四川省绵阳职业技术学校信息安全领导小组

负责校园内网络安全和信息安全管理工作，定期对学校网络用户进行有关安全和网络安全教育并对上网信息进行审查和监控。

组　长：赵全伦　学校党委书记、

副组长：唐　军　学校党委副书记、校长

成　员：汪　芳　学校副校长

刘江岚　学校副校长

张　杰　学校工会主席

熊　刚　学校党政办主任

杨　宴　学校教导处主任

赵永海　学校信息中心主任

四川省绵阳职业技术学校计算机安全管理责任人制度

1、各办公室、教室及功能室计算机实行使用责任人负责制，各责任人全权负责设备的管理、维护和正常使用。如果遇到不能解决的问题及故障，按照《学校电教设备报修制度》及时报修。

2、要严格按照计算机操作规程进行操作，不得非法操作。

3、未经许可，不准外来人员操作计算机，登录学校网络。

4、不准随意将学校服务器上的资料复制给他人使用。

5、对于来历不明的软件不能上机使用，确属教学需要，必须先杀毒后使用。

6、不准在计算机上安装带有病毒的软件。

7、不准在计算机上安装各种游戏软件及播放娱乐性光碟。

8、不准在学校计算机上浏览不健康的网页。

9、严禁故意制作、传播计算机病毒等破坏性程序。

10、不准利用互联网侮辱他人或者捏造事实诽谤他人。

11、不准非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密。

12、不准利用互联网进行盗窃、诈骗、敲诈。

13、不准随意拆卸主机箱，更换鼠标、键盘、音箱、显示器等。

14、计算机长 时间 不用时，要关闭计算机，并切断电源。

四川省绵阳职业技术学校信息发布、审核、登记制度

计算机信息发布实行各信息发布部门提出申请，校长、办公室审核批准，信息中心具体实施的办法，各部门在信息发布方面必须恪守如下规定：

1、发布申请部门应当确保发布信息准确、真实，符合国家有关的各项法律、法规制度；

2、信息发布部门应当对所发布的信息备案记录，以加强管理；

3、信息审核部门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申请部门的请求，并将审核意见及时反馈给申请部门；

4、在审核部门同意的基础上应将信息及时转发给信息中心；

5、信息审核部门应当做好信息请求、处理、转发的备案工作；

6、信息中心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，并确保发布信息的准确性；

7、信息中心对所发布的信息应当做好备案工作。

四川省绵阳职业技术学校信息监视、保存、清除和备份制度

为保证我校校园网健康、安全，高效的应用和发展，杜绝各类违法、犯罪行为的发生，特制定本制度：

1、各级网络管理员应当对本部门的网络使用情况监督、检查，坚决杜绝访问境内外反动、黄色网站，不阅览、传播各类反动、黄色信息；

2、各级网络管理员应当保证本部门计算机内 日志 文件及其他重要数据的完整性、真实性，并做好备份工作，配合各类安全检查；

3、发现本单位计算机存有各类反动及不健康信息，各级管理员应当及时清除，情节较重的应及时上报信息中心；

4、信息中心应定期检查部门计算机内信息状况，对于发现的问题及时处理；

5、各单位上网人员应当强化思想意识，自觉遵守网络法规，积极配合本单位网络管理员做好本单位计算机网络信息安全工作；

6、信息中心在收到部门的报告后应立即向主管领导汇报，并组织调查取证工作，配合上级主管部门的调查。

四川省绵阳职业技术学校病毒检测和网络安全漏洞检测制度

为保证我校校园网的正常运行，防止各类病毒、黑客软件对我校联网主机构成的威胁，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公安部认证的防病毒软件、防黑客软件及垃圾邮件消除软件，并对软件定期升级。

2、各接入部门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、信息中心应定期发布病毒信息，检测校园网内病毒和安全漏洞，并采取必要措施加以防治。

4、校园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。

四川省绵阳职业技术学校网络违法案件报告和协助查处制度

计算机信息网络国际互联网上充斥着大量的黑客、病毒、网络陷阱、色情、非法言论等不安全因素和有害信息。为了加强对互联网的安全保护，维护公共秩序和社会稳定，有效地打击利用互联网进行违法犯罪活动，我校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互联网进行的违法犯罪活动。

为规范我校网络违法案件报告和协助查处的方式，现制定如下制度：发现以下行为之一的，我校将及时向公安机关计算机安全监察机构进行报告。

一、校园网使用用户利用国际联网危害国家安全、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，从事违法犯罪活动。

二、校园网使用用户利用国际联网制作、复制、查阅和传播下列信息：

1、破坏宪法和法律、行政法规实施的；

2、煽动颠覆国家政权，推翻社会主义制度的；

3、煽动分裂国家，破坏国家统一的；

4、煽动民族仇恨、民族歧视，破坏民族 团结 的；

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、教唆犯罪的；

7、然侮辱他人或者捏造事实诽谤他人的；

8、害国家机关信誉的；

9、他违反宪法和法律、行政法规的。

三、校园网使用用户从事下列危害计算机信息网络安全的活动：

1、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；

2、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；

3、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；

4、故意制作、传播计算机病毒等破坏性程序的；

5、其他危害计算机信息网络安全的。

四、校园网使用用户违反法律规定，利用国际互联网侵犯用户的通信自由和通信秘密等等。

四川省绵阳职业技术学校账号使用登记和操作权限管理制度

为了保护我校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，现制定本帐号使用登记和操作权限管理管理制度。

一、校园网络计算机入网申请制度

1、凡学校工作场所的计算机，因工作需要，均可申请计算机入网;

2、申请入网的计算机需指定负责人，报经学校批准，由学校网络中心负责开通网路;

二、校园网络用户申请制度

1、凡学校在职教职，均可免费申请为校园网络用户；

2、申请校园网络用户的教职工需要上报姓名与身份号码，并保证其资料的真实性;

三、校园网 ip 地址管理制度

1、学校网络用户的 ip 地址,由信息中心负责统一管理和分配;

2、每位老师使用的电脑应使用固定 ip 地址并进行绑定，使用真实姓名对计算机进行命名。

3、未经申请批准入网的计算机，不得私自占用其它计算机的 ip 地址或私自乱设 ip 地址，不得私自连接其它入网计算机。网络中心有权切断乱设的 ip 地址入网，以保证校园网络的正常运行。

四、网络账户和操作权限管理制度

1、校园网内各主要网络设备、计算机服务器系统由信息中心统一管理，其他任何人不得擅自操作网络设备,修改网络设置。

2、校园网内各主要网络设备、计算机服务器系统应当正确分配权限，并加口令子以保护，口令应定期修改，任何非系统管理员严禁使用、猜测各类管理员口令。

3、对于网络系统应做好备份工作，确保在系统发生故障时能及时恢复。

4、对于网络系统的设置、修改应当做好登记、备案工作。

5、网络账户申请通过后将根据其日常工作要求设定固定的权限，严禁具有网络授权的管理人员私自提高个别用户的权限;

6、具有对网络内容进行添加、删除、修改等等权限的用户需保护好自己的账户和密码，不得随意出借账户给其他用户。

四川省绵阳职业技术学校网络安全管理人员岗位工作职责

网络是由涪城区信息中心统一接入的教育网，是利用先进实用的计算机技术和网络通信技术。因此我校校园网的所有用户必须遵守网络安全、运行、维护管理办法的有关规定。为规范我校校园网络安全管理，现制定如下网络安全管理人员岗位工作职责。

为规范我校校园网络安全管理，现制定如下网络安全管理人员岗位工作职责。

一、建立并协助管理我校健全的网络安全管理组织：

1、校长为计算机网络安全管理工作第一责任人，负责全面领导本单位计算机的防黄、防黑、防不良信息、防毒等网络安全工作；网络安全管理人员直接向校长负责；

2、学校信息发布明确到个人，网络安全管理人员须负责信息发布的信息安全审核；

3、学校网络安全管理人员要进行网络安全培训。

二、网络安全管理人员岗位日常管理职责：

1、网络安全管理人员应当保障计算机网络设备和配套的设施的安全，保障信息的安全，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；

2、网络安全管理人员必须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》；

3、网络安全管理人员必须接受并配合国家有关部门对本网依法进行的监督检查；必须接受上级网络中心对其进行的网络系统及信息系统的安全检查；

4、网络安全管理人员必须对网络接入的用户，用防火墙技术屏蔽非法站点并保留日志文件，并进行定期检查；

5、网络安全管理人员负责网络安全和网上信息安全。如对网络安全和网上信息安全提出技术措施，须经上级网络中心批准后方可实施；

6、系统管理员每周末对机房的安全情况进行例行检查并记录检查情况；

7、工作人员要树立安全第一的观念，遵纪守法认真贯彻执行《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《计算机信息网络国际联网安全保护管理办法》，保护国家机密，净化网络环境；

8、对用户联网计算机 ip 地址进行添加、删除等操作应做好记录，任何人不得随意更改 ip 地址；

三、网络安全管理人员岗位日常维护职责：

1、每日检查各种设备，确保网络畅通和系统正常运行；

2、定期备份系统数据，仔细阅读记录文件，不放过任何异常现象；

3、规划、管理好各用户组，设定适当用户权限；

4、管理员密码和安全策略属网络中心核心机密，不得泄露；

5、按照正常开、关机顺序启动或关闭设备，非紧急情况不得直接关闭电源，以保证系统的完整性；

6、每周对服务器进行查毒、消毒，禁用未经消毒的存储介质；收集重大病毒“疫情”，提前采取措施；

7、定期维护、保养网络中心交换设备。

四川省绵阳职业技术学校网络安全教育和培训制度

1、定期组织管理员认真学习《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。

2、定期对本单位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。

3、对本单位网络用户进行安全教育和培训，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。

4、不定期地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。

5、定期对学生进行网络安全教育，强化网络安全意识,增强守法观念。

四川省绵阳职业技术学校校园网络安全管理制度

第一条 为了保护我校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，制定本安全管理制度。

第二条 本管理制度所称的校园网络系统，是指由学校投资购买、由网络与信息中心负责维护和管理的校园网络主、辅节点设备、配套的网络线缆设施及网络服务器、工作站所构成的、为校园网络应用及服务的硬件、软件的集成系统。

第三条 校园网系统的安全运行和系统设备管理维护工作由网络中心负责，未经校领导同意、不得擅自安装、拆卸或改变网络设备。

第四条 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，不得危害或侵入未授权的（包括 cernet 或其它互联网在内的）服务器、工作站。

第五条 除校园网负责人，其他个人不得以任何方式对校园网网站进行修改、设置、删除等操作；任何人不得以任何借口盗窃、破坏网络设施。

第六条 网络使用者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。

第七条 校园内从事施工、建设，不得危害计算机网络系统的安全。

第八条 校园网主、辅节点设备及服务器等发生案件、以及遭到黑客攻击后，校园网负责单位必须在二十四小时内向有关部门及公安机关报告。

第九条 严禁在校园网上使用来历不明、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公安部门推荐的杀毒软件检查、杀毒。

第十条 任何人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。

第十一条学校各部门负责人为网络安全负责人。学校微机室一律不准对社会开放。不允许外来人员进入微机室。

四川省绵阳职业技术学校网络安全定期巡查制度

计算机信息网络国际互联网上充斥着大量的黑客、病毒、网络陷阱、色情、非法言论等不安全因素和有害信息。为了加强对互联网的安全保护，维护公共秩序和社会稳定，有效地打击利用互联网进行违法犯罪活动，我校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互联网进行的违法犯罪活动。

为规范我校网络安全的方式，现制定如下网络安全定期巡查制度：

一、实体及人员安全巡查内容：

1、学校网络的建设、改造，是否仍然符合国家标准或行业标准，是否使用经国家认定的设备器材。工程竣工后，是否通过上级部门组织验收方投入使用；

2、学校网络的设计、安装施工，是否由持有对应许可证的单位承担；

3、学校网络线路是否采用管道、直埋、隐蔽方式，尽可能避免明线敷设，以便切实保障网络安全；

4、学校网络实体是否严格按照国家制定的要求存放、使用，是否会有什么安全隐患，发现的安全隐患是否进行了整改等等；

5、学校网络是否具备用户管理、系统监测、适时报警等功能，是否进行最新软件更新、升级等等。

二、网络信息安全巡查内容：

为维护我校网络信息安全，网络安全定期巡查小组人员必须定期对我校网络信息安全进行巡查工作，对如下信息进行删除并追究当事人责任：

1、反对宪法所确定的基本原则的；

2、危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

3、损害国家荣誉和利益的；

4、煽动民族仇恨、民族歧视，破坏民族团结的；

5、破坏国家宗教政策，宣扬封建迷信的；

6、散布谣言，扰乱社会秩序，破坏社会稳定的；

7、散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

8、侮辱或者诽谤他人，侵害他人合法权益的；

9、含有法律、行政法规禁止的其他内容的。

三、网络运行安全巡查内容：

1、学校网络设备进行安全检查，是否具有安全隐患，已查出的安全隐患是否已经排除等等；

2、网络运行是否正常，是否具有较大的安全隐患，如果存在，则必须根据具体情况进行整改，甚至停网进行整顿等等；

四川省绵阳职业技术学校网络信息安全突发事件应急预案

为科学应对网络与信息安全（以下简称信息安全）突发事件，建立健全信息安全应急机制，有效预防、及时控制和大限度消除我校信息安全各类突发事件的危害和影响，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，特定本预案。

本预案适用于我校校园网运行与网络信息方面发生的有可能影响学校安全和正常公共秩序的紧急事件。

一、工作原则与要求

（一）工作原则

1.防范为主，加强监控

宣传普及信息安全防范知识，贯彻预防为主的思想，树立常备不懈的观念，做好应对信息安全突发事件的思想准备预案准备、机制准备和工作准备，从法律、管理、技术、人才等方面，采取多种措施，提高公共防范意识以及基础网络重要信息系统的信息安全综合保障水平。加强对信息安全隐患的日常监测，发现和防范重大信息安全突发性事件，及时取有效的可控措施，迅速控制事件影响范围，力争将损失降到最低程度。

2.以人为本，协同作战

把保障公共利益以及师生的合法权益作为首要任务，由校网络信息安全应急工作领导小组统一领导和协调，督促相部门协同配合、具体实施，完善应急工作体系和机制，最大限度地避免学校及师生员工遭受损失。

3.明确责任，条块结合

按照“谁主管谁负责、谁运营谁负责”以及“条块结合，以条为主”的原则，建立和完善安全责任制及联动工作机制。根据部门职能，各司其职，加强学校部门间、专业科与部门间的协调与配合，共同履行应急处置工作的管理职责。

4.加强储备，常备不懈

加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现信息安全突发公事件应急处置的科学化、程序化与规范化。

（二）工作要求

控制事态，限制在最短时间、最小范围内，使影响和损失减少到最低程度，并尽快恢复学校正常的教学、科研和生秩序。落实工作责任和责任追究制。凡在执行本预案过程中，因工作延误、渎职或不服从指挥、不及时处理，从而造成事拖大、大事拖难、难事拖乱，产生严重后果的，要追究相关人员责任。具体要求如下：

1.明确网络信息安全责任

加强和完善校园网安全管理，采取统一管理和各单位分级负责的管理体制，落实各单位负责人和直接责任人，签署全责任书。各单位要建立健全内部安全保障制度，按照“谁主管、谁负责”、“谁主办、谁负责”的原则，落实责任制明确责任人和职责，细化工作措施和流程，建立完善管理制度和实施办法，加强信息的审查和备案工作，确保网络与信安全。各单位负责人为我校校园网络信息安全管理工作的第一责任人。

2.加强信息审查工作

所有涉密计算机外接国际互联网，必须做好物理隔离。连接国际互联网的计算机不得存储涉及国家秘密、校内部机密的文件。各级各类服务器提供信息服务，必须事先登记、审批，建立使用规范，落实责任人，并具备相应的全防范措施(如：日志留存、安全认证、实时监控、防黑客、防病毒等)，加强网络设备日志分析，及时收集信息，排查安定因素。加强 BBS、留言板等交互式栏目的专人管理，交互

式栏目内容发布实行审核制度，未经审核不得发布，实行块负责制，由版主负责本版块的信息安全，防止信息未经审核即被发布，若出现信息未经审核被发布的情况，应立即关信息发布功能，直至找到原因并排除为止。交互式栏目应具备 IP 地址、身份登记和识别确认功能，对没有合法手续和不备条件的电子公告服务应立即关闭。对于非法网站要做到：发现一个，禁止一个,并及时向主管领导汇报，杜绝其蔓延

立有效的网络防病毒工作机制，及时做好防病毒软件的网上升级，保证病毒库的及时更新。

3.对校园网实施 24 小时监控，必要时实行远程控制

网络管理员应经常对校园网的硬件设备进行状态检查，信息管理员应对校园网上的信息内容进行巡查。对用户上网行实时监控，若发现有异常行为应立即关闭该用户的网络连接，及时记录在案，并对其发出警告和进行批评教育，如发严重违法行为应立即上报有关部门。所有服务器的相关责任人要做到定期检查，认真做好检查记录，了解服务器的工作态，对异常现象和事故及时处理并做好记录。

4.加强突发事件的快速反应

信息化办公室作为校园网的管理部门，要有严格的网络及系统的运行情况监控；宣传部作为校园网络信息内容的监部门，应负责监督、检查各网络系统上发布的信息内容。网络与信息管理员具体负责相应的网络安全和信息安全工作允许有任何触犯国家网络管理条例的网络信息，对突发的网络信息安全事件应做到：

（1）发现后及时向有关部门及领导报告。

（2）保护现场，立即与网络隔离，防止影响扩大。

（3）及时取证，分析、查找原因。

（4）消除有害信息，防止进一步传播，将事件的影响降到最低。

（5）在处置有害信息的过程中，任何单位和个人不得保留、贮存、散布、传播所发现的有害信息。

（6）追究相关责任。根据实际情况提出口头警告、书面警告，停止其使用网络，情节严重和后果影响较大者，提学校保卫处及国家司法机关处理，追究单位负责人和直接责任人的行政或法律责任。

5.及时整顿加强防范

各单位要积极配合信息化办公室的例行检查，并接受其技术指导。针对网络存在的安全隐患和出现的问题，及时提整治方案并具体落实到位，完善信息安全机制，防范信息安全事件再度发生。逐步建立信息安全管理长效工作机制，实校园网络信息安全管理，创造良好的网络环境。

6.在重要、敏感时期，加大网络安全教育宣传力度

加强学生的法律意识和安全意识教育，提高其责任意识和防范能力；开展安全文明上网的教育引导工作，净化校园网上环境，及时收集信息，排查不安定因素；坚持 24 小时值班制度，开通值班电话，保证与上级主管部门、电信部门和地公安机关的热线联系，积极做好预防工作，发现问题及时处理，防患于未然。

7.做好防护措施

做好机房及户外网络设备的防火、防水、防盗、防雷、防鼠等工作。若发生事故，应立即组织人员自救，并报警。

二、应急处理的机构及职责

（一）组织机构

学校成立网络信息安全突发事件应急工作领导小组。组长由分管校领导担任；副组长由党办、校办、信息办公室主要负责人担任；成员由党办、校办、宣传部、教务处、学生处、保卫处、成教院、信息化办公室、计算机专业教研组组成。

在校党委、行政的统一领导下，领导小组随时掌握事态发生、发展的情况，随时汇总、分析、上报情况，确保学校园网的安全，尽快平息事态。

（二）职责

办公室作为校园网络信息内容的监管部门，应负责监督、检查各网络系统上发布的信息内容，并负责舆论监控、管和引导，开展劝阻、疏导工作及法制宣传，同时做好对外新闻联络工作，

对网络违规行为进行查处，根据相关证据及事态影响或破坏程度，对违规者按照相应的制度进行惩处。要时与有关人员深入现场了解情况并开展工作。信息化办公室负责校园网的软硬件系统管理以及日常的网络运行，营造安全稳定的网络环境，做好校园网信息系统全的日常巡查及其日志保存工作，以保证及时发现并处置突发性事件。

三、应急事件分类及处置方法

（一）事件分级

根据网络信息安全突发公共事件的可控性、严重程度和影响范围，一般分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）、Ⅳ级（一般）。

1.Ⅰ级（特别重大）

重要网络与信息系统发生全校性大规模瘫痪，事态发展超出学校的控制能力，对学校安全和正常公共秩序造成特别重损害的突发事件。

2.Ⅱ级（重大）

重要网络与信息系统造成全校性瘫痪，对学校安全和正常公共秩序造成严重损害，需要跨单位协同处置的突发事件

3.Ⅲ级（较大）

某一区域的重要网络与信息系统发生瘫痪，对学校安全和正常公共秩序造成一定损害，但不需要跨单位协同处置的发事件。

4.Ⅳ级（一般）

重要网络与信息系统受到一定程序的损害，对学校师生和其他组织的权益有一定的影响，但不危害学校安全和正常共秩序的突发事件。

（二）处置方法

1.网络出口和核心交换机遭受损坏的，有关人员立即到现场查明事故原因并尽快修复或启动备用设备和出口，同时时通报有关情况。

2.光缆系统受到损坏的，立即组织人员修复，并视影响范围大小决定通报范围。

3.校园网服务器遭入侵的，立即停止该服务器对外发布信息，查找、弥补安全漏洞后，恢复正常的信息并定位攻击源。

4.由于病毒或网络攻击造成网络瘫痪的，及时与上级有关部门和相关专业公司保持联系，针对具体情况拿出修复方案，恢复正常运行。

5.学校主要信息系统受到损害的，立即把有关服务器脱离网络，并查找损害原因，根据不同情况制定恢复办法。

6.对发现发布、传播影响政治稳定的有害信息的，组织人员实行 24 小时网络监控，并开通网络监控电话，发现学校围内的电子公告栏、留言板等交互栏目和网站、网页、个人主页上有发布、传播可能影响政治稳定的有害信息的，立即以处置：保存信息证据，删除或隐藏相关信息，以最快速度缩小影响面，并通知相关管理部门或个人进行处理。情况严的，立即关闭上述有关网络栏目或网站、主页，以待作进一步处理。

7.对利用校园网传播小道消息、泄漏国家秘密问题的，一旦发现，立即保存信息证据，删除或隐藏相关信息，消除响，并对相关管理部门或个人进行批评教育，

责令改正；情况严重的，按照有关网络信息管理的规定进行处理，直至追有关责任人的法律责任。

8.对利用校园网从事非法网上聚集或其他非法活动的，本着“谁主管，谁负责”的原则，上述情况一经出现，立即闭相应网站，通知相关单位主要负责人，果断采取强制性措施，进行紧急处置，坚决予以制止。

9.对利用校园网电子邮件系统和其他途径发送危害国家安全、宣扬法轮功邪教和扰乱社会秩序的各种谣言的，及时握情况，并立即通过删除、隐藏、整理等办法处理信息；通过降低用户等级、封杀用户帐号、批评教育网络用户、隐藏关版面乃至按照有关纪律处理相关用户等，及时消除可能导致不良后果的信息。

四、预案启动和中止

（一）预案启动

发生Ⅲ级及以上网络信息安全突发事件后，即启动本应急预案。

（二）预案中止

网络信息安全突发事件应急处理后，情况得到恢复或得到有效控制，经校网络信息安全突发事件应急工作领导小组讨论结束应急状态，并上报有关领导和部门。