界防护、访问控制、入侵检测、病毒防护等方面建立起全方位的安全体系。

四、对网络安全工作的意见和建议

1、市区要经常组织召开专家讲座和座谈会等形式多样的经验交流活动。

2、经常组织网络安全方面的专门培训，增强安全防范意识，提高网络管理人员的专业水平。

为进一步加强我院信息系统的安全管理，强化信息安全和保密意识，提高信息安全保障水平，按照省卫计委《关于\_\_省卫生系统网络与信息安全督导检查工作的通知》文件要求，我院领导高度重视，成立专项管理组织机构，召开相关科室负责人会议，深入学习和认真贯彻落实文件精神，充分认识到开展网络与信息安全自查工作的重要性和必要性，对自查工作做了详细部署，由主管院长负责安排、协调相关检查部门、监督检查项目，建立健全医院网络安全保密责任制和有关规章制度，严格落实有关网络信息安全保密方面的各项规定，并针对全院各科室的网络信息安全情况进行了专项检查，现将自查情况汇报如下：

一、医院网络建设基本情况

我院信息管理系统于\_\_年\_\_月由\_\_\_\_科技有限公司对医院信息管理系统(HIS系统)进行升级。升级后的前台维护由本院技术人员负责，后台维护及以外事故处理由\_\_\_\_科技有限责任公司技术人员负责。

二、自查工作情况

1、机房安全检查。机房安全主要包括：消防安全、用电安全、硬件安全、软件维护安全、门窗安全和防雷安全等方面安全。医院信息系统服务器机房严格按照机房标准建设，工作人员坚持每天定点巡查。系统服务器、路由器都有UPS电源保护，可以保证在断电3个小时情况下，设备可以运行正常，不至于因突然断电致设备损坏。

2、局域网络安全检查。主要包括网络结构、密码管理、IP管理、存储介质管理等;HIS系统的操作员，每人有自己的登录名和密码，并分配相应的操作员权限，不得使用其他人的操作账户，账户施行“谁使用、谁管理、谁负责”的管理制度。院内局域网均施行固定IP地址，由医院统一分配、管理，无法私自添加新IP，未经分配的IP无法连接到院内局域网。我院局域网内所有计算机USB接口施行完全封闭，有效地避免了因外接介质(如U盘、移动硬盘)而引起中毒或泄密的发生。

3、数据库安全管理。我院对数据安全性采取以下措施：

(1)将数据库中需要保护的部分与其他部分相隔。

(2)采用授权规则，如账户、口令和权限控制等访问控制方法。

(3)数据库账户密码专人管理、专人维护。

(4)数据库用户每6个月必须修改一次密码。

(5)服务器采取虚拟化进行安全管理，当当前服务器出现问题时，及时切换到另一台服务器，确保客户端业务正常运行。

三、应急处置

我院HIS系统服务器运行安全、稳定，并配备了大型UPS电源，可以保证在大面积断电情况下，服务器可运行六小时左右。我院的HIS系统刚刚升级上线不久，服务器未发生过长宕机时间，但医院仍然制定了应急处臵预案，并对收费操作员和护士进行了培训，如果医院出现大面积、长时间停电情况，HIS系统无法正常运行，将临时开始手工收费、记账、发药，以确保诊疗活动能够正常、有序地进行，待到HIS系统恢复正常工作时，再补打发票、补记收费项目。

四、存在问题

我院的网络与信息安全工作做的比较认真、仔细，从未发生过重大的安全事故，各系统运转稳定，各项业务能够正常运行。但自查中也发现了不足之处，如目前医院信息技术人员少，信息安全力量有限，信息安全培训不全面，信息安全意识还够，个别科室缺乏维护信息安全的主动性和自觉性;应急演练开展不足;机房条件差;个别科室的计算机设备配臵偏低，服务期限偏长。

今后要加强信息技术人员的培养，提升信息安全技术水平，加强全院职工的信息安全教育，提高维护信息安全的主动性和自觉性，加大对医院信息化建设投入，提升计算机设备配臵，进一步提高工作效率和系统运行的安全性。

**20\_网络安全管理制度完整版**

本文档由范文网【dddot.com】收集整理，更多优质范文文档请移步dddot.com站内查找