# 最新网络安全应急预案应当按照事件发生后的(大全12篇)

来源：网络 作者：夜幕降临 更新时间：2024-08-30

*在日常的学习、工作、生活中，肯定对各类范文都很熟悉吧。相信许多人会觉得范文很难写？下面我给大家整理了一些优秀范文，希望能够帮助到大家，我们一起来看一看吧。网络安全应急预案应当按照事件发生后的篇一网络安全为人民，网络安全靠人民二、活动时间\_\_...*

在日常的学习、工作、生活中，肯定对各类范文都很熟悉吧。相信许多人会觉得范文很难写？下面我给大家整理了一些优秀范文，希望能够帮助到大家，我们一起来看一看吧。

**网络安全应急预案应当按照事件发生后的篇一**

网络安全为人民，网络安全靠人民

二、活动时间

\_\_\_\_年9月19日——9月25日，其中9月20为主题教育日。

三、参加对象

全校教职工、学生和家长。

四、活动形式

(一)氛围营造

学校在宣传活动期间，用led电子显示屏、微信公众号、网站、q群等多种形式宣传网络安全，营造良好的宣传氛围。

(二)电子屏滚动播出

利用学校大门处的led电子屏，滚动播出网络安全宣传知识，介绍防信息泄露、防网络诈骗等网络安全相关知识。

(三)开展活动

学校以网络安全宣传为主题，通过开展主题队会、举办讲座、国旗下讲话等形式开展网络安全宣传活动。(班主任和德育处提供图片)

(四)网络宣传

学校网站、学校q群、班级q群和翼校通多渠道宣传网络安全知识。(班主任提供发家长q群、发翼校通的图片)

五、活动要求

(一)各部门、每一位教师要高度重视此次宣传活动，按学校方案落实好每一项工作，学校将组织人员对活动情况进行检查。

(二)各班主任务必将活动开展图片于9月23日上午12：00前传余\_\_，邮箱：\_\_，联系电话\_\_。

**网络安全应急预案应当按照事件发生后的篇二**

1、多媒体专用教室及其它配有计算机设备的教室、办公室。

2、学校广播播音系统。

有下列情况应启动应急预案：

1、多媒体专用教室及其它配有计算机设备的教室、办公室等场所发生火灾。

2、设备发生被盗或人为损坏。

3、发现利用网络传播不良信息现象。

4、计算机网络出现病毒。

1、网络设备使用者或管理者发现上述所列情况之一时，应立即报告网络安全领导小

组负责人，同时控制好现场，火灾时，还要组织学生安全、有序地撤离现场。

2、网络安全领导小组接报后，立即向有关部门报告，同时组织有关人员对现场进行

施救或控制，直至问题解决。

（一）火灾发生时处理办法：

1、当火灾发生时，立即切断电源，同时组织学生有序疏散，并将火情通知领导小组。

2、领导小组接报后，立即向有关部门报告，同时组织校内有关人员灭火、疏散学生，

并派人到校门口引领消防部门或上级有关人员到火灾现场，直至火势扑灭。

3、领导小组配合有关部门调查分析火灾原因，进行防火措施改进。

（二）设备发生被盗或人为损害处理办法：

1、发生上述情况时，使用者或管理者应立即告知学校，同时封闭现场。

2、学校领导小组接报后，立即报告相关部门，并组织相关人员配合有关部门进行调查，直至问题解决，恢复设备使用。

（三）不良信息和网络病毒处理办法：

1、发现不良信息或网络病毒，网络管理员应立即终止不良信息或网络病毒的.传播，同时将情况告知学校机关负责人。

2、学校接报后，一方面向集团信息中心报告，请示处理意见。另一方面通告全校计算机用户防病毒方法，并督促网管员进行杀毒处理，直至网络处于安全状态。对不良信息追查信息来源，对未经学校同意，擅自发布信息而造成不良影响者，由学校与园务会讨论后给予一定的处分。触犯法律者交执法部门追究法律责任。

**网络安全应急预案应当按照事件发生后的篇三**

1、网络安全作为学校安全教育之一，通过班会使迷恋网游的学生从思想上深刻认识网络的危害，调节自己的心态，引导到迎战中考的学习中去。

2、针对同学们对电脑游戏的热爱与迷恋，想以此正确引导，疏导同学们对游戏的把握度。

3、使学生认识到作为一名合格中学生，处在当今的网络时代，我们更应该利用网络资源，搞好我们的学习，提高自身素质。

活动形式：

班会活动

活动过程

一、开场导语

二、畅谈网络

网络对青少年的积极作用：

1、互联网为青少年获得各种信息提供了新的渠道。获取信息是青少年上网的第一目的，许多在学校中难以启齿的问题在网上也可以得到满意的回答。互联网信息容量大的特点最大程度地满足了青少年的需求，为青少年提供了最为丰富的信息资源。

2、开拓青少年全球视野，提使青少年的政治视野、知识范畴更加开阔，从而有助于他们全球意识的.形成。通过上网，可以培养他们和各式各样的人交流的能力;通过在网上阅览各类有益图书，触类旁通，提高自身文化素养。

3、网络有助于创新青少年思想教育的手段和方法。利用网络进行德育教育工作，教育者可以以网友的身份和青少年在网上“毫无顾忌”地进行真实心态的平等交流，这对于德育工作者摸清、摸准青少年的思想并开展正面引导和全方位沟通提供了新的快捷的方法。此外，青少年可以同时和多个教育者或教育信息保持快速互动，从而提高思想互动的频率，提上相约，网下聚会，实现网上德育工作的滋润和补充，从而及时化解矛盾，起到温暖人心，调动积极性，激发创造力的作用。

三、网络交友

你在网络上会交网友吗?你是怎么看待网友这个角色的?

案例一，网名为沙子的南京某大学英语专业学生，在聊天时被聊天经验丰富的伊春市毕冬冬的“网上形象”深深吸引，在与他第三次会面时被杀害了。与男网友见面三次后被杀。

案例二，一少女与男网友相处三个月怀孕两次，后男子消失。

**网络安全应急预案应当按照事件发生后的篇四**

1、网络管理员应在接到突发的计算机网络故障报告的第一时间，赶到现计算机或网络故障的第一现场，察看、询问网络故障现象和情况。

2、分析设备或系统的故障；判断故障属于物理性破坏、人为失误造成的安全事件、电脑病毒等恶意代码危害、检测软件引起的系统性瘫痪还是人为的恶意攻击等。

（3）、属于服务器瘫痪引起的；应立即还原服务器操作系统，并还原最近备份的服务器各数据库。如还原操作无效的，应第一时间安排电脑公司技术人员进行抢修，立即联系相关厂商和上级单位，请求技术支援，作好技术处理并通知服务器服务商。

（5）、当发现网络或服务器被非法入侵，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，各部门工作岗位工作人员应断开网络，网络管理员应向应急领导小组组长报告。 网络管理员接报告应核实情况，关闭服务器或系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

（6）、雷击事故；遇雷暴天气，各部门应请示网络管理员同意后关闭服务器，切断电源，暂停站内所有计算机网络工作，暂定车辆检测工作。如已受雷电影响，应将站内全部计算机断网，并逐一检查计算机、交换机、路由器、防火墙等的受损情况，有损坏的联系电脑公司技术人员进行抢修，等雷暴天气消除后再恢复检测。

4、网络管理员在处理网络事故期间，有必要时应立即联系电脑公司技术人员及时查清通信网络故障位置，隔离故障区域，并将事态及时报告计算机网络事故应急领导小组组长；同时及时组织相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

如短时间无法恢复车辆检测的，应在检测大厅和车辆候检区做好故障告示，及检测车辆车主的解释疏导工作；如要长时间排除故障的，应通过“象山报”或网络媒体等渠道进行公告，发布正式恢复检测时间。

5、应急处置结束后，事故情况严重的，应将故障分析报告，在调查、排除故障结束后一日内书面报告站安全生产领导小组。

6、数据保障；重要信息系统均建立备份系统，保证重要数据在受到破坏后可紧急恢复。

7、各岗位的计算机使用人员应增强应急处置能力。加强对突发计算机网络事故的技术准备，提高网络管理人员的防范意识及技能。网络管理员就每月对站内计算机网络开展一次全站范围内的计算机网络安全检查，消除网络安全隐患，提高站内计算机网络的安全防范能力。

**网络安全应急预案应当按照事件发生后的篇五**

1、网站、网页由办公室负责随时监控信息内容。

2、局各单位人员发现在网上出现非法信息时，立即向办公室反映情况；情况紧急的，应先及时采取删除等处理措施，再按程序报告。

3、办公室应在接到通知后10分钟内派出技术人员赶到现场，作好记录，清理非法信息，强化安全防范措施，并将网站网页重新投入使用。

4、妥善保存有关记录、日志或审计记录，将有关情况向安全领导小组汇报，并及时追查非法信息来源。

5、事态严重的，立即向信息安全领导小组组长报告，并根据指示向上级或公安部门报警。

（二）黑客攻击网站服务器或网站软件系统遭破坏性攻击时的应急预案

1、网页源代码及网站上重要的软件系统平时必须存有备份，网站数据库及与软件系统相对应的数据必须有多日的备份，并将它们保存于安全处。

2、当发现网页内容被篡改，或通过入侵监测系统发现有黑客正在进行攻击时，应立即向办公室报告。软件遭破坏性攻击（包括严重病毒）时要将系统停止运行。

3、公室负责人员应在10分钟内赶到现场，首先将被攻击（或病毒感染）的网站服务器等设备从网络中隔离出来，保护现场，并同时向信息安全领导小组通报情况。

4、办公室负责网站恢复与重建被攻击或被破坏的系统，恢复系统数据，并及时追查非法信息来源。主机受到病毒感染时，还应立即告知办公室帮助做好清查补救工作。

5、事态严重的，立即向信息安全领导小组组长报告，并根据指示向上级或公安部门报警。

**网络安全应急预案应当按照事件发生后的篇六**

学生自我防范意识较差，为增强学生对社会适应能力，预防诈骗案件发生经学校研究决定，特制订校园防诈骗安全应急预案如下：

一、指导思想

以上级安全有关文件精神和法规为依据，从维护学校及广大师生员工财产和人身安全，认真贯彻落实上级有关规定和要求，积极主动地做好有关的预防工作。

二、工作原则

坚持“早发现，早报告，早处理”的工作原则，提高快速反应和应急处理能力，切实做好我校防诈骗的各项预防工作。学校领导、各部门要以认真的态度、科学的手段和有效的措施抓好安全防范工作，切实维护学校和广大师生员工的财产安全。

三、常见的诈骗手段

（一）假冒身份进行骗钱

这是诈骗分子常用的诈骗伎俩，作案人常假冒学生或者学生的亲友等，以落难求援或帮助他人的名义行骗。

（二）拾物平分方式进行诈骗

这种诈骗手法比较老土，陈旧，但作案分子利用受害者的贪小便宜、财迷心窍的心理和特点实施行骗。

（三）以假手机掉包真手机的方式进行诈骗

这是社会上流行的一种骗术，该手段也渗透进了校园，使师生深受其害，诈骗分子经常利用学生思想单纯和贪图便宜等心理特点进行诈骗。

（四）假称学生发生车祸或疾病入院治疗需要费用的方式进行诈骗

近年来，针对外地学生家长进行的诈骗案件时有发生，给学生家庭造成巨大的经济损失。

（五）以次充好的方式进行诈骗

诈骗作案分子利用学生对鉴别商品质量能力差，“识货”经验少又图便宜的特点，上门推销各种产品行骗。

（六）以消灾解难的迷信方式进行诈骗

诈骗是一种高智商的犯罪，作案人善于察言观色，揣摩施骗对象的心理需要，他们常抓住受害人急功近利、焦虑等心理需求，以帮助消灾解难等为诱饵，设计骗局，达到其行骗目的。

（七）利用网络信息设局方式进行诈骗

随着网络的普及和高科技的发展，信息传播的速度和广度大大提高；由于网络信息的传播速度快，真假难以识别，犯罪分子利用这个特点，在网上设置骗局诱人上当。

（八）以手机短信形式进行金融诈骗

1、以短信“中大奖”的方式进行诈骗

这些是十分拙劣的诈骗手法，但作案人利用现代化的通讯工具大面积地“播种”，总会有人上当受骗。

2、以套取信用卡、银行卡资金方式进行诈骗

近期出现的诈骗分子利用手机短信实施金融诈骗的新方法，由于这类诈骗案手段迷惑性、欺骗性很强，已经有不少人上当受骗。

四、防诈骗措施

（一）组织措施

1、组织机构

组长：严胤红

成员：吴绍彪及各班主任

2、日常管理机构

保教办为我校防诈骗工作的主管部门，根据学校实际情况，适时启动我校各部门，有效应对诈骗事故的发生，维护校园稳定，保护广大师生员工的财产和人身安全。

（二）具体措施

1、加强防范意识，做好预防诈骗案件的宣传。主要以校园报、手抄报、校园之声为窗口进行宣传。

2、学校所有师生员工都要对学校的安全防诈骗高度重视，一旦发现可疑情况要积极主动及时报警，并迅速向值班老师、学校值班领导或校领导汇报，做到尽快处理和调查。学校电话：\_\_，报警电话：110。

**网络安全应急预案应当按照事件发生后的篇七**

为提高应对网络安全突发事件的能力，形成科学、有效、反应迅速的应急工作机制，确保计算机信息系统的实体安全、运行安全和数据安全，根据《网络安全法》《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互联网管理暂行规定》等有关法规、规定，特制定本预案。

一、组织领导

\_\_镇成立由分管领导任组长，办公室相关同志为成员的网络安全工作领导小组。领导小组负责预防和处理网络安全工作，确保网络安全稳定，具体负责网络安全的协调、调度、检查、考核等工作。

二、分类分级及适用范围

（一）分类分级

本预案所指的网络安全突发事件，是指网络系统突然遭受不可预知外力的破坏、毁损或故障，不良信息在网站乃至整个互联网的传播，发生对国家、社会、公众造成或者可能造成危害的紧急网络安全事件。

事件分类根据网络安全突发事件的发生过程、性质和特征，网络安全突发事件划分为网络安全突发事件和信息安全突发事件。

网络安全突发事件是指自然灾害、事故灾难和人为破坏引起的网络与信息系统的损坏；信息安全突发事件是指利用信息网络进行有目的或有组织的反动宣传、煽动和歪曲事理的不良活动或违法活动。

（1）自然灾害是指地震、台风、雷电、火灾、洪水等。

（2）事故灾难是指电力中断、网络损坏或者是软件、硬件设备故障等。

（3）人为破坏是指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖主义活动等事件。

事件分级

根据网络安全突发事件的可控性、严重程度和影响范围，将网络安全突发事件分为四级：i级（特别重大）、ii级（重大）、iii级（较大）、iv级（一般）。具体级别定义如果国家有关法律法规有明确规定的，按国家有关规定执行。

（1）i级（特别重大）：造成网络与信息系统发生大规模瘫痪，事态的发展超出区一级相关主管部门的控制能力，对国家安全、社会秩序、公共利益造成特别严重损害的突发事件。

（2）ii级（重大）：造成网站或其它上一级部门重要网络与信息系统瘫痪，对国家安全、社会秩序、公共利益造成严重损害的突发事件。

（3）iii级（较大）：造成网站网络与信息系统瘫痪，对国家安全、社会秩序、公共利益造成一定损害置的突发事件。

（4）iv级（一般）：造成网站网络重要网络与信息系统受到一定程度的损坏，但不危害国家安全、社会秩序和公共利益的突发事件。

（二）适用范围

本预案适用于发生与本预案定义的i－iv级网络与信息安全突发事件和可能导致i－iv级的网络与信息安全突发事件的应对处置工作。

三、工作原则

1、积极防御、综合防范。立足安全防护，加强预警，重点保护重要信息网络和关系社会稳定的重要信息系统；从预防、监控、应急处理、应急保障和打击不法行为等环节，在管理、技术、宣传等方面，采取多种措施，充分发挥各方面的作用，构筑网络与信息安全保障体系。

2、明确责任、分级负责。按照“谁主管、谁负责”的原则，加强网络安全管理，认真落实各项安全管理制度和措施。加强计算机信息网络安全的宣传和教育，进一步提高工作人员的信息安全意识。

3、落实措施、确保安全。要对网络设备、服务器等设施定期开展安全检查，对发现安全漏洞和隐患的进行及时整改；要实行网站的巡察制度，密切关注互联网信息动态，要按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

4、加强技术储备、规范应急处置措施与操作流程，树立常备不懈的观念，定期进行预案演练，确保应急预案切实可行。

5、事故上报

当发生网络安全突发事件时，应及时按规定向有关部门报告。初次报告最迟不得超过2小时，重大和特别重大的网络安全突发事件必须实行态势进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

四、事后处理

网络与信息安全突发事件经应急处置后，得到有效控制，事态下降到一定程度或基本得以解决，将各监测统计数据上报上级有关部门，由有关部门提出应急结束的建议，经批准后实施。

五、监督管理

1、加强对网络与信息安全等方面专业技能的培训，指定专人负责安全技术工作。

2、定期演练。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

在应急处置工作结束后，应立即组织有关人员组成事件调查组，查清事件发生的原因及财产损失情况，总结经验教训，写出调查评估报告，报应急领导小组，并根据问责制的有关规定，对有关责任人员作出处理。特别重大网站网络与信息安全突发公共事件的调查评估报告，报应急领导小组，必要时采取合理的形式向社会公众通报。

**网络安全应急预案应当按照事件发生后的篇八**

为确保发生网络安全问题时各项应急工作高效、有序地进行，最大限度地减少损失，根据互联网网络安全相关条例及教育局文件精神，结合我校校园网工作实际，特制定本预案。

（一）组织机构及职责

1、校园网络安全应急领导小组（下称领导小组）及职责

组长：校长

副组长：副校级领导

成员：各处室（委、会）、年级组负责人

主要职责及应急程序：

（1）加强领导，健全组织，强化工作职责，完善各项应急预案的制定和各项措施的落实；

（5）调动一切积极因素，全面保证和促进学校网络安全稳定地运行。

（6）网络安全事故发生后，视情况负责向上级汇报。

2、学校网站不良信息处理小组及职责

组长：分管安全的校长

副组长：分管宣传的校级领导、招宣处负责人

成员：各处室（委、会）、年级组负责人、网站管理员

主要职责及应急程序：网站管理员应定期巡检网络信息内容和安全情况，由于我校的对外宣传网站是建设在成都为人科技（8211），故学校网站一旦发现问题均由学校网站不良信息处理小组指定相关人员与公司沟通，尽快保全证据并处理事故，将影响降到最低。

（3）打印不良信息页面留存；

（4）立刻向领导小组组长汇报，领导小组视情况向上级主管部门汇报或向公安机关报案；

（6）从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

3、网络恶意攻击事故处理小组及职责

组长：分管安全的校长

副组长：分管现代教育技术的校级领导、现代教育技术中心负责人

成员：各处室（委、会）、年级组负责人、网络管理员

主要职责及应急程序：

网络管理员发现网络恶意攻击，立刻确定该攻击来自校内还是校外，受攻击的设备有哪些，影响范围有多大。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断校园网的服务器及公网的网络连接，以保护重要数据及信息，迅速向网络恶意攻击事故处理小组，小组判断是否须要启动应急预案。

启动应急预案后：

（2）保全好网络恶意攻击证据，分析重要数据安全及设备安全情况；

（5）从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

（二）网络安全事故应急方案

1、各小组在发现网络安全事故后，第一时间向领导小组汇报。

2、领导小组得悉网络安全紧急情况后立即赶赴现场，各种网络安全事故处理小组迅速集结待命。

4、相关小组在领导小组的统一组织指挥下，迅速按各小组职责和应急程序组织事故应急防护：

（4）事故源处理完成后，逐步恢复网络运行，监控事故源是否仍然存在；

（5）针对此次事故，进一步确定相关安全措施、总结经验，加强防范；

（6）从事故一发生到处理的整个过程，必须及时向领导小组组长汇报，听从安排，注意做好保密。

5、积极做好广大师生的思想宣传教育工作，迅速恢复正常秩序，全力维护校园网安全稳定。

6、事后迅速查清事件发生原因，查明责任人，并报领导小组根据责任情况进行处理。

（三）其他

在应急行动中，各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。

**网络安全应急预案应当按照事件发生后的篇九**

为提高学校处理突发信息网络事件的能力，形成科学、有效、反应迅速的应急工作机制，确保学校重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减少网络与信息安全突发公共事件的危害，特制定本预案。

1.预防为主。立足安全防护，加强预警，重点保护基础信息网络和重要信息系统，从预防、监控、应急处理、应急保障和打击犯罪等环节，采取多种措施，共同构筑网络与信息安全保障体系。

2.快速反应。在网络与信息安全突发公共事件发生时，按照快速反应机制，及时获取充分而准确的信息，迅速处置，最大程度地减少危害和影响。

3.以人为本。把保障学校、师生利益的合法权益的安全作为首要任务，及时采取措施，最大限度地避免各类有形、无形财产遭受损失。

4.分级负责。按照“谁主管谁负责、谁使用谁负责”以及“条块结合”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，加强协调与配合，形成合力，共同履行应急处置工作的管理职责。

南通理工学院网络安全领导小组。

组长：王宝根

副组长：李晏墅、陈勇

成员：王振兴、韩小祥、张鹏飞、王卫星、王佳

网络安全领导小组职责

1.负责编制、修订突发网络安全事件应急预案。

2.通过各种渠道和技术手段获取安全预警信息，周期性或即时性地向校园网用户发布安全预警；对异常流量来源进行监控，并妥善处理各种异常情况。

3.及时组织专业技术人员突发网络安全事件进行应急处置；负责调查和处置突发网络安全事件，及时上报并按照相关规定作好善后工作。

4.负责组建网络安全事件应急队伍并组织培训和演练。

学校信息化建设管理办公室和各学院、各部门信息系统管理员明确职责和管理范围，根据实际情况，建立多角度的网络安全防护体系，安排应急值班，确保到岗到人，联络畅通，处理及时准确。

1.建立安全、可靠、稳定运行的机房环境，防火、防盗、防雷电、防水、防静电、防尘；建立备份电源系统；加强所有人员防火、防盗等基本技能培训。

2.实行实时监视和监测，采用堡垒机账户认证等方式接入，避免非法接入和虚假路由信息。

3.重要系统采用可靠、稳定的硬件和冗余机制，落实数据备份机制，遵守安全操作规范；安装有效的防病毒软件，及时更新升级扫描引擎；及时更新操作系统补丁；加强对校园网内所有用户和信息系统管理员的安全技术培训。

4.安装具有入侵检测功能的硬件防火墙，监测恶意攻击、病毒等非法侵入，控制有害信息经过网络的传播，建立网关控制、内容过滤等控制手段。

5.信息系统上线前应由安全领导小组、系统供应商或网络安全评估单位对信息系统进行安全评估，评估合格后再予上线，评估不合格的应进行整改后再上线。

1.学校网站、网页被篡改或出现非法言论时的紧急处置措施

（1）网站、网页由具体负责人员随时密切监视信息内容。每天早、晚两次不少于一小时。

（2）发现学校网页出现非法信息时，负责人员应立即关闭学校网站，并向网络安全领导小组组长通报情况。

（3）具体负责的技术人员应在接到通知后30分钟内赶到现场，作好必要的记录，清理非法信息，强化安全防范措施，并将网站网页重新恢复启用。

（4）网站维护员应妥善保存有关记录及日志或审计记录。

（5）网站维护员应立即追查非法信息来源。

（6）工作人员会商后，将有关情况向安全领导小组领导汇报。

（7）安全领导组召开安全领导组会议，如认为情况严重，应及时向上级机关和公安部门报警。

2.黑客攻击时的紧急处置措施

（1）当系统管理人员通过入侵检测系统发现有黑客正在进行攻击时,应立即从网络中隔离被攻击的系统，并向网络安全员通报情况。

（2）网络管理员应在30分钟内赶到现场，收集被攻击系统的日志等资料，保护现场，同时向网络安全领导小组副组长汇报情况。

（3）网络管理员和网络安全员负责被破坏系统的恢复与重建工作。

（4）网络管理员协同有关部门共同追查非法攻击来源，评估攻击危害性。

（5）网络安全领导小组会商后，如认为情况严重，则立即向校保卫处或公安部门报警。

3.病毒安全紧急处置措施

（1）当发现计算机感染病毒后，应立即将该机从网络上隔离出来。

（2）对该设备的硬盘进行数据备份。

（3）启用反病毒软件对该机进行杀毒处理，同时用病毒检测软件对其他机器进行病毒扫描和清除。

（4）如发现反病毒软件无法处理该病毒，应对中毒系统进行评估后格式化该系统硬盘，重做系统后进行数据恢复。

4.数据库安全紧急处置措施

（1）数据库系统要至少准备两个以上数据库备份，备份的数据做到异地存储。

（2）一旦数据库崩溃，应立即向网络安全员报告，同时通知学校各部门暂缓上传上报数据。

（3）系统管理员应对主机系统进行维修，如遇无法解决的问题，应立即向小组领导报告，并向软硬件提供商请求支援。

（4）系统修复启动后，使用最近的数据库备份，按照要求将其恢复到主机系统中。

（5）如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。

（6）如果两个备份均无法恢复，应立即向有关厂商请求紧急支援。

5.广域网外部线路中断紧急处置措施

（1）广域网线路中断后，有关人员应立即调整出口策略，启动备用线路接续工作，同时向网络安全员报告。

（2）网络管理员接到报告后，应迅速判断故障节点，查明故障原因。

（3）如属我方管辖范围，由网络管理员立即予以恢复。如遇无法恢复情况，立即向有关厂商请求支援。

（4）如属运营商管辖范围，立即与运营商维护部门联系，请求修复。

（5）如果多条线路同时中断，网络管理员应在判断故障节点，查明故障原因后，尽快与其他相关领导和工作人员研究恢复措施，并立即向安全领导小组组长汇报。

（6）经安全领导小组同意后，应通告各下属单位相关原因，并暂缓使用网络服务。

6.局域网中断紧急处置措施

（1）局域网中断后，网络管理员应立即判断故障节点，查明故障原因，并向网络安全领导小组副组长汇报。

（2）如属线路故障，应第一时间恢复链路通信，然后按照布线标准重新安装线路。

（3）如属路由器、交换机等网络设备故障，应立即与设备提供商联系更换设备，并调试畅通。

（4）如属路由器、交换机配置文件破坏，应迅速按照根据备份配置重新配置，并调试畅通。如遇无法解决的技术问题，立即向有关厂商请求支援。

（5）如有必要，应向安全领导组组长汇报。

7.设备安全紧急处置措施

（1）小型机、服务器等关键设备损坏后，有关人员应立即向网络管理员和网络安全员汇报。

（2）网络管理员和网络安全员应立即查明原因。

（3）如果能够自行恢复，应立即用备件替换受损部件。

（4）如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。

（5）如果设备一时不能修复，应向安全领导小组领导汇报，并告知学校各部门、学院，暂停相关服务。

8.人员疏散与机房灭火预案

（1）一旦机房发生火灾，应遵照下列原则：首先保人员安全；其次保关键设备、数据安全；三是保一般设备安全。

（2）人员疏散的程序是：机房值班人员立即按响火警警报，并通过119电话向公安消防请求支援，所有不参与灭火的人员按照预先确定的线路，迅速从机房中撤出。

（3）人员灭火的程序是：首先切断所有电源，启动自动气体灭火系统，从指定位置取出泡沫灭火器进行灭火。

9.供电中断后的应急措施

（1）供电中断后，机房值班人员应立即查看是否切换到备用ups电源，并关闭不重要的服务器和网络设备，以减少机房用电量，保证ups给主要设备和服务器供电。

（2）机房值班人员应立即查明原因，并向值班领导汇报，并通过学校主要通知渠道发布相关公告通知校园网用户。

（3）如因学校内部线路故障，应及时联系后勤值班电工迅速恢复。

（4）如果是市电供应的原因，应立即与后勤部门联系,了解具体情况。

（5）如果后勤部门预先告知需长时间停电，应做如下安排：

预计停电2小时以内，由ups供电。

预计停电2小时以上，4小时以内，关闭非关键设备。

预计停电超过4小时，关闭所有设备，待供电恢复后再开机。

10.发生不可抗力事件的紧急处置措施

（1）信息办平时应储备一些关键设备的备件，在发生意外时能及时更换。

（2）一旦发生故障，导致设备损坏，应立即向组长汇报。

（3）组长接到汇报后，应在30分钟内安排相关负责人赶到现场指挥处置。

（4）相关负责人到达现场后，经检测无法自行恢复的情况下，应在立即联系技术人员和供应商售后服务部门，寻找安全可靠的地点，重新构建新的系统和网络，并将相关数据予以恢复。

11.关键人员不在岗的紧急处置措施

（1）对于关键岗位平时应做好人员储备，确保一项工作有两人能操作。

（2）一旦发生关键人员不在岗的情况，首先应向值班领导汇报情况。

（3）经值班领导批准后，由备用人员上岗操作。

应急处置工作结束后，分管领导组织有关人员和技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，根据应急处置中暴露出的管理、协调和技术问题，改进和完善预案，实施针对性演练，总结经验教训，整改存在的隐患，组织恢复正常工作秩序。

（一）通信保障

信息办值班人员应在值班期间保持24小时通讯畅通。

（二）装备保障

信息办负责建立并保持电力、空调、机房等网络安全运行基本环境，并预留一定数量的信息网络硬件和软件设备，指定专人保管和维护。

（三）数据保障

重要信息系统均建立备份系统，保证重要数据在受到破坏后可紧急恢复。

（四）队伍保障

建立符合要求的网络与信息安全保障技术支持力量，对学校的网络与信息安全保障工作人员提供技术支持和培训服务。

（一）宣传教育和培训

将信息网络突发事件的应急管理、工作流程等列为培训内容，增强应急处置能力。加强对信息网络突发事件的技术准备培训，提高技术人员的防范意识及技能。信息办每年至少开展一次部门范围内的信息网络安全教育，提高信息安全防范意识和能力。

（二）预案演练

网络安全领导小组每年至少安排一次演练，建立应急预案定期演练制度。通过演练，发现和解决应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

（三）责任与奖惩

网络安全领导小组不定期组织对各项制度、计划、方案、人员及物资等进行检查，对在网络安全事件应急处置中做出突出贡献的集体和个人，提出表彰奖励建议；对玩忽职守，造成不良影响或严重后果的，按学校相关规定提出处理意见，追究其责任。

（一）预案更新

结合信息网络快速发展和经济社会发展状况，配合相关法律法规的制定、修改和完善，适时修订本预案。

（二）制定和解释

本预案由信息化建设管理办公室制定并解释。

**网络安全应急预案应当按照事件发生后的篇十**

深入宣传贯彻在全国网络安全和信息化工作会议上的重要讲话精神，宣传国家网络安全工作取得的重大成就，深入宣传贯彻《中华人民共和国网络安全法》等相关法律法规，围绕宣传主题和宣传内容、编制发放宣传资料。通过校园广播、微信公众号、主题班会等多种形式参与网络安全宣传教育活动，普及网络安全知识，提升广大师生网络安全意识和防护技能。

二、活动时间

9月17日——9月23日

三、宣传主题

网络安全伴我行

四、活动内容

(一)开展网络安全“校园日”宣传活动

2.将网络安全知识纳入中小学安全知识网络答题活动中。

(二)举办“网络安全大讲堂”知识专题讲座

2.组织广大师生收看网络安全知识专题视频讲座。

(三)组织网络安全知识专题竞赛

1.各校组织教师认真学习《公务人员网络安全基础知识读本》，并组织安全知识竞赛;

2.举办中小学生网络安全知识竞赛;

3.组织全区中小学生参加20\_年全省学生安全知识网络答题活动。

(四)积极开展“小安全卫士”宣传活动

按照团市委的指导，组织青少年积极参加网络安全科普教育活动，利用微博、微信等形式发起文明上网的倡议活动。

五、工作要求

1.各学校要把网络安全宣传作为重大的政治任务来抓，切实加强领导，明确目标任务，落实工作责任，强化工作措施，狠抓工作落实，扎实推进网络安全宣传周活动平安有序。

2.活动期间，各校要善于收集活动资料，总结经验，有条件的学校可以通过制作视频宣传片的形式加大宣传教育。

3.各学校于9月25日之前，将活动情况报区教育局\_\_邮箱。

**网络安全应急预案应当按照事件发生后的篇十一**

为更好地加强校园网络系统、学校网站、师生个人主页的管理，认真落实网络和信息安全保障制度，防范和处理校园网络管理重大突发事件和敏感事件，确保网络提供稳定、安全的信息服务，特制定本方案。

一、强化组织机构，加强管理控制

学校成立以校长周卫庆为组长的网络安全管理领导小组，组员由分管校长林亚琴，网络管理员夏雪峰、陈佩君、陈建伟，安全保卫负责人吴小芳，各块主要负责人王红燕、许露艳、杨婷婷组成。网管员夏雪峰兼任突发事件处理联系人。通过成立组织机构，强化意识，明确职责，加强控制，保障网络安全管理落到实处。

二、加强业务培训，提高防范水平

积极参加上级举办的网管员培训，提高网管员的网络管理水平。同时积极开展相关培训，以网管员为主要力量，定期对教师和学生开展互联网安全和文明上网的宣传教育，提高全体师生上网的法制意识、责任意识、政治意识、自律意识和安全意识，形成广大师生共同抵制网上有害信息的良好氛围，保证校园网络系统安全运行，更好地为教育科学服务。

加强网络安全建设，保证软件防火墙和防病毒软件的及时有效的更新，提高网络系统防御攻击的能力。

三、执行审查制度，保证新闻真实健康

对校园新闻，采取校长审批制。学校通讯报道工作落实专人负责，报道内容在校园网发布或向上级有关部门发送时，由校长先做审批，经同意后方能发布或传送。未经校长同意而发布的有损于学校和社会形象的言论，发布人要负法律责任，并按有关规定追究责任。同时在新闻发布系统上严格设置权限管理，让通过校长室认证的人员才可以在网络上发布合法的消息。

四、加强安全管理，快速有效应急

网管员坚持做到每天至少一次的安全检测，及时了解网络运行情况，以保障校园网的安全性、稳定性和可靠性。对非法站点作好过滤，并定期备份重要文件，网络备份和光盘刻录备份相结合，日志必须保存60天。

一旦发现校园网上出现违反校园网络安全管理制度的行为，立即停止校园网络的使用。对有害的信息则立即删除。校网络安全管理领导小组立即组织有关人员进行查处，对违纪人员依照有关法律、法规和校纪校规，作出严肃处理。

**网络安全应急预案应当按照事件发生后的篇十二**

为确保发生网络安全问题时各项应急工作高效、有序地进行，最大限度地减少损失，根据互联网网络安全相关条例及上级相关部门文件精神，结合我校校园网工作实际，特制定本预案。

二、本预案的适用范围

适用于在本校区电脑发生不良信息、网上恶意攻击等事故.

三、应急指挥领导小组

组长：郝江玉

副组长：郭振华、甄蕾

成员：杨雨霏、周游莉、刘莹、张霞及各班班主任

四、积极预防网络和信息事故发生

（1）加强领导，健全组织，强化工作职责，完善各项应急预案的制定和各项措施的落实。

（2）充分利用各种渠道进行网络安全知识的.宣传教育，组织、指导全校网络安全常识的普及教育，广泛开展网络安全和有关技能训练，不断提高广大师幼的防范意识和基本技能。

（3）认真搞好各项物资保障，严格按照预案要求积极配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资，强化管理，使之保持良好工作状态。

（4）采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。

（5）调动一切积极因素，全面保证和促进学校网络安全稳定地运行。

五、各级处理预案

1、网站不良信息事故处理预案

（1）一旦发现学校网站上出现不良信息（或者被黑客攻击修改了网页），立刻关闭网站。

（2）备份不良信息出现的目录、备份不良信息出现时间前后一个星期内的http连接日志、备份防火墙中不良信息出现时间前后一个星期内的网络连接日志。

（3）打印不良信息页面留存。

（4）完全隔离出现不良信息的目录，使其不能再被访问。

（5）删除不良信息，并清查整个网站所有内容，确保没有任何不良信息，重新开通网站服务，并测试网站运行。

（6）修改该目录名，对该目录进行安全性检测，升级安全级别，升级程序，去除不安全隐患，关闭不安全栏目，重新开放该目录的网络连接，并进行测试，正常后，重新修改该目录的上级链接。

（7）全面查对http日志，防火墙网络连接日志，确定该不良信息的源ip地址，如果来自校内，则立刻全面升级此次事件为最高紧急事件，立刻向领导小组组长汇报，视情节严重程度领导小组可决定是否向公安机关报案。

（8）从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

2、网络恶意攻击事故处理预案

（2）如果攻击来自校外，立刻从防火墙中查出对方ip地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

为确保发生网络安全问题时各项应急工作高效、有序地进行，最大限度地减少损失，根据互联网网络安全相关条例及上级相关部门文件精神，结合我校校园网工作实际，特制定本预案。

六、日常管理

1、领导小组依法发布有关消息和警报，全面组织各项网络安全防御、处理工作。各有关组员随时准备执行应急任务。

2、网络管理员对校园内外所属网络硬件软件设备及接入网络的计算机设备定期进行全面检查，封堵、更新有安全隐患的设备及网络环境。

3、加强对校园网内计算机设备的管理，加强对学校网络的使用者（学生和教师）的网络安全教育。加强对重要网络设备的软件防护以及硬件防护，确保正常的运行软件硬件环境。

4、加强各类值班值勤，保持通讯畅通，及时掌握学校情况，全力维护正常教学、工作和生活秩序。

5、按预案落实各项物资准备。

七、网络安全事故发生后有关行动

1、领导小组得悉消防紧急情况后立即赶赴本级指挥所，各种网络安全事故处理小组迅速集结待命。

2、应急小组成员听从组织指挥，迅速组织本级抢险防护。

（1）确保web网站信息安全为首要任务,学校公网连接。迅速发出紧急警报，所有相关成员集中进行事故分析，确定处理方案。

（2）确保校内其它接入设备的信息安全：经过分析，可以迅速关闭、切断其他接入设备的所有网络连接，防止滋生其他接入设备的安全事故。

（3）分析网络，确定事故源：使用各种网络管理工具，迅速确定事故源，按相关程序进行处理。

（4）事故源处理完成后，逐步恢复网络运行，监控事故源是否仍然存在。

（5）针对此次事故，进一步确定相关安全措施、总结经验，加强防范。

（6）从事故一发生到处理的整个过程，必须及时向领导小组组长以及教务处以及校长汇报，听从安排，注意做好保密。

3、积极做好广大师生的思想宣传教育工作，迅速恢复正常秩序，全力维护校园网安全稳定。

4、迅速了解和掌握事故情况，及时汇总上报。

5、事后迅速查清事件发生原因，查明责任人，并报领导小组根据责任情况进行处理。

八、其他

1、在应急行动中，学校各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。

2、各部门应根据本预案，结合本部门实际情况，认真制定本部门的应急预案，并切实落实各项组织措施。

本文档由028GTXX.CN范文网提供，海量范文请访问 https://www.028gtxx.cn