



迁西县职业技术教育中心

Qianxi Vocational and technical education center

迁西职教中心

信息化设备与使用管理制度



目录

迁西职教中心数字化校园管理制度	1
信息中心机房管理制度	5
网络安全管理制度	7
安全教育培训制度	9
信息内容审核制度	10
信息中心保密制度	11
教师入网管理制度	12
计算机教室上机制度	13
多媒体教室教学系统使用管理制度	15
校园无线网络安全管理制 度	17
迁西职教中心软件正版化管理办法	18
《计算机信息网络国际联 网安全保护管理办法》	21
迁西职教中心笔记本电脑 使用与管理制度	27
迁西职教中心监控系统管 理制度	29



迁西职教中心数字化校园管理制度

总则

为了保障我校校园网络系统安全、促进我校校园数字化应用和发展、保证校园网络的正常运行，为我校师生提供一个先进、可靠、安全的计算机信息化网络教学、科研和办公环境，促进学校与外界的信息交流、资源共享和科研合作，制定本管理条例。

第一章 管理组织机构

第一条 校园网管理小组由学校校长、分管副校长、行政办、教务处、政务处和学校信息中心负责人组成，下设校园网络信息安全小组。

第二条 校园网管理小组的主要职责是：

1. 负责制定我校计算机校园网及信息化建设的中长期发展规划；
2. 统筹入网部门与校园网中心主结点的联接；
3. 监督校园网的运行及网络安全、保密事宜；
4. 研究和审定校园网建设和运行中的重大决策。

第三条 校园网信息安全小组由分管副校长牵头，各处、室主要负责人为本室的网络安全责任人。

第四条 信息中心在校园网管理小组指导下开展具体工作，负责校园网的短期规划、建设、日常技术运行管理。

第五条 校园网的信息安全稽查工作由学校办公室负责。



第二章 应用安全管理

第六条 我校校园网信息安全由校园网信息安全小组负责。

第七条 学校任何室和个人不得利用校园网络从事危害国家安全、泄露国家机密的活动，不得危害计算机网络及信息系统的安全。

第八条 校园网出口处应安装防火墙以便对有害连接和有害信息进行记录和过滤。所有提供公开服务的计算机上均应安装病毒防火墙和入侵检测系统，对网络连接进行记录。

第九条 校园网用户必须自觉接受并配合信息中心进行的监督检查以及所采取的必要措施。

第十条 配备的防病毒软件必须是经过公安部门认证的产品。对防病毒软件必须及时进行升级和更新。

第十一条 任何连入校园网络的计算机均须安装病毒防火墙。重要部门的计算机，如财务用机、图书管理系统、应当做到专人、专管、专用，避免交叉使用。

第十二条 严禁使用来历不明的光盘、软盘、硬盘及其它移动存储器。对外来光盘、U 盘、硬盘及其它移动存储器，使用前要进行病毒检测，确认无病毒方可使用。

第十三条 如用户发现计算机感染病毒，必须马上将受感染的计算机与校园网隔离，防止病毒扩散，同时上报信息中心，以便迅速对网络 and 所有工作站进行查毒。



第三章 信息管理

第十四条 校园网用户不得利用校园网及互联网查阅、复制和传播危害国家、破坏安定、有碍社会治安和伤风败俗的各种不良信息。

第十五条 学校各处、室对上网信息进行审查，严格把关，凡涉及国家及学校机密的信息严禁上网。校园网用户不允许在网络上发布不真实的信息。

第十六条 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。信息资源保密等级可分为：（1）可向互联网公开的；（2）可向校内公开的。

第四章 数字化校园平台教学应用

第十七条 学校重视和加强学校信息化建设，各处室应根据履行职能，利用计算机网络技术和通讯技术，在校园网平台上开展信息开发、应用与研究工作的，实现办公自动化、信息化，管理科学化、规范化，以信息化促进管理水平提高，全面提高教育教学质量。

第十八条 广大教师要认真学习计算机基本知识，不断提高计算机应用能力；正确地使用计算机，独立完成常规事务，开发网络教学课程，将计算机更好地应用于教育教学和管理。

第十九条 学校将积极引进一些制作质量好，学科内容精，教学设



计特色鲜明的优秀的网络教学课程。供广大的教师和学生共享。积极引进和开发制作平台，为教师提供良好的开发环境和技术支持。

第二十条 学校鼓励各教研组、各科组利用网络集体备课，并制作出内容充实、版面活泼、能充分利用多媒体手段将抽象内容具体、形象、生动化的网络教学课程。

第五章 违约责任与处罚

第二十一条 违反本条例规定，有下列行为之一者，学校及校园网管理部门可提出警告、停止其使用网络，情节严重者，提交校行政部门或有关司法部门处理。

第六章 附 则

第二十二条 本管理条例若与国家或上级部门的有关管理法规相抵触，则以后者为准。

第二十三条 本管理条例解释权为我校校园网管理小组。

第二十四条 本管理条例自公布之日起生效实施

迁西县职业技术教育中心

2015 年 3 月 18 日



信息中心机房管理制度

为科学、有效地管理机房，促进系统安全应并 j、高效运行，特制定本规章制度。

1、路由器、交换机和服务器的，以及通信设备是网络的关键设备，须放置在机房指定位置，

不得自行配置或更换，更不能挪作它用。

2、机房的设备情况、温度、湿度、电力等系统由管理人员定期负责检查，确保各机器 24 小时不间断工作。遇有临时停电或雷电天气，做好机房监控，必要时需采取安保措施，避免发生意外。及时发现、报告、解决硬件系统出现的故障，保障系统的正常运行。

3、管理人员需做好各种记录，对本地局域网络、广域网等各种线路做好标识，并建立文

档。新增设备在安装完成投入使用后需将各种资料归档，并由专人保管。对所发生的故障、处理过程和结果等做好详细登记。

4、未发生故障时，当班人员不可对中继、光纤、网线及各种设备进行任何调试。机房内服务器、网络设备、UPS 电源、空调等重要设施由专人严格按照规定操作，严禁随意开关。管理人员的操作须严格按照操作规程进行，任何人不得擅自更改系统设置。

5、严格遵守保密制度，数据资料 and 软件必须由专人负责保管，未经允许、不得私自拷贝、

下载和外借；严禁任何人使用未经检测允许的介质(软盘、光盘等)。

未经许可任何人不得挪



用和外借机房内的各类设备、资料及物品。

6、机房禁止放置易燃、易爆、腐蚀、强磁性物品。管理人员须做到防静电、防火、防潮、防尘、防热。禁止将机房内的电源引出挪作他用。

7、严格控制进入机房人员，非机房人员未经许可不得入内。确有必要进入机房的人员，须由机房管理员陪同下进行有关操作。对违反操作规程者，机房管理员有权制止和纠正；对不听劝阻造成不良后果的，视情节轻重追究责任。



网络安全管理制度

一. 组织工作人员认真学习《计算机信息网络国际互联网安全保护管理办法》，提高工作人员的维护网络安全的警惕性和自觉性。

二. 负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。

三. 加强对单位的信息发布的审核管理工作，杜绝违犯《计算机信息网络国际互联网安全保护管理办法》的内容出现。

四. 一旦发现从事下列危害计算机信息网络安全的活动，做好记录并立即向当地公安机关报告。：

（一）未经允许进入计算机信息网络或者使用计算机信息网络资源；

（二）未经允许对计算机信息网络功能进行删除、修改或者增加；

（三）未经允许对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）从事其他危害计算机信息网络安全的活动。

五. 在信息发布的审核过程中，如发现有以下行为的，并保留有关原始记录，在二十四小时内向当地公安机关报告：

（一）煽动抗拒、破坏宪法和法律、行政法规实施

（二）煽动颠覆国家政权，推翻社会主义制度

（三）煽动分裂国家、破坏国家统一



(四) 煽动民族仇恨、民族歧视、破坏民族团结

(五) 捏造或者歪曲事实、散布谣言，扰乱社会秩序

(六) 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪

(七) 公然侮辱他人或者捏造事实诽谤他人

(八) 损害国家机关信誉

(九) 其他违反宪法和法律、行政法规将一律不予以发布。

六. 接受并配合公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。



安全教育培训制度

一、定期组织管理人员认真学习《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》，提高工作人员的维护网络安全的警惕性和自觉性。

二、负责对本网络用户进行安全教育和培训，使用户自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。

三、对信息源接入单位进行安全教育和培训，使他们自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，杜绝发布违反《计算机信息网络国际互联网安全保护管理办法》的信息内容。

四、不定期地邀请公安机关有关人员进行信息安全方面的培训，加强对有害信息，特别是影射性有害信息的识别能力，提高防范能力。



信息内容审核制度

一、必须认真执行信息发布审核管理工作，杜绝违犯《计算机信息网络国际联网安全保护 管理办法》的情形出现。

二、对在本网站发布信息的信源单位提供的信息进行认真检查，不得有危害国家安全、泄露国家秘密，侵犯国家的、社会的、集体的利益和公民的合法权益的内容出现。

三、对发布公共言论的建立完善的审核检查制度，并定时检查，防止违犯《计算机信息网络国际联网安全保护管理办法》的言论出现。

四、一旦在本单位发现用户制作、复制、查阅和传播下列信息的：

1. 煽动抗拒、破坏宪法和法律、行政法规实施
2. 煽动颠覆国家政权，推翻社会主义制度
3. 煽动分裂国家、破坏国家统一
4. 煽动民族仇恨、民族歧视、破坏民族团结
5. 捏造或者歪曲事实、散布谣言，扰乱社会秩序
6. 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪
7. 公然侮辱他人或者捏造事实诽谤他人
8. 损害国家机关信誉
9. 其他违反宪法和法律、行政法规

按照国家有关规定，删除本网络中含有上述内容的地址、目录或者关闭服务器。并保留原始记录，在二十四小时之内向当地公安机关报告。



信息中心保密制度

- 1、严格执行国家保密局《信息系统和信息设备使用保密管理规定》
- 2、不该说的秘密，绝对不说；不该知道的秘密，绝对不问；不该看的秘密，绝对不看；不该记录的秘密，绝对不记录。
- 3、遵守信息安全的“五禁止”，即：禁止将涉密信息系统接入国际互联网及其他公共信息网络；禁止在涉密计算机与非涉密计算机之间交叉使用 U 盘等移动存储设备；禁止在没有防护措施的情况下将国际互联网等公共信息网络上的数据拷贝到涉密信息系统；禁止涉密计算机、涉密移动存储设备与非涉密计算机、非涉密移动存储设备混用；禁止使用具有无线互联功能的设备接入网路或处理涉密信息。同时遵守涉密信息不上网，上网信息不涉密。
- 4、不将秘密文件、资料和存储介质放在不安全的地方。
- 5、不得擅自翻印、复印、传抄、拷贝秘密文件、资料、数据。
- 6、严格执行档案借阅制度，涉密文件未经审批不得借阅。
- 7、严格执行档案和数据硬盘销毁制度，不向废品收购部门或个人出售秘密文件资料和硬盘。不得私自销毁秘密文件、资料。
- 8、不隐瞒失密、泄密事故；保密检查不敷衍，不马虎。



教师入网管理制度

一、我校教师上网全部实行指定账户或 IP 入网。每位教师只允许使用自己的上网帐号或 IP，一人一号(ID)。

二、对信息源接入教师进行安全教育和培训，使他们自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容。

四、发现有违犯《计算机信息网络国际互联网安全保护管理办法》情形的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告。



计算机教室上机制度

教师上机制度

- 1、自觉遵守机房管理制度，爱护机器设备，保持机房清洁卫生。
- 2、注意安全防火、防盗，最后一人离开机房时应拉开电闸，锁好门窗。
- 3、不得带人和使用外来电子存储设备。
- 4、不得改动 CMOS 信息和硬盘分区信息，不得随意格式化硬盘和删除、改名系统文件。若有必要作对系统配置信息或系统文件有影响的操作时，先制定好保存和恢复有关信息的方案，并由组长同意后方可操作。
- 5、不得制作计算机病毒或其他有关程序，不得在系统文件设置密码等方式给他人上机操作设置障碍。
- 6、不得随意打开机箱拆卸或调换机器部件，若发现机器运转异常现象时，应及时报告组长。
- 7、每次上机，应认真填写上机登记表。

学生上机制度

- 1、按时上机和下机，不迟到、不早退。
- 2、要按照上机指导教师的课程安排，认真完成上机操作任务，不得作与上机操作无关的事或操作。



-
- 3、要爱护公物，不损坏或带出机房的任何物品和设备。
 - 4、不得带入外来磁盘。在操作过程中若发现机器运转异常现象时，应立即报告上机指导教师。
 - 5、保持肃静，不得大声喧哗、乱走动。
 - 6、在机房须穿拖鞋。不得乱扔东西，每次上机操作之前，要用干净抹布认真擦好工作台和机器表面，每天最后一组要全面打扫卫生。
 - 7、不要随意打开机箱、电源插座等高压电设备，注意用电安全。
 - 8、严格遵守机房管理制度，自觉维护软、硬件设备，保证正常上机。



多媒体教室教学系统使用管理制度

为了保证教师安全、正确、合理使用教室多媒体教学系统，本着“谁领用，谁保管，谁负责”的精神，为此我们制定了以下须知：

一、班主任老师具有配合学校做好财产管理的职责，必须做好班级内多媒体设备的保管工作，教育学生爱护公物，防止设备的人为损坏。科任老师向班主任申请使用，负责该节课程中多媒体设备的完好性。

二、严格按照《使用操作说明》使用，严禁擅自拆装机器，保持系统完整。各班级指定专门信息员，请认真填写使用记录。平时注意做好设备的防尘、防潮、防磁工作。在一般情况下，保证多媒体设备的正常运行，在力所能及的范围内做好多媒体系统的日常清洁、维修、保养工作。

三、教室多媒体系统主要应用于教学，不允许各班自行安装新的软件，运行本计算机没有的软件时与信息处联系，由其负责安装。禁止安装游戏软件特别是黑客软件，如发现将受到严厉的处罚并赔偿全部损失。

四、为了保证各学科教师都能方便、正常地使用电脑，已将各班的“桌面主题”统一设置成标准状态，“屏幕保护”和“节能状态”已全部关掉。请各班不要设置具有个性色彩的“桌面主题”、“屏幕保护”等。

五、各班的数据资料安全由自己负责，不要放在C盘和“我的文



档”里。不要轻易设置成“共享”状态，不要随意更改 IP 地址，更不要登录其他计算机时擅自删除别人的文件。

六、建议各班级不要设置计算机“开机密码”，特别是不要试图进入 COMS 修改计算机的基本设置。显示分辨率已设置，请各班级不要改动即可。

七、为确保系统在安全第一的前提下能发挥最大的作用，请各班信息员和班主任要按时参加管理部门组织的技术和管理的定期培训，不断提高使用技能，更好地为教学服务，确保正常的教学秩序。

八、除机器维修人员外，任何人都不得私自打开主机外壳，私自拆装多媒体设备。遵守操作规程，发现设备出现故障，请及时与信息处联系，并做好相应的故障登记工作。如因非正常操作而发生的机器故障，其维修费用由使用人（班级）自负。

九、每学期开学时，向信息处领用多媒体设备。领用时请清点所有多媒体设备配件，正确无误后请在教室多媒体教学系统领用清单上签字，经签字后领用生效，该机器就由领用人（班级）使用和保管。每学期结束时考试前一周，由信息处对各班级多媒体设备检查验收，并办好归还手续。

十、对电器要经常检查，及时维修，不用时立即切断电源，杜绝可能发生的事故。如不使用时设备用后即时加锁，下班时认真检查电源、柜锁，关好所有门窗（防止雨水进教室损坏设备）。杜绝长明电和 24 小时不关机现象。

十一、如遇技术问题，请及时与信息处取得联系。设备故障要及时报修。



校园无线网络安全管理制度

为了保护校园无线网络系统的安全、促进学校计算机网络的应用和发展，规范无线网络的使用，防止在无管理、无防护的状态下使用WIFI无线网络造成学校敏感信息泄露、重要数据损坏、网页劫持、电脑病毒感染、业务系统被非法控制等严重后果，加强学校网络环境安全建设，更好的为教育教学服务，特制定本管理办法。

一、学校各部门如需使用无线网络接入服务，应统一向学校网络部提交申请，由信息中心负责开通服务。

二、学校网络结构由信息中心统一规划建设并负责管理维护，任何部门和个人不得私自更改网络结构，办公室如需无线网络设备等必须事先与网络部取得联系。

三、办公、教学电脑及个人手机等设备所用IP地址必须由信息中心指定的方式设置，不可擅自改动。

四、无线网络密码统一由学校信息中心负责管理和设置。如密码变更，需由学校信息中心负责修改并通知相关使用人员。

三、未经允许，严禁个人私自接入无线路由器、无线发射和接收装置。

四、无线AP密钥不要随便告诉非本校教师。学生严禁使用无线网络。

五、本制度自公布之日起执行。



迁西职教中心软件正版化管理办法

第一条 为进一步加强软件正版化工作，规范正版软件管理，增强尊重和保护知识产权意识，确保从源头杜绝盗版侵权软件使用，减少信息安全事件发生，使软件正版化工作制度化、规范化、常态化。根据《中华人民共和国著作权法》和《计算机软件保护条例》等相关法律法规，结合学校实际，特制定本办法。

第二条 正版软件的管理和使用应坚持统一政策、归口管理、责任到人、物尽其用的原则。软件正版化工作的重点是确保我校办公、教学和科研用计算机，所使用的操作系统、办公软件、杀毒软件为正版软件。

第三条 学校成立软件正版化工作领导小组，主管校长任组长，行政办公室、信息中心、财务处、设备处、各部系主要负责人为领导小组成员。领导小组的主要职责是研究制定软件正版化工作相关规划和制度，统筹领导、协调推进、监督考核软件正版化工作。

第四条 学校软件正版化工作领导小组办公室设在学校行政办公室，负责制定软件正版化年度工作计划，确定软件配置标准，组织软件正版化工作实施，监督考核软件正版化工作落实。财务处负责编制年度正版软件采购预算，确保资金到位。

第五条 学校各部门、各部系主要负责人为本单位软件正版化工作的第一责任人，计算机使用人为直接责任人。各单位需设专人负责软件正版化相关工作。

第六条 学校各部门、各部系每年根据工作需求制定正版软件采购



计划，经学校软件正版化工作领导小组办公室审定后，方可纳入部门年度预算。

第七条 学校要建立健全正版软件采购制度，所有采购软件必须为正版软件。采购前，必须明确软件的版本、软件的兼容性、安全性等技术标准以及软件的使用方式和使用年限等授权模式，必须对软件的升级和技术支持等售后服务提出明确要求；采购时，要严格执行财经纪律和采购法；采购后，应及时入账并进行国有资产登记，妥善保存有关的软件介质、说明书、使用许可证（或合同）等相关资料。

第八条 教职工在学校办公、教学和科研工作中使用计算机时，必须按规定使用正版软件，并遵守以下规定：

（一）计算机内已安装未获授权软件的，应立即移除；

（二）对以团体、场地授权等身份获得特许使用权的软件，需确保已安装的软件的数目没有超过已购置的软件特许权证书数目和许可期限；

（三）以授权形式取得购置的软件到期后，应当立即停止使用并及时办理处置手续；

（四）购买新计算机时，已预装相关软件（OEM）的，要核对该软件是否已获得相应的特许使用权并取得相关证书；同时不得要求或允许销售商安装非正版软件；

（五）未经许可，不得向其他单位或个人提供任何我校购买的正版软件及其复制品；

（六）不得在网上下载并安装未经授权的计算机软件；

（七）不得故意规避或者破坏软件著作权人为保护其著作权而采用的技术措施；



(八) 不得故意删除或者改变计算机软件权限管理信息。

第九条 学校要定期组织软件正版化工作培训，提供软件正版化工作的技术支持与保障，不断提高教职工使用正版软件和保护知识产权的法律意识，提升教职工的软件使用和操作水平，使正版软件更好地服务于学校各项工作。

第十条 学校各部门、各部系需积极组织开展本部门软件正版化工作，按时报送软件正版化工作年度总结和相关信息表格，积极配合学校对软件正版化工作的督促和检查。学校软件正版化工作领导小组将按相关规定对各部门软件正版化工作进行督查和考评。

第十一条 本办法适用于全校各处室、部系及全体教职工。

第十二条 本办法由学校软件正版化工作领导小组办公室负责解释，自发布之日起执行。

迁西职教中心

2020.11.6



《计算机信息网络国际联网安全保护管理办法》

(1997年12月11日国务院批准 1997年12月30日公安部发布)

第一章 总则

第一条 为了加强对计算机信息网络国际联网的安全保护,维护公共秩序和社会稳定,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》和其他法律、行政法规的规定,制定本办法。

第二条 中华人民共和国境内的计算机信息网络国际联网安全保护管理,适用本办法。

第三条 公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全,维护从事国际联网业务的单位和个人的合法权益和公众利益。

第四条 任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密,不得侵犯国家的、社会的、集体的利益和公民的合法权益,不得从事违法犯罪活动。

第五条 任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息:

- (一)煽动抗拒、破坏宪法和法律、行政法规实施的;
- (二)煽动颠覆国家政权,推翻社会主义制度的;
- (三)煽动分裂国家、破坏国家统一的;
- (四)煽动民族仇恨、民族歧视,破坏民族团结的;



(五)捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

(六)宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

(七)公然侮辱他人或者捏造事实诽谤他人的；

(八)损害国家机关信誉的；

(九)其他违反宪法和法律、行政法规的。

第六条 任何单位和个人不得从事下列危害计算机信息网络安全的活动：

(一)未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

(二)未经允许，对计算机信息网络功能进行删除、修改或者增加的；

(三)未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

(四)故意制作、传播计算机病毒等破坏性程序的；

(五)其他危害计算机信息安全的。

第七条 用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

第二章 安全保护责任

第八条 从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条 国际出入口信道提供单位、互联单位的主管部门或者主管



单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十条 互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

(一)负责本网络的安全保护管理工作，建立健全安全保护管理制度；

(二)落实安全保护技术措施，保障本网络的运行安全和信息安全；

(三)负责对本网络用户的安全教育和培训；

(四)对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

(五)建立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；

(六)发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告；

(七)按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十一条 用户在接入单位办理入网手续时，应当填写用户备案表。备案表由公安部监制。

第十二条 互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织(包括跨省、自治区、直辖市联网的单位和所属的分支机构)，应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备



案，并及时报告本网络中接入单位和用户的变更情况。

第十三条 使用公用帐号的注册者应当加强对公用帐号的管理，建立帐号使用登记制度。用户帐号不得转借、转让。

第十四条 涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。前款所列单位的计算机信息网络与国际联网，应当采取相应的安全保护措施。

第三章 安全监督

第十五条 省、自治区、直辖市公安厅(局)，地(市)、县(市)公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条 公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

第十七条 公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

第十八条 公安机关计算机管理监察机构发现含有本办法第五条所列内容的地址、目录或者服务器时，应当通知有关单位关闭或者删除。

第十九条 公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关



规定移送有关部门或者司法机关处理。

第四章 法律责任

第二十条 违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款，情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

第二十一条 有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

(一) 未建立安全保护管理制度的；

(二) 未采取安全技术保护措施的；

(三) 未对网络用户进行安全教育和培训的；

(四) 未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；

(五) 对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的；

(六) 未建立电子公告系统的用户登记和信息管理制度的；

(七) 未按照国家有关规定，删除网络地址、目录或者关闭服务器



的；

(八) 未建立公用帐号使用登记制度的；

(九) 转借、转让用户帐号的。

第二十二条 违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。

第二十三条 违反本办法第十一条、第十二条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过六个月的处罚。

第五章 附则

第二十四条 与香港特别行政区和台湾、澳门地区联网的计算机信息网络的安全保护管理，参照本办法执行。

第二十五条 本办法自发布之日起施

《计算机信息网络国际联网安全保护管理办法》是由[中华人民共和国国务院](#)于 1997 年 12 月 11 日批准，公安部于 1997 年 12 月 16 日颁布，于 1997 年 12 月 30 日实施，法规文号为公安部令（第 33 号），效力级别为行政法规。



迁西职教中心笔记本电脑使用与管理制度

为了提升我校教育信息化水平，提高教师的信息技术，更好地服务教学，我校积极为一线教师配备了笔记本电脑。为规范学校笔记本电脑的管理和使用，高效发挥其信息化办公的作用，进一步提高学校的信息化教育工作水平，特制订笔记本电脑使用与管理制度。

1、给教师配备的笔记本电脑属于固定资产，归学校所有，由学校统一管理，并由信息中心统一编号入册入库，采用“借用保管”方式由教师个人使用保管，不要与他人互换。

2、笔记本电脑实行借用领取签字制度。教师领用时必须在领用审批单上签字，领取后该教师就是笔记本电脑的使用者和保管者，不得借于其他任何人员使用。

3、正式教师的笔记本电脑，在岗期间由本人管理、维护和使用，离岗后上交学校。非正式教师每学期初领取自己笔记本电脑，学期末归还或续借笔记本，管理员做好登记。

4、教师调离学校或退休时，应及时将完好笔记本电脑归还学校。

5、笔记本交给个人使用后，其保管和安全等一切由该教师负责。教师要做好笔记本的日常维护，保证在使用期间外观及一切配件不受损害。如因使用或保管不当造成损失的，由个人负责并赔偿。

6、领取笔记本电脑后，如果其发生自然硬件故障，及时联系学校，保修期内由厂家和经销商维修。人为损坏的，自行找专业部门维修，处理好后，配置和性能不得低于原有设备。

7、为提高笔记本电脑的使用效率，优先服务于日常教育教学教研



和办公使用，不得从事其他无关的活动。

8、任何个人无权更换配发的笔记本电脑及其配件，不得擅自对笔记本电脑进行拆机、改装、扩容、升级等。

9、笔记本电脑要正确使用与保养。使用时轻拿轻放，用完后关机存放。屏幕、键盘和外壳等要用专用软布并采用正确方法擦拭，不要把任何液体溅入设备。要定期对笔记本电脑的电池充电保养。

10、要注意数据和信息安全，重要资料另行备份。安装和使用正版软件，并部署安全防护软件，谨防病毒入侵。

11、笔记本电脑(含外设)为电子设备，具有一定的有效生命周期，其后期使用和维修遵循以下原则：

(1) 属于自然故障的，质保期内由经销商或售后负责维修。

(2) 自然故障超过质保期但未超过六年的，主机由学校负责维修。

(3) 其他情况(主机超过六年的；鼠标、电源、硬盘超过质保期的)，上报学校备案后自行找专业部门维修或更换。

(4) 因电脑寿命终结或达到最大使用年限而不能继续正常使用时，由学校鉴定后收回，可根据当时政策和条件重新分配代用设备。

(5) 计算周期以新笔记本电脑首次领用日期为开始日期，累计满12个自然月为一年，不满一个月(按30天)不计算。

12、其他未尽事宜，最终解释权归学校所有。

迁西县职业技术教育中心

2021年3月



迁西职教中心监控系统管理制度

校园监控系统是学校安防的重要组成部分，为实现平安校园提供了重要的保障。学校监控室是学校视频监控系统的控制中心，为了加强学校监控系统操作室的管理，确保监控系统的正常使用和安全运作，充分发挥其作用，特制定本规定。

一、行为准则

1. 监控室设备每天 24 小时运行，工作人员必须严格遵守按程序调取监控录像；
2. 要保持室内的清洁卫生，不准在监控室内存放杂物和个人物品；
3. 注意防潮、控制恒温。严禁在监控室内吸烟、使用明火及违章电器；
4. 不得利用监控设备做与工作无关的事情；
5. 经常检查和维护系统，保证系统设备处于良好工作状态，发现问题及时上报，以便及时处理；
6. 未经允许，非工作人员禁止进入监控室。确因调取录像需要（如破案），需由学校指定专门人员协同工作人员进入监控室调取录像。
7. 严禁携带易燃、易爆、有毒的物品进入监控室；严禁使用有干扰仪器正常运行的电子设备。

二、管理准则

1. 要按“先填写监控调取手续，再调取监控录像”的原则进行监控录像的调取。
2. 不得让非工作人员私自调取监控录像；



3. 特殊情况下工作人员不能调取录像的,需由学校指定专人进行;
4. 注意监控录像的安全保密,不得外泄录像信息;
5. 密切注意监控设备运行状况,保证监控设备系统的正常运作,发现设备出现异常和故障要及时报修,并向设备管理专业人员或保卫处领导报告;
6. 不得擅自改变视频系统设备,设施的位置和用途;
7. 不得删改、破坏视频资料原始数据记录;
8. 不得擅自复制、提供、传播视频信息。
9. 严禁擅自开发、修改、升级、删除、安装影响监控系统正常运行和安全的程序或软件;
10. 不得无故中断监控;监控录制的资料应妥善保存,未经允许,不得随意更改、删除原有资料。

三、保密准则

1. 非监控室人员不得进入监控室,师生、员工、观访者和外来人员需到监控室查看资料,必须经领导批准方可进入监控室查看;
2. 未经主管领导批准,值班人员不得修改系统设置。
3. 监控室值班人员必须具有保密意识,校园监控的范围、监控设备的布防严禁外传,不得在监控室以外的场所议论有关录像的内容;
4. 配合行政主管部门管理或公安机关、国家安全机关依法查询调用;
5. 以上规定一经颁布,立即生效,望相关人员严格按照本规定执行。

迁西县职业技术教育中心

2017年3月