安全管理员、信息审核员、信息管理员安全责任制度

第一条

第二条 安全管理员及其安全责任

一．安全管理员的职责是：

（一）依据国家有关法规政策，从事本单位的信息网络安全保护工作，确保网络安全运行。

（二）在公安机关公共信息网络安全监察部门的监督、指导下进行信息网络安全检查和安全宣传工作。

（三）向公安机关及时报告发生在本单位网上的有关信息、安全事故和违法犯罪案件，并协助公安机关做好现场保护和技术取证工作。

（四）有关危害信息网络安全的计算机病毒、黑客等方面的情报信息及时向公安机关报告。

（五）与信息网络安全保护有关的其他工作。

二．安全管理员应具备以下条件：

（一）遵守国家法律法规，无违法犯罪记录；

（二）具有一定的计算机网络专业技术知识；

（三）经过计算机安全员培训，并考试合格。基本掌握国家信息网络安全方面的法律法规和有关政策。

三．安全管理员的安全责任

（一）要认真学习党的教育方针，认真学习专业知识，刻苦钻研业务。要有高度的事业心和责任感，严格遵守各项规章制度，认真履行自己的职责，服从学校安全组织的领导，担负学校网络和信息安全保护工作。

（二）加强防范意识和措施，确保网络设备的安全。密切与学校各有关人员的联系，模范执行各项安全的规章。

（三）安全管理员要熟悉掌握设备的性能、使用方法及排除一般故障的能力，要定期对设备安全检查。

（四）按照计算机安全管理行业技术规范要求，定期对学校计算机信息系统进行安全检查测试，及时排除各种安全隐患；

（五）负责学校新购置设备的安全检查和验收工作，对新购置的操作系统、维修后的计算系统或从外拷贝回来以及要与外单位交换的软件进行严格的检查，确认无毒无害后才能使用，确保计算机系统安全运行；

（六）接受公安机关的安全技术培训，加强与公安机关的联系。发生安全事故和计算机犯罪案件时，应采取妥善措施，保护现场，避免危害的扩大，及时向学校主管部门汇报。

第三条 信息审核员及其安全责任

学校各单位的信息审核员具体负责本单位的信息发布，对所在单位上网发布的信息进行审核，并签发同意发布意见，要求对发布的信息进行申请人的姓名、信息的内容、发布的时间进行检查和登记，对过时的信息要要求所属信息管理员进行及时的删除，同时进行登记和备份，并将进行硬盘或光盘的备份。

第四条 信息管理员及其安全责任

学校各单位的信息管理员必须认真做好本单位网站管理，定期更新本单位网站内容。各单位的信息管理员必须时刻监视本单位网站内容，防止有害信息的传播，发现有害信息的应立即报告学校信息中心，发生安全事故或计算机违法犯罪案件时，立即向公安机关网监部门报告并采取妥善措施，保护现场，避免危害的扩散，畅通与公安机关网监部门联系渠道。

信息管理员应承担以下工作责任。

一．负责本单位网站安全运行。

二．沟通与校园网络与管理部门的安全联系。

三．负责本单位网站的信息安全。

四．熟悉计算机网络应用技术及正常使用方法，做好信息提供服务。

五．不断学习计算机网络技术和信息安全等有关知识，努力提高自身的工作水平。

六．对上传的信息认真检查，合格后方可分布，并且填好有关记录。

七．有独立服务器的单位，所属信息发布设备不得随意提供他人使用，并定期检查设备和操作系统安全。

八．做好防火、防盗工作，保持设备运行正常。 学校安全组织及其职责学校安全组织的职责是负责统一管理学校校园网络的规划、建设和管理工作。学校的计算机信息系统新建、改建和扩建必须制定安全技术方案，并报当地公安网监部门和教育主管部门备案。

安全管理员的职责

（一） 依据国家有关法规政策，从事本单位的信息网络安全保护工作，确保网络安全运行。

（二） 在公安机关公共信息网络安全监察部门的监督、指导下进行信息网络安全检查和安全宣传工作。

（三） 向公安机关及时报告发生在本单位网上的有关信息、安全事故和违法犯罪案件，并协助公安机关做好现场保护和技术取证工作。

（四） 有关危害信息网络安全的计算机病毒、黑客等方面的情报信息及时向公安机关报告。

（五） 与信息网络安全保护有关的其他工作。

江油市职业中学校

病毒检测及网络安全漏洞检测制度

第一条 学校各单位对任何要上传至本校服务器的文件，必须先对要上传文件进行病毒检测，确保没有病毒感染后方可上传。

第二条 学校各单位要对进入学校校园网内长期或临时使用的计算机进行防病毒软件和放火墙软件的安装检查。

第三条 学校各单位对进入学校校园网内的计算机必须定期进行病毒检测，防止病毒感染和传播。

第四条 网络管理员及学校各单位的信息管理员必须定期对计算机进行病毒检测，防止病毒入侵和传播。

第五条 网络管理员、安全管理员及学校各单位的信息管理员必须定期对计算机进行安全漏洞检测，对服务器系统进行必要的系统补丁或升级，预防及修补网络安全漏洞。

江油市职业中学校

计算机信息网络国际联网单位安全管理制度

计算机信息网络国际联网安全保护管理是社会公共安全的重要组成部分，根据《全国人大常委会关于维护互联网安全的决定》、《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》等法律法规要求，计算机信息网络单位应当采取如下的安全管理基本措施：

1、建立健全安全组织；

2、人事安全管理，即广泛开展计算机信息网络安全宣传，提高全员信息安全意识；

3、健全规章制度，落实安全防范责任制；

4、运行安全管理，即深入开展安全检查，切实整改安全隐患；

5、安全技术保障，即加强重点保护，落实安全标准；

6、加强风险管理意识，开展系统安全审核，积极改善安全措施。

建立、健全安全管理制度，是安全管理的关键。规范化的安全管理，能够最大限度地遏制或避免各种计算机危害，是保障计算机信息网络系统安全的最重要环节。

安全管理制度分为安全技术管理制度和安全事务管理制度两类：

一、安全事务管理制度，主要包括：

1、保密制度。

2、人事管理制度：（1）人员审查制度；（2）安全培训制度；（3）综合考评制度；（4）人员调离规定。

3、环境安全保护制度：（1）实体安全配置规定（按照有关国家标准及行业

标准制定）；（2）设备维护专人制度；（3）安全检查制度；（4）危险品管理制度等。

4、计算中心出入管理制度。

5、应急计划与备份。

6、日志审计制度。审计工作应长期不间断进行，对实体安全、信息安全、系统安全进行全面审计，重要信息网络系统定期与公安机关网监部门共同进行安全检查。

7、安全保护管理工作、经验、范例、事故、案件等安全事件报告制度。

二、安全技术管理制度，主要包括：

1、严格的技术文件管理制度；

2、严格的操作规程；

3、完备的系统维护制度；

4、电磁环境控制办法（防电磁干扰、防信息泄露）；

5、磁媒体安全管理、软件安全管理、数据库安全管理、输入输出控制等信息网络系统人员操作制度；

6、计算机病毒防治制度；

7、网络安全控制制度。

入网计算机使用和管理制度

1、 学校的入网计算机应有专人负责、严格管理。定期组织有关人员认真学习"江苏省公用信息网账号用户入网责任书"中的各项规定，并严格执行。

2、 要妥善保管用户账号和密码。用户账号和密码由专人掌握，不得泄密，以免造成损失。

3、 工作日每天定期开机入网查询，教委分发于电子信箱的邮件应及时收阅。要求采用电子邮件上报的材料和数据应按时发送上报。

4、 使用信息网时，操作人员要遵守国家的有关法律和法规，遵守社会公德，不得在网上传播、散布、复制以下信息：

1、 危害国家安全、社会稳定的信息；

2、 泄露国家机密的信息；

3、 与国家现有政策、法律、法规相抵触的信息；

4、 涉及色情、淫秽的信息；

5、 赌博信息；

6、 有损害社会公德和侵害他人合法权益的信息。

5、 盲目接收来路不明的电子邮件，以防病毒侵入，影响计算机正常运行。平时应做好经常性的查毒和杀毒工作，加强对计算机进行常规的维护保养。

6、 计算机上网应有上网记录，对每次入网时间、上网操作人员、内容等作记录以备查。

网络帐号使用登记及操作权限管理制度

第一条 任何人员必须通过合法的登记注册并取得合法帐号后方可使用校园网，没有通过合法的登记注册取得合法帐号而进入校园网的用户被视为非法侵入。

第二条 校园网内各节点的网络设备、服务器等，由信息中心统一管理，除信息中心教师外，其他任何人不得擅自拆卸、毁坏上述设备，或者通过网络对上述设备的设置进行非法修改。

第三条 网络管理员必须监视帐号使用情况，发现帐号用于违反此管理制度的应当立即封锁或删除帐号。

第四条 网络管理员拥有建立、修改、删除网络使用帐号以及赋予帐号使用权限的权力。

第五条 网络管理员对盗用他人帐号的人员有责任进行监控，并向信息中心或公安部门报告。

第六条 网络管理员对违反国家网络安全规定的帐号有责任进行监控其使用行为，并向公安部门报告

校园网安全管理条例

校园网是学校重要的基础设施之一，为全体师生员工提供一种先进、可靠、安全的计算机网络环境，支持学校的教学、科研和管理工作。为充分发挥校园网的作用，特制订本条例。

1、 校园网的所有工作人员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。

2、 任何个人不得利用计算机网络从事危害国家安全、泄露国家秘密的活动；不得查阅、复制和传播有碍社会治安和伤风败俗的信息。

3、 校园网的所有工作人员和用户必须接受和配合学校治安部门依法进行的监督检查和采取的必要措施。

4、 校园网实行统一管理、分层负责制。网络中心对校管资源进行管理，各部门管理人员负责部门级资源的管理，计算机系统管理员对计算机系统进行管理。

5、 严禁任何用户擅自连入校园网，入网单位和个人要办理入网登记手续，并签署相应的信息安全协议。

6、 各部门设专人负责审查上网信息，严禁涉及国家机密的信息上网。

7、 校园网工作人员和用户在网络上发现有碍社会治安和不健康的信息时有义务及时上报网络管理人员，并自觉立即销毁。

8、 校园网各部门管理机构设定网络安全员，负责相应的网络安全和信息安全工作，并定期对网络用户进行有关信息安全和网络安全教育。

9、 违反本条例规定，有下列行为之一者，校园网络中心可提出警告或停止

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。

①、 查阅、复制或传播下列信息的:

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;

煽动抗拒、破坏宪法和国家法律、行政法规的实施;

捏造或者歪曲事实，故意散布谣言，扰乱社会秩序;

公然侮辱他人或者捏造事实诽谤他人;

宣扬封建迷信、淫秽、色情、暴力、 杀、恐怖等。

②、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。

③、盗用他人账号。

④、私自转借、转让用户账号造成危害。

⑤、故意制作、传播计算机病毒等破坏性程序。

⑥、不按国家和学校有关规定擅自接纳网络用户。

⑦、上网信息审查不严，造成严重后果。

校园网违法犯罪案件和事故、病毒、有害信息的报告、协查制度

第一条 使用校园网的任何人员发现违反国家和学校有关计算机网络安全管理规定的有害信息，应当及时向信息中心报告。

第二条 使用校园网的任何人员发现违反网络安全法规的或传播有害信息的人员，应当及时向信息中心报告，或报送公安机关网监部门查处。

第三条 使用校园网的任何人员应配合学校信息中心和公安机关追查有害信息、有害电子邮件的来源，并协助做好取证工作。

校园网信息发布、审核、登记制度

第一条 任何人员不得利用学校网站、论坛和电子留言板等危害国家安全、泄露国家秘密，不得侵犯国家、社会、集体利益和其他公民的合法权益，不得利用学校网站及论坛制作、复制和传播下列信息:

（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，或者进行其他恶意攻击的;

（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;

（十）进行商业广告行为的。

第二条 学校的各办公室、班级、教师或学生，如果要在本校校园网上建立网站、论坛与电子留言板等必须按照学校有关规定，进行相关报批手续，经信息中心

登记、批准后，才能正式使用与发布信息。同时要做好这些信息发布系统有害信息检测报警技术措施，并做好发布信息记录包括：信息内容、发布时间、发布 IP 地址以及记录备份保存 60 天。

第三条 只有遵循本制度第一条的人员才可以注册登记为本校网站及论坛的用户。

第四条 学校的信息安全员、信息审核员、信息管理员、网络管理员按照各自的职能必须定期（每天至少一次）检查自己职责管理范围内链接网站（包括个人主页）、论坛与电子留言板等的信息内容，若发现其包含有害信息的应及时取消其链接。

第五条 学校的信息安全员、信息审核员、信息管理员、网络管理员必须定期（每天至少一次）检查网站内容及论坛或留言板发表内容，若发现其包含有害信息的必须及时删除和取消其用户资格，有违反法律法规的应及时交上报学校信息中心，情节严重的、涉及国家安全的应立即上报市公安局信息科。

校园网信息巡查、保存、清除和备份制度

第一条 学校的信息安全员、信息审核员、信息管理员、网络管理员必须监视网站及论坛发布的信息，做到定期巡查，一般每天至少一次，节假日特别要加强巡查，防止有人通过本校网络发布有害信息。

第二条 网络管理员，必须定期或每天对服务器进行备份，可以采用定时完全备份或增量备份的方法，备份数据应和服务器采用不同介质，如采用光盘刻录备份或服务器异地备份的方法，以备服务器受破坏后能回复正常使用。

第三条 网络管理员，必须定期对服务器里的多余、无用、临时文件进行删除工作。

信息安全法律、法规教育和培训工作制度

第一条 定期安排学校校园网的各层次使用人员参加网络与信息安全教育，加强学校各类应用人员的网络与信息安全意识。

第二条 学校定期安排网络管理员参加关于计算机网络的安全培训，提高其网络管理能力。

第三条 学校定期组织安全管理员、信息审核员、信息管理员和网络管理员认真学习《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。

第四条 学校定期组织对师生进行安全教育和培训，使学校的全体教师和学生自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，掌握基本的网络安全知识。

第五条 学校加强对信息发布的各级单位有关人员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。

第六条 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，提高防犯能力。