成都市教育局文件

成教技〔2010〕5号　　签发人：王励中

成都市教育局关于
加强成都教育专网管理工作的通知

各区（市）县教育局、高新区社会事业局，各市直属学校（单位）、市管民办校：

成都教育专网是我市实现城乡教育均衡化、一体化，实现教育现代化的一个重要信息化基础设施。为加强教育专网管理，确保系统稳定、安全、高效运行，现就专网管理工作提出以下要求：

一、建立市、县两级网管中心，完善网管队伍建设

设立教育专网市、县两级网管中心，协同完成教育专网网络系统的运营管理、运行维护以及信息网络安全保障等工作。

市级网管中心负责专网全网系统的运行管理与安全指导工作，并承担市级网络中心运行管理与维护。

县级网管中心承担县级网络中心运行管理与维护；负责对辖

区接入学校（单位）网管工作进行管理和指导；负责与上级网管部门的业务对接等工作。县级网管中心应配备不低于2名技术人员的专职网管队伍，实施“计算机安全员”持证上岗管理。

二、加强培训，不断提高专业素质

各区(市)县要积极开展对网管人员的技术与信息安全培训，要积极创造条件为人员培训、研讨、交流、参观学习提供机会，促其尽快成长，胜任工作，不断提高网管工作质量和为教育管理、教学服务的支持能力，为创建良好互动与积极协同的教育专网运营机制作好人员与技术储备。

三、建设网管工作信息平台，建立协同网管机制

市级网管中心负责建设教育专网网管协同工作信息平台，实现对网管信息、安全预警信息、管理策略等的及时发布，面向用户提供技术答疑与辅导服务，在线处置各级网络故障申报。各县级网管中心通过平台完成专网运行情况月报。

四、切实加强内部管理，确保专网系统性能与稳定运行

1、规范设备使用，保证系统处于良好运行状态

各区（市）县要切实加强对专网设备的规范使用、维护保养与财产安全管理。严禁在无技术论证情况下对县级网络中心设备进行部件拆卸、添加以及对配置模块进行调换与混用；严禁在无数据备份、无应急恢复措施下对中心设备、系统的配置参数进行

调整与改动; 要作好网络中心在后期完善建设过程中的施工安全管理，积极保证系统处于良好运行状态和安全运行环境。

2、规范专网接入，实施互联网出口集中管理

为保证我市教育电子政务、信息化管理以及教育资源的正常使用和专网系统安全，各区（市）县要求切实按照《成都市教育局关于加强和规范我市学校信息网络系统安全管理工作的通知》（成教办〔2007〕55 号）和成都教育专网项目建设要求，由县级网络中心归口开展本区县教育专网互联网接入建设，集中实施信息网络安全防范与内容审计、上网日志记录等管理。

原则上，已接入教育专网的学校（单位）只能使用专网光纤作为本单位网络的出口接入线路，确因工作需要需保留互联网接入和其他接入线路的，须落实相应的信息网络安全保护措施，并报县级网管中心检查、审批及备案，否则不能通过任何线路接入互联网。

区县专网接入学校（单位）不得向未获县级网管中心批准的单位、机构、个体用户等提供网络接入服务，县级网管中心要定期对辖区专网接入对象进行检查与清理。

3、作好县级网络中心互联网出口带宽建设和流量控制管理，保证正常教育教学与应用开展

县级网络中心互联网出口带宽的建设质量和有效管理直接

影响网内用户的工作和学习，其带宽大小应按照“科学分析、合理计算、适当余量”的原则进行建设。

为保证广大师生的正常教育教学使用，县级网络中心应积极完善基于用户 IP 地址，可实现双向流量控制和应用层监控的互联网出口流量控制建设。合理分配互联网出口带宽资源，主动应对、检测和防止不正常应用对网络带宽资源的消耗。积极保证普通高中学校远程培训教室计算机信息点等关键应用、优先应用的互联网带宽需求，对非正常、不合理的使用行为进行有效控制。

4、合理规划子网，规范使用内网 IP 地址，正确设置 TCP/IP 参数

成都教育专网全网采用子网方式实施管理，专网使用的各类内网 IP 地址不得混编和交叉使用，以保证专网系统的正常、稳定和安全运行，迅速定位故障点与原因，实施有效管理，发挥专网性能。

教育专网全网内网用户 IP 采用实名制管理，网内用户 IP 不得使用 NAT（地址转换），各区（市）县应严格按照《成都教育专网管理办法(试行)》和《成都教育专网 IP 地址实施方案》要求，在规定的本区县地址段范围内，对辖区各专网接入学校（单位）正确部署、分配和预留内网 IP 地址段。专网各接入学校（单位）须对内部网络实施合理的子网划分，用户计算机须正确设置

TCP/IP 属性各项参数，对未按要求设置参数引起网络故障和影响专网正常运行的接入学校（单位），县级网管中心应果断处置，限期整改。

5、作好信息网络安全管理

各区（市）县要切实按照《成都市教育局关于加强和规范我市学校信息网络系统安全管理工作的通知》（成教办〔2007〕55号）要求，积极落实区县专网互联网出口安全防范措施和各项管理制度；对县级中心重要业务系统数据实施备份；严禁设立没有防范措施、审核控制和专人管理的 BBS、聊天室等交互性栏目；严禁将二级域名提供非教育单位及个体用户使用；严禁对非教育用户提供空间租赁和服务器托管服务；切实按上级管理部门要求完成特控、敏感时期的信息安全监控与汇报工作。

区（市）县教育局应与专网接入学校（单位）签定《教育专网安全责任书》。专网接入单位及用户要自觉维护专网利益，不得利用教育专网从事危害国家安全、危害计算机信息网络安全、干扰网络用户以及破坏网络服务和影响网络系统安全稳定运行的活动。

6、完善教育网站信息内容监管

各区（市）县、学校要加强对教育网站人员的道德规范建设。网站上网信息须坚持“先审后发”原则，注意作好网站发布信息、

链接内容等的常规安全巡检工作；要强化保密意识，不得发布涉密信息以及不适合公开的信息；对真实性不能确定的内容不作转载；要提高知识产权保护意识，对转载内容应注明出处和作者。

7、加强教育网站备案与域名管理

各区（市）县要切实按照《成都市教育局关于加强和规范我市学校信息网络系统安全管理工作的通知》（成教办［2007］55号）文件要求，加强对教育网站 ICP 备案工作的检查力度。

网站首页底端应明确标明 ICP 备案编号，设置“网上报警岗亭”电子标志并实施相应链接。要注意提高对教育门户网站、信息化管理平台，资源服务系统等相关域名（含中文域名）保护性注册意识；保证注册域名有效期，以防过期后被别有用心者抢注。

五、建立信息网络突发事件应急预案

各区（市）县应按照国家和相关部门要求，积极建立区县专网信息网络突发事件应急预案，认真做好对各类信息网络突发事件的防范与应急处理，提高预处理突发事件的能力和水平，形成科学、有效、反应迅速的应急工作机制，确保区县专网系统重要实体安全、运行业务安全和数据安全，最大限度减少突发事件危害。

六、保证网络运行维持经费投入

市、县两级网络中心是成都教育专网的系统核心枢纽与管理

中心，为用户提供 7X24 小时全天候电信级运营服务。各区（市）县应将教育专网相关网络服务费，网络中心日常管理、运行维护等费用列入信息技术专项经费，给予积极保障。

附件:《成都教育专网管理办法（试行）》

二　一　年五月四日

主题词: 教育专网　管理工作　通知

成都市教育局办公室　　2010 年 5 月 5 日印发

（共印 7 份）

附件

成都教育专网管理办法(试行)

第一章　总　则

第一条　为加强成都教育专网管理，促进我市教育信息网络的健康发展，根据《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》和《四川省公安厅、教育厅关于加强和规范我省校园网计算机信息系统安全保护工作的通知》（川公信安〔2004〕197号）、《成都市教育局关于印发〈成都市教育计算机信息系统安全建设规范〉和〈成都市教育计算机信息系统安全管理细则〉的通知》（成教办〔2002〕33号）、《成都市教育局关于印发成都市教育网站和网校管理办法的通知》（成教发〔2005〕27号）、《成都市教育局关于加强和规范我市计算机信息网络系统安全管理工作的通知》（成教办发〔2007〕55号）及相关法律、法规，结合我市实际情况，制定本管理办法。

第二条　本管理办法所称成都教育专网（下简称教育专网），是指由成都市教育系统自建，由各级教育局机关、教育事业单位、各级各类学校等接入点联接构成的市域计算机信息网络系统。包括由组网路由设备、数据交换设备、信息网络安全设备以及配套

的网络线缆设施、应用服务器、工作站、网站等构成，以网络应用为目的并提供教育信息资源服务的软、硬件集成系统；信息服务包括文字、图片、数据以及音、视频等。

第三条 本管理办法所称网站，是指成都市各级教育局机关、教育事业单位、各级各类学校等开设，提供教育信息资源服务的站点系统（含下级站点）。

第四条 教育专网接入、使用单位和个人均须严格遵守国家有关法律法规和本管理办法，自觉维护成都教育专网利益，遵守社会公德，严格执行有关安全管理制度，不允许利用教育专网系统从事任何违反国家法律法规和社会公德的活动。

第二章 工作机构及职责

第五条 成都市教育局领导成都教育专网的发展规划、建设、管理与系统开发。各区（市）县教育局负责区县教育专网的建设和运营管理，负责落实各项教育信息网络管理制度、管理措施以及信息网络安全教育、技术培训等工作。

第六条 教育专网市、区两级网管中心是具体承担专网系统两级运营管理、运行维护以及信息网络安全保障的工作部门。其主要职责是：

（一）依据国家法规和上级管理部门要求，实施和协同开展

专网管理工作，落实各级管理责任，协调事务。

（二）具体承担教育专网市、区两级网络中心网管工作，承担区域内教育门户网站、教育资源系统以及各种教育管理信息化应用平台、信息服务系统的管理、维护和信息安全保障；全力保证中心各系统正常、稳定安全运行以及专网设备、物资财产安全。

（三）作为教育信息网络系统网管部门，接受上级管理部门和国家安全机关的监督和检查。

（四）具体开展信息网络安全教育和人员培训；对安全管理工作的开展和落实情况进行监督、检查和指导。

（五） 指导学校（单位）开展教育专网的接入建设、管理与维护，负责对接入学校（单位）的网络管理与维护工作进行技术指导、监督与检查、考核。

第七条　校级网管中心作为校园网络系统技术管理和系统维护的工作部门，按照上级管理部门要求，具体负责全校校园网络系统日常运行管理与技术维护和服务保障等工作，认真贯彻执行各项信息网络安全管理制度。其主要职责是：

（一）按上级网管部门要求，规范完成专网接入建设和校园网系统建设。

（二）按要求具体开展校园网络系统的日常运行管理与技术维护，向校园网络用户提供技术咨询与使用指导。

（三）具体开展校园信息网络安全防范工作，落实安全保护措施。

（四）具体开展对校园用户的安全教育和培训。

（五）接受上级网络管理部门和国家安全机关的监督和检查。

第八条　教育专网市级、区级、校级网管中心积极协同开展教育专网全网系统的运行管理工作，及时处理各种信息网络突发事件与网络故障，积极保证专网全网链路畅通和系统稳定安全运行。

第三章　网络系统管理

第九条　教育专网市级网管中心统一负责专网全网系统的运行管理与安全指导工作。各区级网管中心负责区县专网系统的日常运行管理和信息安全工作。教育专网接入单位和使用人员须服从网管中心的管理、监督和指导。

第十条　教育专网各级网络接入和使用部门及用户等应积极配合网管中心开展教育专网网络信息安全工作，接受并配合国家有关部门依法进行的监督检查。

第十一条　不允许进行任何破坏教育专网网络系统构架，降低教育专网组网技术标准、传输性能、内网安全和干扰网络服务、

破坏网络设备以及影响专网系统安全稳定运行的行为。

第十二条　全市教育部门和集体办学校、教育机关、事业单位须统一接入教育专网，以保证教育信息与资源共享。未经教育专网网络运维管理和安全负责单位同意，严禁任何单位、社会机构、个人等接入和使用教育专网。

第十三条　除有特殊使用要求或提供特殊服务外，教育专网系统内的应用平台、服务系统信息及数据等应采用一定的限制和保密措施实施有效管理。

第十四条　需建设和开展个人主页服务、电子邮箱，开通 IP 地址等上网服务的用户，须向网络管理部门申请，并提供相关真实信息资料和开通要求等文字说明，经区级网管中心审核批准并备案后方可开通。

第十五条　凡利用学校校名、学校校园网络或使用教育网站域名的论坛类网站、博客托管（BSP）和主页空间服务的，需经区级网管中心批准后才能上线。

第十六条 为有效防范网上非法活动，积极净化教育信息网络环境，各区（市）县要统一本区县教育专网互联网出口建设，区级网络中心须采取积极、有效的技术手段和管理手段，建立健全安全保护措施，落实安全技术设备设施，监控、封堵、清除网上有害信息，防止有害侵入，确保教育专网网络安全和信息安全。

第十七条 教育专网用户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几系统进行删除、修改或增加。

（四）故意制作、传播计算机病毒、木马等破坏性程序。

（五）使用各类黑客软件进行黑客攻击活动。

（六）其他危害计算机信息网络安全的活动。

第十八条　区县教育专网工程建设、竣工、验收等相关备案资料由区级网管中心集中归类和建档保管，主要包括以下几类基本资料:

（一）区级网络平台建设，至少包括:《工程概况》;《教育专网技术设计方案》;《区县专网系统拓扑结构示意图》;《学校VLAN ID、用户 IP 段分配表》;《学校接入路由器网管地址、网关地址分配表》、《压力测试工作报告（含压力测试记录表）》;《工程质量自检报告》等。

（二）区级网络中心建设，至少包括:《网络中心拓扑图》;

《中心设备用户、网管、LOOP BACK 等内部 IP 地址分配表》;《区域 WEB 公网 IP、域名与内部 IP 的地址映射对应表》;《核心骨干路由器、核心交换机等重要组网、信息安全、数据交换设备的参数配置表》;《路由器、交换机、内容审计、服务器等管理帐号及密码清单》;《专网组网端口对照表》以及机房防雷接地系统、气体类自动消防系统的行管验收合格材料等。

（三）用户接入建设，包括:《专网接入学校（单位）汇总表》;《学校 IP 分配、VLAN 及 TCP/IP 参数分配表》等。

第四章　网络运行管理

第十九条　所有接入并使用教育专网的单位及个人须严格遵守执行国家有关法律法规，严格执行安全保密制度，遵守社会公德。不得制作、下载、复制、查阅、发布、传播下列内容:

（一）危害国家安全，泄漏国家机密的;

（二）宣扬邪教、迷信的;

（三）宣传低级淫秽有伤风化的;

（四）散布谣言，破坏社会稳定的;

（五）从事商业广告推销的。

不得利用教育专网系统进行下列危害信息安全的活动:

（一）干扰其他网络用户;

（二）发布不真实信息;

（三）以不真实身份使用网络资源;

（四）传播计算机病毒，破坏计算机信息系统功能、数据和应用程序。

（五）侵犯他人知识产权的。

（六）未经区级网管中心和有关部门批准，私自建立网站或提供对外网络服务的。

（七）在 BBS、留言板、聊天室上对他人进行人身攻击，发表消极、低级庸俗言论，发表煽动性、集结性言论，发表各类未经许可的广告信息，使用各种公众人物的名字及其他不健康的内容作为自己的网名的。

（八）其他危害计算机信息网络安全的。

第二十条　严禁制造和传播计算机病毒以及其他有害数据或危害计算机信息系统安全的程序、工具软件、插件、控件。严禁在教育专网上使用来历不明、引发病毒传染的软件；对于来历不明的可能引起计算机病毒的软件应使用杀毒软件检查、杀毒。

第二十一条　除教育专网网络管理维护和系统安全负责单位外，任何人不得以任何方式登录任何功能的专网管理节点、服务器等进行修改、设置、删除和服务功能更改等操作。

第二十二条　除教育专网运维管理和安全负责单位因工作

原因外，任何人不得以任何借口移动、更换专网网络设备及设施。

第二十三条 教育专网各级网管中心应规范使用和保养设备，保证网络系统处于良好运行状态。

（一）网管、技维人员等应严格遵循设备厂商提供的《使用手册》相关要求和注意事项，规范操作行为。

（二）严禁在无技术论证、无产品厂商和教育专网建设商技术指导与支持的情况下对专网设备进行部件拆卸或添加以及对路由器、交换机等重要核心设备配件及模块进行调换和混用。

（三）严禁在无备份和无恢复措施及应急预案的情况下对网络中心设备、系统等的参数配置进行调整、改动以及对系统实施切换。

（四）加强机房在后续完善建设、扩充建设项目实施过程中的现场安全管理与监管，杜绝人为损坏和破坏性施工等事件发生。

（五）积极作好对专网设备、物资的专项使用和财产安全管理。

（六）积极作好机房防雷接地、气体类自动消防、温湿度控制设备及相关安保系统的常规安全检查与维护保养，切实为中心设备及系统的安全运行、人员人身安全等提供保障。

（七）积极保持机房场地环境的整洁与规范。

第二十四条 任何人不得利用设备或软件技术从事用户帐户、口令的侦听与盗用活动。

第二十五条 任何人不得盗用 IP 地址和利用更换 IP 地址从事违反法律、法规以及破坏教育专网正常运行和其他非法行为。

第二十六条 网络用户应使用由网管部门、系统管理员等分配的帐号登录，并对自己的帐号及密码加强管理，作到正确与规范使用；不得把帐号和密码转借他人，防止他人盗用后在网上进行非法活动。

第二十七条 成都教育专网全网采用子网方式管理。专网各接入学校（单位）应按要求合理规划网络管理、办公网、教学网、网络教室等内部子网，规范、正确使用专网 IP 地址。

（一）对专网使用的“网络设备互连及网管地址”、“LOOPBACK 地址”、“中心应用地址”、“用户地址”等各类内网 IP 地址不得混编和交叉使用，以保证专网系统的正常、稳定和安全运行，迅速定位故障点与原因，实施有效管理，发挥专网性能。

（二）各区（市）县应按照《成都教育专网 IP 地址实施方案》要求，在规定的本区县地址段范围内，对辖区各专网接入学校（单位）正确部署和分配专网内网 IP 地址段。

（三）成都教育专网全网内网用户 IP 采用实名管理，网内

用户 IP 不得使用 NAT（地址转换）。

（四）教育专网内各接入计算机须按要求正确设置 TCP/IP 属性各项参数，不得随意更换用户 IP 地址，不发生 IP 地址冲突，首选 DNS 服务器地址须统一设置为教育专网市级 DNS 服务器地址。

（五）学校在实施计算机单机装备以及网络教室、校园网、办公网等局域网络建设时（包括后期实施项目），其每台计算机的用户 IP 地址必须按照区级网管中心所分配和预留的方案执行，不得使用其他学校的 IP 地址段。

第二十八条 教育专网市、区两级网管中心须加强对网络系统的运行状态监控与管理，及时排除故障；随时查看上网日志，屏蔽含有有害信息、有害数据的网站、网页。

第二十九条 教育专网各级网络中心应及时做好服务器操作系统、数据库以及应用软件的补丁升级与维护工作；及时作好防杀毒、木马查杀等软件（系统）的特征库、规则库升级工作，积极完善防病毒、防木马、防攻击安全措施，随时防范病毒、木马和黑客攻击。

第三十条 教育专网市、区两级网管中心要严格设置安全策略，对网络中心运行的重要业务系统文件、数据、操作系统等实施定期备份；定期核查数据备份容量是否异常；对网络、信息、

数据和重要应用系统等要建立应急处理机制，并落实恢复保障措施。

第三十一条 教育专网各级网管中心应加强管理人员帐号、口令及使用权限等的管理，对中心内网的路由器、交换机、防火墙、入侵检测、内容审计、应用服务器等设备、信息化管理平台、应用服务系统的管理级帐号、口令等必须实施保密等级管理；不得向第三方及其他单位和个人提供这些信息，对确因工作需要的，应与相关方签定《保密协议》。

第三十二条 重要工作岗位帐号、口令、技术资料、管理资料等交接须在网络中心负责人现场监管下完成，接手人员应当场更换口令设置。

第三十三条 教育专网各接入单位应有专人负责对本单位网络用户 IP 地址进行备案管理，如发现联网计算机从事危害国家安全，泄漏国家机密等违法活动或其他不良活动时，应及时关闭其 IP 地址。

第三十四条 教育专网市、区两级中心应作好互联网出口建设与流控管理，积极保证正常教育教学和应用工作开展。

（一）网络中心互联网出口带宽大小应以实际使用需求为基础，按照“科学分析、合理计算、适当余量”的原则进行建设，逐步扩充，合理调整。

（二）网络中心要积极完善出口流量监控建设；合理分配带宽资源；要主动检测和防止不正常应用对网络带宽资源的非正常消耗，保证关键应用和优先应用，对非正常、不合理的使用行为要进行有效控制；要根据业务发展变化，科学、合理优化中心配置环境，努力改善和保障应用服务质量，为广大师生的正常使用需求提供保障。

第三十五条 作好域名解析与管理，及时有效提供网站 WEB 服务。

（一）教育专网全网内网 DNS 解析服务采用一级市级 DNS 方式建设，各区（市）县不建设本区域区级 DNS，由市级网络中心集中向全网用户提供内网域名解析服务。

（二）各区（市）县应及时将辖区所使用的已注册域名、学校自编域名等资料上报市级网络中心（包括即时性的增加、减少与修改）。市级网管中心接报后，应及时在市级专网 DNS 服务器解析数据库中填加和处理，以保证用户的正常使用。

（三）市、区两级网络中心在本级中心路由设备上应及时作好所辖教育网站、管理平台、资源应用服务系统等的服务器公网 IP 与专网内网 IP 的映射，以满足社会公众来自互联网的正常访问需要。

（四）教育专网内网各学校网站自编域名全部采用在区县一

级域名下的二级域名方式进行管理。网站域名按照学校单位中文全称的首写字母组成，但应尽量避免不规范的命名以及可能会产生歧义的名称，以免因特殊原因而造成 WEB 服务的限制。

（五）学校自编网站域名有对外提供互联网访问（即外网访问）需求时，除作好 WEB 服务器建设之外，还应及时向相关服务商办理域名注册和公网 IP 租赁手续；网管中心在本级中心路由器及相关设备上同步完成服务器公网 IP 及内网 IP 地址的关系映射。

第三十六条 未经区（市）县网管中心获批同意的单位、个体用户等不得擅自接入教育，专网网管部门要对辖区专网接入单位的互联网接入情况进行定期检查与清理。

第三十七条　校园内从事施工、建设，不得危害教育专网网络系统的运行安全。

第五章　网络信息管理

第三十八条　教育专网的所有工作人员和网络用户须对所提供、使用的信息负责。不得利用计算机联网从事危害国家安全、公共信息安全、泄露国家机密的犯罪活动。不得利用网络制作、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）损害学校形象和学校利益的;

（十）其他违反宪法和法律、行政法规的。

第三十九条　教育专网用户要树立强烈的网络安全意识，上网信息必须遵守国家法律法规，坚持实事求是，宣传教育，服务教育，有利于促进教育事业的发展。

第四十条　教育专网用户均有义务帮助审查上网信息，杜绝涉及国家机密或国家禁止的信息上网。如发现违法犯罪行为和有害的、有碍社会治安和不健康的信息，应及时上报，网管中心接报后应及时处理，以防造成更大的社会影响。

第四十一条　相关工作部门和个人要认真贯彻落实各项保密工作，根据国家保密管理相关规定，凡涉及到机密以及有重要文件的计算机应与公共网络隔离，防止重要文件被盗取或丢失。

第四十二条　要切实加强对教育网站的管理，加强网站信息员道德规范建设，对真实性不能确定的内容不作转载；要提高知识产权保护意识，对转载内容应注明出处和作者。

第四十三条　网站信息内容须符合国家有关法律、法规的规定，所有图片、文字应符合有关法律和行政法规的要求，在发布之前必须认真审阅，确保其正确性。

第四十四条　网站链接对象应为政府类网站、教育部门（单位）网站以及提供教育信息与资源服务等与教育工作和业务相关的主流网站（网页），应尽可能避免与商业性质网站链接。对外链接服务器时应注意：

（一）链接网站的合法性，网站（网页）内不携带病毒、恶意代码；

（二）含有修改浏览者默认页的网页不得链接；

（三）严禁链接含有违反中国法律法规内容的网页或网站；

（四）不得链接有关成人等不适合大众(特别是青少年)阅读的网页或网站；

（五）不得链接含有对网站及服务器进行攻击等有害行为的网页或网站；

（六）不得链接含有恶意修改访问者计算机注册表等系统信息或对访问者计算机进行入侵、攻击、破坏等程序或代码的网页

或网站。

（七）在未得到被链接网站许可的情况下，不得使用深度链接方式链接相关信息和视频。

第四十五条　网站开发应注意代码安全，尽量避免出现安全漏洞，若发现应及时进行漏洞修复。

第四十六条　未经网站负责人和网站管理员同意，任何人不得擅自增加、删除或修改网站栏目及其信息内容；信息内容等添加应在指定区域内完成。

第四十七条　指定专人定期检查网站及其链接对象能否正常访问，页面有无异常信息。

第四十八条　网站信息发布实行制度化、规范化管理，责任明确，执行过程严密，管理措施到位。未经批准发布信息，造成不良影响的，或监管工作不到位造成一定后果的，将追究直接责任人和发布人的责任；情节严重，触犯刑律的，移交司法机关处理。

（一）上网信息和相关服务遵循“谁发布、谁负责，谁承诺、谁办理”原则。

（二）确保信息的准确和客观。信息源要真实和可靠，对于来源不明、内容不准的信息不予采集和上传。

（三）属转载的信息应注明信息来源，严格对上传信息的标

题和内容进行审核。

（四）应指定单位内工作认真负责的人员承担信息上传工作。

（五）对发布信息进行网上检查与复验。

（六）信息发布的信息源采集与文本整编、审核签字、上传、网上复核等一系列工作过程和环节须进行登记备案。

第四十九条　论坛、聊天室、留言板、贴吧等网站交互式栏目实行实名注册，禁止匿名注册。对所有发布信息进行严格审核。定期对栏目信息内容进行巡查和清理。

（一）交互式栏目应设置信息安全责任条款相关申明。

（二）实名注册过程须对提交注册申请的用户进行身份资料验证，验证合格者方可注册成功。

（三）系统只对成功注册的合法用户提供制贴提交功能，对访客不提供任何制贴、提交功能。

（四）对提交信息的采用审核控制机制。由专人负责对提交的标题、内容等进行审核，只有通过审核后的信息才能发布。

（五）严禁设立没有任何审核防范措施和专人管理的论坛、聊天室、留言板、贴吧、评论板等交互式栏目。

（六）交互式栏目实行 24 小时巡查制度。

（七）定期专人对交互式栏目内容进行清理和维护。

第五十条　禁止对非教育专网用户（学校、部门、个人等）开展空间租赁服务。按规范途径获得空间租赁使用的校内用户，不得上传发布、制作、传播以下信息:

（一）反对宪法所确定的基本原则的，为国家法律法规或公共道德所禁止的或不欢迎的。

（二）危害国家安全，泄露国家秘密，损害国家荣誉和利益的，颠覆国家政权，破坏国家统一的。

（三）破坏国家宗教政策，宣扬邪教、迷信的； 散布淫秽、赌博、暴力、恐怖或者教唆犯罪的。

（四）散布谣言，扰乱社会秩序，破坏社会稳定的。

（五）煽动民族仇恨、宣扬民族歧视，破坏民族团结的，或者侵害民族风俗、习惯的。

（六）漫骂、辱骂、诽谤他人，对他人进行人身攻击、人格侮辱、侵害他人隐私、侵害他人合法权益的言论。

（七）散布淫秽、赌博、暴力、恐怖或者教唆犯罪的。

（八）可能导致任何电脑软件、硬件或通讯设备的功能中断、被破坏或被限制的含有电脑病毒。

（九）可能欺诈到用户合法权益、利益或可能盗用、窃取用户个人信息、帐号密码等信息的。

（十）对服务器进行攻击、捣乱，影响服务器正常运作的。

第五十一条　各级网管中心应加强对“家校通”、“校讯通”、“校信通”等家校互动短信平台发送内容的清理与安全管理。

第五十二条 各级信息网络安全管理部门对各类上网信息进行安全监管。一经发现非法内容、有害信息等，应立即进行截屏和数据库备份等现场证据保全，并在最短的时间内删除非法内容及有害信息，恢复网站内容，同时向信息网络安全领导小组和公安网监部门报告，协助相关部门追查。

第五十三条　教育专网各级网管部门应切实按上级管理部门要求完成特控、敏感时期的信息安全监控与汇报工作。

第五十四条　各区县要重视和加强对网站备案与域名管理工作。

（一）切实按照《互联网信息服务管理办法》（国务院令 292 号）和《非经营性互联网信息服务备案管理办法》（信息产业部令第 33 号）以及《成都市信息化办公室关于加强政府网站及相关应用系统备案工作的通知》相关规定和要求，及时完成网站 ICP 备案（工信部备案网站：http://www.miibeian.gov.cn），各网站在首页底端应明确标明 ICP 备案编号，设置“网上报警岗亭”电子标志并实施相应链接。

（二）要注意提高对教育门户网站、资源服务网站以及相关教育信息化应用系统等与使用密切相关域名（含中文域名）的保

护性注册意识；切实保证网站注册域名的有效期，以防过期后被别有用心者抢注。

第五十五条　学生上网须有老师的具体指导，教师要积极引导学生正确、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。

第六章　安全保护技术手段和措施

第五十六条　区县教育专网应统一互联网出口，建立和落实安全保护技术手段和措施；确因工作需要需保留互联网接入的学校（单位）应向区级网管中心提出申请并采取必要的信息安全技术保护措施，应通过区级网管中心现场检查与安全评估和审批，否则不能接入互联网，确保网络信息系统安全。

（一）采用防火墙技术加强网络接入安全保护。通过细致的系统配置，实现内外网的安全隔离和访问控制，降低网络安全风险。

（二）采用入侵检测技术，利用先进的基于网络数据流实时智能分析技术判断来自网络内部和外部的入侵企图，进行报警，响应和联动技术防范处理，提升系统综合抗网络攻击防范能力。

（三）实施网络安全扫描主动防御，制定安全检测策略，对安全配置和应用服务进行安全分析，及时消除网络安全漏洞，更

正系统错误配置，进行安全加固，有效提高网络的安全性。

（四）制定路由器访问控制列表参数配置规范；规范组网方式，定期对关键端口进行漏洞扫描，对重要端口进行实时入侵检测。

（五）集中加强对暴力、色情、反动等有害信息的内容过滤，以及对网站、网页浏览、访问、下载等行为的审计、监控和屏蔽隔离。

（六）具有防止网页、网站信息被篡改的安全保护技术措施以及被篡改后的恢复措施。

第五十七条　加强在系统运行状态监控、内容审核管理、用户使用访问等方面的日志记录功能和措施，作到跟踪记录的及时和准确。

（一）严格设置安全策略，对重要文件、数据、系统的备份、恢复及处理突发性事件的应急措施；有害信息监测报警技术措施；60 天以上的系统运行日志记录保存措施。

（二）开设有论坛、聊天室、留言板、贴吧等交互形式电子公告服务的，落实实名注册和发布人、发布人 IP 地址、发布时间、发布信息内容以及审核人、审核人 IP 地址、审核时间等记录措施；60 天以上记录备份保存措施（含对删除内容的保留）。

（三）开设个人主页服务的，落实实名注册和 60 天以上维

护日志、用户访问日志的记录措施。

（四）能提供用户、IP 地址、所使用计算机、上网时间的追踪功能；具备有防止色情、反动、邪教等有害信息的过滤屏蔽功能，记录备份保存 60 天以上。

第五十八条　根据运行业务使用功能及服务对象安全策略部署的不同，对网络中心各功能区域进行合理 VLAN 划分，有效堵塞网络风暴，降低来自系统内部之间的安全风险，保护各功能区域的正常和安全使用。

第五十九条　制定操作系统安装规范。包括硬盘分区、网段名，服务器名命名规则、操作系统用户的命名和权限、系统参数配置，力求杜绝安全参数配置不合理而引发的技术风险。

第六十条　制定应用系统安装、用户命名、业务权限设置规范。有效防止因业务操作权限授权没有实现岗位间的相互制约、相互监督所造成的风险。

第六十一条　完善重要业务系统、数据的人工、自动等备份机制建设，制订数据备份管理规范，包括备份类型、备份策略、备份保管、备份检查，保证了数据备份工作真正落到实处。

第六十二条　服务器、网管及工作管理等网络中心内网联网计算机须安装正版的操作系统与数据库系统软件，重视和加强对计算机病毒、木马程序的监控防范和处理。

选用经公安部门认定合格的计算机病毒防杀和木马查杀等专业、正版工具软件。

及时对系统进行安全扫描，查杀计算机病毒和木马程序。

第六十三条　开设邮件系统服务的，落实反垃圾、反病毒邮件的技术防范措施。

第六十四条　对新安装的信息安全保护产品（安全系统），应在正确完成参数配置并经测试后才能正式上线，以保证技术防范措施的有效贯彻。

第六十五条　根据需要，落实其他互联网信息网络安全技术防护措施。

第七章　附则

第六十六条　对违反规定的使用部门和个人，各级网管部门应采取提醒、警告、内部通告、批评，停止网络连接等措施进行处罚，情节严重的应按照国家相关规定移交公安部门处理。

第六十七条　本办法自公布之日起执行，由成都市教育技术装备管理所负责解释。各区（市）县、学校(单位)可参照本管理办法和制度样本（附件），依据国家相关法律、法规和部门规章以及教育及公共信息安全管理部门下发文件等，结合实际情况制定具体的管理制度、实施细则和工作记录表格。

第六十八条　成都市教育技术装备管理所将根据我市教育信息网络实际情况并结合上级部门有关规定，对本办法条例适时予以修订。

附件:

1、制定依据

2、教育专网管理制度（含内容）

附件 1

制 定 依 据

一、国家主要法规、部门规章

1、《中华人民共和国计算机信息系统安全保护条例》

2、《中华人民共和国计算机信息网络国际联网安全保护管理办法》

3、《互联网安全保护技术措施规定》

4、《国家互联网电子公告服务管理规定》

5、《计算机病毒防治管理办法》

6、《非经营性互联网信息服务备案管理办法》

二、教育及公共信息安全管理部门主要文件

1、《教育部关于在教育系统深入开展打击淫秽色情网站专项行动的通知》-（教社政〔2004〕10 号）

2、《四川省公安厅、教育厅关于加强和规范我省校园网计算机信息系统安全保护工作的通知》-（川公信安〔2004〕197 号）

3、《成都市教育局关于印发〈成都市教育计算机信息系统安全建设规范〉和〈成都市教育计算机信息系统安全管理细则〉的通知》-（成教办〔2002〕33 号）

4、《成都市教育局关于印发成都市教育网站和网校管理办法

的通知》-（成教发〔2005〕27 号）

5、《成都市教育局关于加强和规范我市计算机信息网络系统安全管理工作的通知》-（成教办发〔2007〕55 号）

6、《成都市校园计算机信息网络系统安全管理办法(试行)》

附件 2

教育专网管理制度（含内容）

1、《教育专网网络管理分工制度》

2、《成都教育网网络安全管理制度》

3、《网络管理员职责》

4、《网络权限管理制度》

5、《密码管理制度》

6、《中心机房管理制度》

7、《专网设备使用管理制度》

8、《计算机病毒防范和安全漏洞检测制度》

9、《信息发布、审核、登记管理制度》

10、《论坛、聊天室、留言板等电子公告服务管理制度》

11、《24 小时交互式栏目信息巡查制度》

12、《信息监控、保存、清除和备份制度》

13、《突发应急处理制度》

14、《违法犯罪案件和事故、病毒、有害信息报告、协查制度》

15、《教育网站及从业人员自律条约》

教育专网网络管理分工制度

为进一步加强成都教育专网网络管理，建立良好的“校”-“县”-“市”三级网管联动工作机制，积极保证教育专网的正常运转，维护教育专网的正常、健康与有序发展，特制定本制度。

第一条 成都市教育局领导成都教育专网的规划、建设与系统开发等工作。

第二条 成都教育技术装备管理所具体负责成都教育专网的建设、管理、培训、技术指导与监督检查与考核，承担教育专网市级网络中心网管工作；负责按照国家和相关管理部门要求，针对教育信息网络有可能出现的各种突发事件，制订突发信息网络事件应急工作预案。

第三条 各区（市）县教育专网网络中心承担区县专网网管工作，积极管理和维护专网系统的稳定、安全运行，积极协助市级网络中心开展管理工作。作为一级网管技术部门，负责对辖区专网接入学校（单位）的网络管理与维护工作进行技术指导、监督与检查、考核，负责与上级网管部门的业务对接。

第四条 教育专网接入学校应有校园网络管理机构，并接受市、区两级网管部门的指导。

第五条 针对教育专网的三级覆盖特性，建立成都教育专网

“校级”-“县级”-“市级”三级网管联动工作机制。通过市级网络中心统一建设的市、区两级网管协同工作信息平台，积极实施专网《月运行报告》、《月运情通报》机制；实现对专网全网管理工作信息、预警信息、管理策略等的及时发布与通告；面向全网用户提供丰富的在线交流、技术答疑与辅导等互动功能，及时处理各种网络故障，处置在线通报的各种网络信息管理事件。

第六条 教育专网各级网管中心应积极协同，切实做好教育专网各类突发事件的防范与应急处理，提高预处理突发事件的能力和水平，形成科学、有效、反应迅速的应急工作机制，确保各级网络中心、专网系统重要实体安全、运行业务安全和数据安全，最大限度减少突发事件危害。

成都教育网网络安全管理制度

第一条 成都教育网所有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教育网站安全、稳定运行及子网站的活动。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、木马程序、间谍软件的;

（八）法律和法规禁止的其他有害信息。

第二条 网络用户发现有害信息和遭到黑客攻击时，须在第一时间向网管中心报告。网管中心在已保存有关信息和日志记录的前提下，应及时删除有关信息，恢复系统的正常运行和服务。情况紧急时，应采取关闭相关设备或暂停服务应用等积极措施，制止其扩散。情节严重或影响恶劣的，区级网管中心应及时上报市级网管中心（成都市教育技术装备管理所）或直接向公安网监部门报告，并协助查处。

第三条 任何单位和个人不得在教育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 教育网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 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，必须经信息发布工作负责人初审和单位分管领导签审后才可发布。

第六条 教育网各接入单位和学校要确定一名负责人为本单位网络安全责任人，领导网管机构做好本单位和学校的网络和信息安全工作，积极建立和实行岗位责任制。

第七条 网络管理人员应加强责任心，保证各设备、系统的良好运行，充分发挥效率，最大限度地为用户服务、为教育服务。

第八条 教育网各接入单位和学校各信息终端用户须受网络管理员监督管理。区级专网要统一出口、统一管理；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；要建立上网日志记录，时间不少于 90 天，方便日后的检查和监督工作。

第九条 与教育网站内网实施联网的网络系统与计算机，必须事先向网管部门提出申请，由网管中心建立用户档案并备案后，方可联网。

第十条 教育网站（含各子站）的信息数据要实施保密措施。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）可向本城域网站公开的；

（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。

第十一条 任何单位和个人不得利用联网计算机从事下列危害教育网站及本地局域网安全的活动:

（一）未经允许，非法访问、远程连接和管理及控制教育网站的服务器、工作站及其它相关设备和系统;

（二）未经允许，对教育网站上所具有的功能、程序、数据进行删除、修改和增加;

（三）故意制作、传播计算机病毒与破坏性程序;

（四）其他危害教育网站安全的行为。

第十二条 严禁在网络上使用来历不明、引发病毒传染、木马传播的软件,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进行查杀。

第十三条 故意输入计算机病毒，造成危害城域网站及网站网络安全的,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。

第十四条 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。

第十五条 教育网络范围内从事施工、建设，不得危害网络系统的安全。

第十六条 违反本管理制度，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。

网络管理员职责

第一条 热爱本职工作；努力钻研业务，积极掌握最新技术动态。

第二条 执行国家相关法令、法规，严格遵守各项网管规章制度。

第三条 正确、规范使用设备，保证网络系统处于良好运行状态。

第四条 积极熟悉机房设备及系统性能，认真细致作好日常监控工作；及时排除安全隐患，解决故障，积极为各应用系统正常使用提供技术和服务支持保证。

第五条 设备及系统运行出现异常紧急状态时，应及时上报。

第六条 建立机房硬件和软件的财产登记制度，做到帐物相符。作好各种工作设备、器材、技术资料、软件资料的规范化管理。

第七条 做好网管日志工作；每月应向主管人员提交当月工作及事件记录。

第八条 保持设备机房、网管用房室内整洁，网管用房清洁工作每日一次，设备机房保洁工作每周一次。

第九条 上班时间，不利用计算机及相关设备进行与工作无关的活动；不得收看反动、色情的内容；不得在网上存储、发布或传播具有反动、黄色、暴力等有害内容的信息。

第十条 离开时，应对机房进行检查，认真作好防火、防盗工作。

第十一条 严格遵守值班制度，服从值班安排。

网络权限管理制度

为进一步加强成都教育专网网络的安全管理，避免操作权限失控，保证教育专网的正常运转，维护教育专网用户的上网秩序，特制定本制度。

第一条 教育专网各级网络中心（市级网络中心、区级网络中心、校园网络中心）负责管理应辖范围内的所有服务器，网络通讯、数据交换、信息网络安全及其他相关设备及系统，非工作人员不得擅自操作，修改和调整其设置参数和服务功能等。

第二条 教育专网各级网络（城域骨干网络、县域主干网络、校园接入网络）核心管理设备和系统，网络中心应正确分配权限，并实施严密管理口令予以保护，口令应定期修改，非工作人员严

禁使用、扫描或猜测口令。

第三条 教育专网各级网络中心核心与主要设备、系统等的配置信息，各级网络中心应积极做好定期备份工作，确保在系统发生故障时能及时恢复，以保障教育专网系统的正常运行。对因工作需要而改变、调整的设置参数等，须做好登记、备案工作。

第四条 教育专网的各使用单位、部门及人员应对网络中心分配的上传和下载口令予以保护，如因保护不善而造成的不良后果由使用人员自行承担。

第五条 需设立 WEB 服务器、FTP 服务器等公开站点的部门，须向网络中心提出申请，填写登记表格，由使用部门负责人签字同意，并经单位主管领导审核批准后方可设立，同时应指定专人负责管理。上述站点都要接受上级网络中心的监督。

第六条 网站信息内容更新由网站建设部门负责实施。

第七条 各级网络中心、各使用部门管理人员要明确管理职责，不得擅自将自己操作权限转交他人，避免操作权限失控；未经批准不得超越权限操作。

第八条 严禁供应商（厂商）通过技术手段对已投入运行的教育专网各级网络核心通讯和安全保护设备（系统）等进行遥控和远程维护。已投入运行的系统数据未经批准严禁向厂家或第三方提供远程管理及使用权限。

第九条 严格遵守保密纪律，增强保密意识，不能向无关人

员泄露教育专网网络的 IP 管理部署体系以及专网核心设备及系统的参数配置、管理帐号等技术资料。

密码管理制度

第一条 网络建设、管理与维护等人员应严格执行密码管理规定，规范使用；对操作密码定期更改，任何密码不得外泄，如有因密码外泄而造成各种损失的，由当事人负全部责任。

第二条 不同级别的管理人员应掌握有不同权限的密码，密码由各管理人员负责，不得记在纸上，不得用字母或数字简单构成，应规范设置。

第三条 最高级别密码最多只能由两名最高管理人员掌握。

第四条 如因安装软硬件网络设备而需要安装单位知道密码的，在安装调试好后，应及时更改。

第五条 各级各类帐号及密码不得公开与透露。因用户个人原因造成自己的帐号和密码丢失的，将由用户个人承担一切后果。

中心机房管理制度

第一条 机房出入管理

（一）机房钥匙由机房工作人员保管，不能随意转借，丢失要及时上报。

（二）机房工作人员早进入、晚离开时应检查服务器、网络设备、安全设备、机房运行保障系统等设备运转是否正常；离开时察看灯、门、窗、锁是否关好。

（三）加强安全防范意识，中心机房无人时必须锁门。

（四）值班期间，值班人员不能擅离岗位。

（五）严禁非中心机房管理人员、操作人员进入机房，特殊情况需经网管中心负责人批准，并认真填写登记表后方可进入并保证至少一名机房工作人员在场。

（六）进入机房人员应遵守机房管理的各项规章制度，更换专用工作鞋或鞋套。

第二条　机房参观管理

（一）经领导批准，外来人员才予安排参观。

（二）外来人员参观机房，须有单位指定人员或网管人员陪同。

（三）处理秘密事务时，不得接待参观人员或观看。

（四）参观人员未经网管负责人同意，不得擅自操作和调阅文档资料。

（五）参观人员应遵守机房管理制度；不得拥挤、喧哗、损坏机房设备设施。

（六）参观结束后，网管人员应整理如常。

第三条 机房安全管理

（一）机房工作人员随时监控中心设备运行状况，发现异常情况应立即按照正确规程进行操作，发现重大问题应及时上报。

（二）完善网络安全机制，定时升级病毒库、规则库，及时做好防“黑”、防病毒、防木马工作。

（三）非机房工作人员一律不准擅自操作机房任何设备。

（四）机房工作人员应严格执行密码管理规定，对操作密码定期更改，任何密码不得外泄。

（五）机房工作人员应恪守保密制度，不得擅自泄露中心各种信息资料与数据。

（六）机房内严禁吸烟、喝水、饮食、嬉戏和进行剧烈运动，保持机房安静。

（七）定期对机房内设置的消防系统、器材及设备、不间断电源等进行检查及维护，以保证其有效性。

（八）进入机房人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品。机房及周边地区严禁烟火，不能明火作业。

第四条 机房操作管理

（一）机房工作人员应密切监视中心设备运行状况，确保安全、高效运行。

（二）严格做好各种数据、文件的备份工作。所有重要图片、文档和中心服务器数据库要定期进行备份和保管。

（三）机房工作人员未经负责人批准，不得在中心机房设备上编写、修改、更换各类软件系统及更改设备参数配置。

（四）各类软件系统的维护、增删、配置的更改，各类硬件设备的添加、更换必须经单位负责人批准后方可进行。

（五）每日对机房环境进行清洁，以保持机房整洁；定期进行一次大清扫，对机器设备吸尘清洁。

（六）部门负责人应定期与不定期对制度的执行情况进行检查，督促各项制度的落实，并作为人员考核之依据。

第五条 软盘、光盘、技术资料管理

（一）中心机房数据资料盘片、技术文档等归类集中存放，由专人统一保管，个人未经许可不得复制或复印和随便带离、外借。因工作需要允许外借时，应有详细记录。

（二）严防使用网络中心的软件从事商业牟利活动

（三）各类盘片使用应有明确记录，注明盘片使用用途。无法继续使用盘片经检查，确认它方无法进行数据恢复后方可报损。

（四）建立软件安装使用档案，注明软件名称、所安装使用的系统及使用人员等信息。

（五）外来程序、数据盘片和软件须经检查后方可使用，必

要时留存保管。

（六）重要数据、资料的保管应选择在安全、防盗场所。

专网设备使用管理制度

成都教育专网属自建、自管专网，组网路由器、交换机、内容审计、存储设备、服务器等是专网系统运行和承载业务正常服务的重要保证。成都教育专网各级网管、技维人员等应规范使用设备，保证网络系统处于良好运行状态。

第一条 各级网管、技维人员等应严格遵循设备《使用手册》相关要求和注意事项，规范操作行为；

第二条 严禁在无技术论证、无产品厂商和教育专网建设商技术指导与支持的情况下对专网设备进行部件拆卸或添加以及对路由器、交换机等重要核心设备配件及模块进行调换和混用；

第三条 严禁在无备份和无恢复措施及应急预案的情况下对网络中心设备、系统等的参数配置进行调整、改动以及对系统实施切换；

第四条 加强机房在后续完善建设、扩充建设项目实施过程中的施工现场安全管理与监管，杜绝人为损坏和破坏性施工等情况的发生。

第五条 积极作好对专网设备、物资的专项使用和财产安全

管理，作好常规、维护保养工作。

第六条 积极保持机房环境整洁与规范，使设备及网络系统处于良好运行状态和安全运行环境。

计算机病毒防范和安全漏洞检测制度

为保证教育专网系统的正常运行，防止各类病毒、木马程序、黑客软件对网络系统构成的威胁，最大限度地减少此类损失，特制定本制度。

第一条 教育专网各级网络的管理和维护部门应有较强的计算机病毒防范意识，随时了解和掌握最新的病毒发展趋势，根据不同病毒的发作条件及发作时间、周期、特征等，建立病毒预警和公告机制，作好防范工作。

第二条 教育专网各级网络中心应采用合理的计算机病毒防范技术和手段对网络系统进行有效监控，切实保证教育专网安全、稳定的运行。

第三条 教育专网各级网络内所有的服务器、计算机单机都须安装经公安部门认定合格的计算机防、杀病毒软件（系统）。并定期对防、杀毒软件进行病毒库或系统模块升级，保证处于最新功能服务状态。

第四条 定期对系统进行病毒和木马程序的检测与查杀，防

止病毒感染、传播和信息资料被窃取。 发现病毒、木马程序，但不能彻底清除或仍存在安全隐患时，应及时备份染毒文件，并通过合法、规范途径上报公安机关。

第五条 严禁使用来历不明或无法确定其是否含有病毒的存储介质。若确需安装，安装前应进行病毒检测，确认无病毒后方可使用。

第六条 经远程通信传送的程序或数据，须事先经过检测确认无病毒后方可使用。对外发布或传送的数据、信息须事先进行有效的病毒检测。

第七条 有 FTP 账号的工作人员负责上传下载文件的安全，如发现上传下载文件含有病毒，应及时查杀，并找出病毒文件来源。

第八条 专网使用用户，禁止登录非法网站，发现垃圾邮件、来路不明或携带病毒的，不要随意打开，应立即彻底删除。定期对邮箱进行清理和维护。

第九条 为防止单机系统被非法侵入，教育专网各级网络中心内网所有操作系统为 windows2000、windows2003、windowsXP 或 windows7 的办公机器，应设置规范的操作系统管理员密码。

第十条 教育专网各级网络服务器除因应用的客观需要外，均应开启防火墙功能。为加强单机防病毒能力，强调病毒以“防”为主的思想，所有操作系统为 windows2000、windows2003、

windowsXP 或 windows7 的计算机，必须打开 Windows 自动更新程序，及时安装和更新各类系统补丁。

第十一条 教育专网各级网络中心应对下级网络进行有效的网络安全配置，并要求下级单位报告已发现网络安全漏洞。

第十二条 网络技术员应定期对服务器进行系统漏洞扫描并及时安装和更新各类系统补丁。避免安全漏洞出现，抵御他人攻击。

第十三条 网络管理中心应随时检查 Windows 防火墙、在线病毒检测等网络安全技术措施的配置，以防止网络安全漏洞造成的后果扩散。

第十四条 新购置的计算机，在使用前应当认真检查，积极采取防止计算机病毒感染的措施，试运行正常后，才能投入正式运行或者联网运行。

第十五条 严格执行计算机操作规程和各项管理制度，加强管理人员和工作人员的防病毒教育，应积极作好对广大师生安全防范技能的相关基础培训工作。

信息发布、审核、登记管理制度

为进一步提高信息发布的质量，加强安全管理，使成都教育专网信息发布工作规范化、制度化，更好的为教育教学工作服务，

严防信息安全事故，特制定本制度。

第一条 信息发布工作要严格审核和管理，确保上网信息的合法性、真实性、准确性，符合国家有关的各项法律、法规制度。

第二条 任何人员不得利用本单位计算机和网站信息发布系统，从事危害国家安全、泄露国家秘密，不得从事赌博违法犯罪活动，不得侵犯国家、社会、集体利益和其他公民的合法权益，不得制作、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，扰乱社会秩序和破坏社会安定团结的;

（六）宣扬封建迷信、淫秽、色情、邪教、赌博、暴力、凶杀、恐怖、邪教、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。

第三条 上网的信息需填写《上网信息审核登记表》，必须经审核，并以电子文档形式进行登记。未经审签的信息不得以任何

理由或借口在网上发布。

第四条 信息采集员完成信息源的采集和编录，完成制档并签字；信息员对所提供的信息内容合法性、真实性等负责。

第五条 网络信息安全工作主要负责人负责完成对发布信息的审核，并签署审核意见。负责信息审核工作的人员应在充分理解国家有关的各项法律、法规制度的基础上及时处理信息发布的申请，并将审核意见及时反馈。

第六条 信息的上传须由单位内政治可靠、业务能力强、有责任心的同志担任和完成，其他任何人员均不得参与信息的上传工作。

第七条 凡经正式发布的各类网上信息在发布后均应作好电子文档备份。

第八条 负责发布的人员对所收到的经过审核后的信息在确认审核意见后，应及时在网上发布，以确保发布信息的及时和准确。上传后，发布人应对信息原档进行即时保存，并在网上完成对信息内容的检查和校对，确定无误。同时完成发布人、发布时间等上传登记。

第九条 为规范对上网信息的管理，方便上级部门的检查。凡有关信息采集、发布、审核和上传登记的所有人员签名、审核意见、发布过程记要以及发布的文件、数据、文字及图像等资料均由学校指定的负责部门或人员统一归口管理。

第十条 教育专网各级网络管理人员、网络安全员必须定期检查各网站内容及论坛、留言板等交互式栏目发表的内容，检查个人使用的计算机和公共用机，若发现其包含有害信息的必须删除，保留发布信息者的注册资料(包括登录 IP)与有害信息，有违反法律法规的应及时交予公安部门查处。

论坛、聊天室、留言板等电子公告服务管理制度

为加强对教育专网电子公告服务（以下简称电子公告服务）的有效管理，规范电子公告信息发布行为，维护国家安全和社会稳定，保障公民、法人和其他组织的合法权益，根据《计算机信息网络国际互联网安全保护管理办法》和《互联网电子公告服务管理规定》的规定，制定本制度。

第一条 本规定所称电子公告服务，是指以电子论坛、网络聊天室、留言版等交互形式为上网用户提供信息发布条件的服务行为。

第二条 开展电子公告服务，应建立健全用户实名登记和信息管理制度,且应当具备下列条件:

（一）有确定的电子公告服务类别和栏目;

（二）有完善的电子公告服务规则和注册警示;

（三）有安全保障措施，包括上网用户登记程序、上网用户

信息安全管理制度、技术保障设施;

（四）有相应的专业管理人员和技术人员，能够对电子公告服务实施有效管理。

第三条 上网用户使用电子公告服务系统，应当遵守法律、法规，并对所发布的信息负责。

第四条 应对用户进行安全知识传递，提高其网络安全、法律意识。

第五条 落实网络管理员和版主职责，共同维护电子公告系统的信息安全 。

（一）对版主的聘用本着认真慎重的态度、认真核实版主身份，做好版主聘用记录;

（二）对各版聘用版主实行有针对性的网络安全教育，落实版主职责，提高版主的责任感;

（三）落实信息的“先审后发”管理，必须将审核职责落实到人。版主负责检查各版信息内容，如发现违反国家法规、规章的应即时予以删除，情节严重者，做好原始记录，报告网络管理员和学校信息网络安全管理机构。

（四）网络管理员负责考核各版主，如发现不能正常履行版主职责者，将予以警告，严重者予以解聘;

（五）在版主负责栏目中发现重大问题未得到及时解决者，即时对版主予以解聘。

第六条 网站开通的论坛、贴吧、留言板等交互式栏目应采用技术成熟、符合规定的程序模板，日志记录数据要完备。

（一）日志记录应能够记录访问者的 IP 地址；被访问过的网页、资源；被访问的开始和结束时间；

（二）具备确认使用者真实身份的功能和措施，使用者必须通过登录验证后才能发布信息，要有限制未明身份用户发布信息的功能；

（三）记录用户上传和发布过的内容等信息；

（四）系统能准确记录使用者的操作过程。这些系统日志记录信息应最少保存 60 天。

第七条 各单位要注意清理缺乏有效管理的交互式栏目。在因工作需要临时产生的、试验使用的网站论坛、留言板等交互式栏目，在工作结束或使用完毕后必须立即清理删除。

第八条 不断提高网站的防黑、防病毒防范能力。及时对服务器安装系统补丁程序，及时升级防杀毒和木马程序专杀的软件系统。作好网站以及交互式栏目中各目录的访问权限设置和检查工作。

第九条 一旦发现网站、论坛、留言板上出现不良内容、异常现象，应先立即保护现场，保留有关原始记录，备份数据和日志，暂停相应的网站和交互栏目，及时上报上级信息网络安全管理部门。需要公安部门协助的，可以直接通过网上报警服务上报

公安网监部门。

24 小时交互式栏目信息巡查制度

为进一步加强对教育专网网站论坛、留言板等交互式栏目的有效管理，根据《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》和《互联网电子公告服务管理规定》等国家法规、规章，特制定本规定。

第一条 凡在网站或服务主页上开办了公告栏、论坛、聊天室、留言板等交互式栏目的，每个栏目均须确定专人进行信息安全管理;

第二条 各栏目负责信息安全管理的人员须每日定时巡查栏目内包括 FTP 上传的信息，敏感时期按有关部门的通知要求值守。

第三条 各栏目负责信息安全管理的人员若发现栏目内出现有害信息、不良信息及其他违反国家法律法规的信息，须在保存好有关记录（发贴人的 IP、发贴时间和内容等）后立即删除有害信息，并及时报校网络管理中心。校园网管理中心按规定要求和程序向上级有关部门报告，必要时协助有关部门查证。

第四条 单位负责信息安全的专管人员每天定时对网站主页以及论坛、聊天室、留言板等交互式栏目信息进行巡查、监管。

第五条 单位负责信息安全的专管人员在发现或接到栏目管理员或用户有关有害信息的报告后，要认真做好详细情况记录，并按程序逐级上报。

第六条 对公安机关公共信息安全监察部门确定需查证的案件，各级负责信息安全管理的人员要认真协助调查，并做好详细记录，必要时须提交书面调查报告。不得拖延、推委。

信息监控、保存、清除和备份制度

为加强对教育信息网络安全的有效管理，维护国家安全和社会稳定，根据《计算机信息网络国际互联网安全保护管理办法》及相关规定，制定本制度。

第一条 教育信息网络是进行教育管理、教育教学、学术研究的信息化媒体，教育网络接入单位信息网络安全领导小组必须对所发布的信息进行有效的审查和监视。

第二条 教育网络网络中心和信息安全负责部门必须定时对已发布的合法信息进行有效的安全监视，以确保运行安全，信息不受外来的非法攻击。

第三条 教育网络网络中心、相关系统管理维护部门及人员应将每次新近发布信息进行有效备份，以便在出现系统故障或信息安全异常情况时能及时进行恢复。

第四条 指定的责任部门或人员应将信息发布工作过程的全部原件按要求进行统一归口管理和存档。包括各种方式、形式的信息原档以及凡有关信息在采集、审核、发布和上传登记的所有环节签名、审核意见等。

第五条 各上网场所应严格上网制度，对各上网主机实行责任使用，严格按照有关规定使用网络，禁止利用网络浏览、下载、保存反动以及黄赌毒等违法信息。

第六条 负责网络信息管理的部门及人员应对网络运行进行随时监控，对网上不良信息及时进行清除，对网上的不良行为及时处理，以保证校园网络的良好运行。

第七条 教育网络网络中心、负责网络信息安全的人员须定期对计算机信息系统运行日志进行备份，确保有 60 天的日志记录留存，个人用户上网记录必须保存 60 天以上。

第八条 教育网络网络中心、负责网络信息安全的人员定期对系统安全运行日志进行必要的巡查，对出现的安全隐患进行必要的处理。

突发事件应急处理制度

为切实做好成都教育网对突发事件的防范与应急处理，进一步提高预处理突发事件的能力和水平，形成科学、有效、反应迅

速的应急工作机制，确保成都教育网市、区两级网络中心及专网系统重要实体安全、运行业务安全和信息数据安全，最大限度减少网络中心信息网络安全等突发事件的危害，根据《成都教育专网信息网络突发事件应急预案（试行）》相关要求，特制定本制度。

第一条 教育专网各级网管中心应对信息网络系统的日常运行状态、服务功能等及时进行监控。

第二条 一旦发现系统被攻击、破坏或出现不良、有害、反动等违反国家法规或明令禁止的信息，应在第一时间进行相关页面信息内容、网络监测数据、和相关系统运行日志等证据的备份保留。对不良、有害、反动等违反国家法规或明令禁止的信息在确定证据保留后立即进行删除并恢复正常；对无法进行即时处理的，应立即切断系统与互联网的通讯链路或停止相关服务（进行现场保留），同时报告校信息安全工作管理机构和公安机关。分析、查找原因，总结教训，并制定积极防、治措施，加强管理。

第三条 遇到已有病毒防治产品无法清除的计算机病毒或病毒引起的计算机系统瘫痪、程序和数据严重破坏等情况时，应立即断开网络、关闭计算机，防止病毒扩散、数据丢失；全面检查其它工作站有无相同现象；立即向上级报告，需要技术支持的可同时与计算机反病毒厂商联系；病毒处置工作完成后，应积极分析病毒感染的原因和教训，及时制定、修改病毒防治策略。

第四条 及时作好操作系统、数据库系统漏洞补丁和反黑、防杀病毒、木马查杀等软件（系统）的升级工作，检查系统防火墙，确保其处于良好的运行状态。

第五条 遇到黑客攻击可以根据不同情况分别采取加强保护、中断对方连接、反跟踪等及其它处理措施或启用备份系统恢复。

违法犯罪案件和事故、病毒、有害信息报告、协查制度

为加强对教育专网信息安全的有效管理，维护国家安全和社会稳定，根据《计算机信息网络国际互联网安全保护管理办法》及相关规定，坚决防止、杜绝计算机信息网络犯罪行为的发怔，特制定本制度。

第一条 成都教育专网各接入单位和网络用户应当自觉遵守网络法规，严禁利用计算机从事违法犯罪行为。

第二条 网管部门发现网内有害信息或网内用户的网络违法违规情况，应及时向主管领导和上级主管部门报告，协助相关部门做好查处工作。

第三条 任何使用本单位网络的人员若发现有害信息时应及时通知网络安全员。

第四条 网络管理员发现有害信息，应当及时采取措施制止，

并立即上报主管部门。

第五条 教育专网各级网络遭受到病毒、黑客的攻击，应报告主管部门，同时做好查杀病毒和系统保护工作。

第六条 各用户对计算机信息系统中发生的违法犯罪行为和危害网络运行的重大安全事件和事故，应采取应急措施防止危害扩大，保留有关原始记录，并在24小时内向主管部门报告。

第七条 教育专网各级管理中心应对校园网络的运行安全进行有效监控，密切关注网络违法案件和不良事件的发展等，情节严重的要及时上报公安机关，尽量做到防患于未然。

第八条 教育专网各级网络管理中心应对教育专网信息网络安全进行有效监控，发现任何违反网络安全法规的或传播有害信息的人员，立即报送公安机关网监部门，交予公安部门查处。

第九条 对于他人利用本网发生的计算机违法犯罪行为，网络技术员应当及时制止并立即上报公安机关网监部门。

第十条 对于本网所遭受到的攻击，网络技术员应在发现情况的3小时内上报当地公安机关网监部门，同时做好系统保护工作和原始记录。

第十一条 教育专网各级网络管理中心及任何使用本单位计算机网络的人员应配合公安机关追查有害信息、有害电子邮件的来源，协助做好取证工作；应积极配合公安机关对违法案件的查处。

第十二条 按照公安机关意见，若需保守机密的，本单位人员必须遵守相关，不得向外透露相关信息。

第十三条 教育专网各用户有义务接受网络管理员和上级主管部门的监督、检查，并应积极配合做好违法犯罪案件的查处工作。

第十四条 教育专网各级网络管理中心要对信息网络系统的有关运行日志进行有效保存，以便于对违法事件的查处。

教育网站及从业人员自律条约

为进一步规范我市教育网站建设与信息服务行为，维护我市良好教育信息网络发展环境，更好地为成都教育信息化、现代化建设服务，特制定本规则：

第一条 遵循爱国、守法、公平、诚信的基本原则，从维护国家和教育网站整体利益的高度出发，自觉遵守国家有关法律、法规和政策。

第二条 始终高举爱国主义旗帜，大力弘扬中华民族优秀文化传统和社会主义道德。

第三条 不制作和传播危害国家安全和社会稳定、违反法律法规以及淫秽、色情、迷信等有害的信息,坚决抵制与中华民族优秀文化传统和道德规范相违背的信息内容。

第四条 教育新闻信息服务要尊重和保护知识产权;提供的新闻信息内容导向正确、客观真实、来源合法；提供的其他服务文明健康。

第五条 加强管理，自觉维护广大用户的合法权益，引导广大用户文明使用网络，增强网络道德意识，自觉抵制有害信息的传播。

第六条 不与非法网站建立任何性质的合作关系；不与其他网站或企业建立违背政府有关部门规定的联盟或协作关系。

第七条 对利用互联网络电子公告服务系统，短信息服务系统传播淫秽、色情等不良信息的用户，应将其 IP 地址列入“黑名单”，对涉嫌犯罪的，并主动向公安机关举报。

第八条 自觉接受政府和相关行业部门的管理和公众的监督，加强网站及从业人员的管理和教育，提高从业人员的业务和道德水平。

第九条 自觉遵守本规则的自律要求，在网站内部形成严格规范的自律机制，推动本规则的实施。