# 最新网络安全应急预案应当按照事件发生后的 网络安全应急预案(汇总16篇)

来源：网络 作者：琴心剑胆 更新时间：2025-07-30

*在日常的学习、工作、生活中，肯定对各类范文都很熟悉吧。范文怎么写才能发挥它最大的作用呢？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以建设幸福为出发点，加强网络安全监管工作...*

在日常的学习、工作、生活中，肯定对各类范文都很熟悉吧。范文怎么写才能发挥它最大的作用呢？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**

以建设幸福为出发点，加强网络安全监管工作，坚持积极防御、综合防范的方针，全面提高信息安全防护能力。重点保障基础信息网络和重要信息系统安全，创建安全的网络环境，保障信息化健康发展，维护公众利益，促进社会和谐稳定。

二、工作目标。

通过开展网络安全监管专项行动，进一步提高基础信息网络和重要信息系统安全防护水平，深入推进信息安全保障体系建设，健全统筹协调、分工合作的管理体制，强化信息安全监测、预警与应急处置能力，深化各类政务及公共服务重要信息系统的信息安全风险评估与等级保护工作，打造可信、可控、可用的信息安全防护基础设施和网络行为文明、信息系统安全的互联网应用环境。

三、组织领导。

成立我局网络安全监管专项整治工作领导小组，由办公室、执法大队、市场管理科、广电科等组成。

四、工作职责。

负责全县互联网文化活动的日常管理工作，对从事互联网文化活动的单位进行初审或备案，对互联网文化活动违反国家有关法规的行为实施处罚;依法负责对互联网上网服务营业场所的审核及管理;督促县广电总台做好互联网等信息网络传输视听节目(包括影视类音像制品)的管理。

五、整治任务。

按照国家和省、市、县要求，认真做好重要时期信息安全保障工作。确保基础信息网络传输安全，保障重要信息系统安全、平稳运行，强化对互联网及通信网络信息安全内容的监管，严格防范非法有害信息在网络空间的散播。

六、总体安排。

第一阶段：调查摸底，健全机制阶段(5月)。

第二阶段：评估自评估、自测评，综合整治阶段(6月至9月)。

第三阶段：检查验收，巩固提高阶段(10月)。

七、工作要求。

1、提高认识，加强领导。要充分认识信息安全保障工作的重要性和紧迫性，落实部门责任，各司其职，常抓不懈。做好本系统、本行业内各类信息网络和重要信息系统的安全管理工作。

2、明确职责，加强配合。要在整治工作领导小组统一领导协调下，各司其职，分头齐进，相互配合，迅速开展整治工作。同时，定期召开会议，通报情况，研究问题，部署任务，协调行动，确保整治工作有序开展。

3、突出重点，狠抓落实。要将整治工作列入重要工作内容，结合实际，认真制定针对性强、可操作性好的整治措施。对重要信息系统落实责任到人，严控重大信息安全事件的发生，不放过任何小问题，确保整治工作取得实效。

4、完善机制，长效监管。网络安全管理和互联网安全监管是一项长期、复杂的工作，要坚持常抓不懈，及时研究新情况、解决新问题，不断完善长效管理机制，确保网络信息安全，促进社会和谐健康发展。

**网络安全应急预案应当按照事件发生后的篇二**

随着internet的普及与发展，网络犯罪已经成为当今社会犯罪形态的一种重要形式，针对校园网信息网络安全事件的主要形式为网络攻击与系统侵入、境内外犯罪分子撰写或转贴的反动言论及淫秽图像为代表的非法有害信息。一旦在校园网上出现网络安全事件或有害信息，将会严重损害学校声誉，甚至对社会稳定产生不利影响，将影响学校的发展。为及时处置校园网信息网络安全事件，保障校园网作用的正常发挥，特制定本预案。

组长：石东华

副组长：李双华、陈双、邱仁建、贾先慧

1.计算机专用教室、多媒体专用教室及其它配有计算机设备的教室、办公室。

2.其它计算机辅助设备包括打印机、电视机等。

3.广播播音系统。

出现下列情况应启动应急预案：

1.计算机网络出现病毒且传播迅速，对学校网络安全造成潜在危险的情况。

2.计算机及相关设备发生被盗或人为恶意损坏。

3.发现利用网络传播不良信息现象。

信息网络安全事件定义：

a.校园网内网站主页被恶意纂改、交互式栏目里发表反政府、分裂国家和色情内容的信息及损害国家、学校声誉的谣言。

b.校园网内网络被非法入侵，应用服务器上的`数据被非法拷贝、修改、删除。

c.在网站上发布的内容违反国家的法律法规、侵犯知识版权，已经造成严重后果。

4.出现黑客攻击等其它致使学校网络不能正常运转或数据丢失的情况。

1.网络设备使用者或管理者发现上述所列情况之一时，应立即报告网络领导小组负责人（组长或副组长），同时控制好现场。

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控制或维修恢复，直至问题解决。

（一）网络出现病毒且传播迅速，对学校网络安全造成潜在危险的处理办法。

1.发生上述情况时，使用者或管理者应立即告知学校，同时断开网线。

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

（二）计算机及相关设备发生被盗或人为恶意损坏处理办法

1.发生上述情况时，使用者或管理者应立即告知学校，并保护好现场。

2.学校领导小组接报后，立即报告学校安全领导小组，同时组织相关人员配合有关部门进行调查，待取证等相关工作结束并获得允许后，要及时恢复设备使用。并妥善作好善后工作。

（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负责人。

2.学校接报后，一方面向上级报告，请示处理意见。另一方面切断校园网络，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，由学校办公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。

（四）出现黑客攻击等其它致使学校网络不能正常运转或数据丢失的情况处理办法。

1.发生上述情况时，使用者或管理者应立即告知学校，同时断开网线

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

**网络安全应急预案应当按照事件发生后的篇三**

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四**

建立健全公共互联网网络安全突发事件应急组织体系和工作机制，提高公共互联网网络安全突发事件综合应对能力，确保及时有效地控制、减轻和消除公共互联网网络安全突发事件造成的社会危害和损失，保证公共互联网持续稳定运行和数据安全，维护国家网络空间安全，保障经济运行和社会秩序。

1.2编制依据

《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《中华人民共和国电信条例》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》等相关规定。

1.3适用范围

本预案适用于面向社会提供服务的基础电信企业、域名注册管理和服务机构(以下简称域名机构)、互联网企业(含工业互联网平台企业)发生网络安全突发事件的应对工作。

本预案所称网络安全突发事件，是指突然发生的，由网络攻击、网络入侵、恶意程序等导致的，造成或可能造成严重社会危害或影响，需要电信主管部门组织采取应急处置措施予以应对的网络中断(拥塞)、系统瘫痪(异常)、数据泄露(丢失)、病毒传播等事件。

本预案所称电信主管部门包括工业和信息化部及各省(自治区、直辖市)通信管理局。

工业和信息化部对国家重大活动期间网络安全突发事件应对工作另有规定的，从其规定。

1.4工作原则

公共互联网网络安全突发事件应急工作坚持统一领导、分级负责;坚持统一指挥、密切协同、快速反应、科学处置;坚持预防为主，预防与应急相结合;落实基础电信企业、域名机构、互联网服务提供者的主体责任;充分发挥网络安全专业机构、网络安全企业和专家学者等各方面力量的作用。

2.组织体系

2.1领导机构与职责

在中央网信办统筹协调下，工业和信息化部网络安全和信息化领导小组(以下简称部领导小组)统一领导公共互联网网络安全突发事件应急管理工作，负责特别重大公共互联网网络安全突发事件的统一指挥和协调。

2.2办事机构与职责

在中央网信办下设的国家网络安全应急办公室统筹协调下，在部领导小组统一领导下，工业和信息化部网络安全应急办公室(以下简称部应急办)负责公共互联网网络安全应急管理事务性工作;及时向部领导小组报告突发事件情况，提出特别重大网络安全突发事件应对措施建议;负责重大网络安全突发事件的统一指挥和协调;根据需要协调较大、一般网络安全突发事件应对工作。

部应急办具体工作由工业和信息化部网络安全管理局承担，有关单位明确负责人和联络员参与部应急办工作。

2.3其他相关单位职责

各省(自治区、直辖市)通信管理局负责组织、指挥、协调本行政区域相关单位开展公共互联网网络安全突发事件的预防、监测、报告和应急处置工作。

基础电信企业、域名机构、互联网企业负责本单位网络安全突发事件预防、监测、报告和应急处置工作，为其他单位的网络安全突发事件应对提供技术支持。

国家计算机网络应急技术处理协调中心、中国信息通信研究院、中国软件评测中心、国家工业信息安全发展研究中心(以下统称网络安全专业机构)负责监测、报告公共互联网网络安全突发事件和预警信息，为应急工作提供决策支持和技术支撑。

鼓励网络安全企业支撑参与公共互联网网络安全突发事件应对工作。

3.事件分级

根据社会影响范围和危害程度，公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。

3.1特别重大事件

符合下列情形之一的，为特别重大网络安全事件：

(1)全国范围大量互联网用户无法正常上网;

(2).cn国家顶级域名系统解析效率大幅下降;

(3)1亿以上互联网用户信息泄露;

(4)网络病毒在全国范围大面积爆发;

(5)其他造成或可能造成特别重大危害或影响的网络安全事件。

3.2重大事件

符合下列情形之一的，为重大网络安全事件：

(1)多个省大量互联网用户无法正常上网;

(2)在全国范围有影响力的网站或平台访问出现严重异常;

(3)大型域名解析系统访问出现严重异常;

(4)1千万以上互联网用户信息泄露;

(5)网络病毒在多个省范围内大面积爆发;

(6)其他造成或可能造成重大危害或影响的网络安全事件。

3.3较大事件

符合下列情形之一的，为较大网络安全事件：

(1)1个省内大量互联网用户无法正常上网;

(2)在省内有影响力的网站或平台访问出现严重异常;

(3)1百万以上互联网用户信息泄露;

(4)网络病毒在1个省范围内大面积爆发;

(5)其他造成或可能造成较大危害或影响的网络安全事件。

3.4一般事件

符合下列情形之一的，为一般网络安全事件：

(1)1个地市大量互联网用户无法正常上网;

(2)10万以上互联网用户信息泄露;

(3)其他造成或可能造成一般危害或影响的网络安全事件。

4.监测预警

4.1事件监测

基础电信企业、域名机构、互联网企业应当对本单位网络和系统的运行状况进行密切监测，一旦发生本预案规定的\'网络安全突发事件，应当立即通过电话等方式向部应急办和相关省(自治区、直辖市)通信管理局报告，不得迟报、谎报、瞒报、漏报。

网络安全专业机构、网络安全企业应当通过多种途径监测、收集已经发生的公共互联网网络安全突发事件信息，并及时向部应急办和相关省(自治区、直辖市)通信管理局报告。

报告突发事件信息时，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议。

4.2预警监测

基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业应当通过多种途径监测、收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生突发事件的可能性及其可能造成的影响进行分析评估;认为可能发生特别重大或重大突发事件的，应当立即向部应急办报告;认为可能发生较大或一般突发事件的，应当立即向相关省(自治区、直辖市)通信管理局报告。

4.3预警分级

建立公共互联网网络突发事件预警制度，按照紧急程度、发展态势和可能造成的危害程度，公共互联网网络突发事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全突发事件。

4.4预警发布

部应急办和各省(自治区、直辖市)通信管理局应当及时汇总分析突发事件隐患和预警信息，必要时组织相关单位、专业技术人员、专家学者进行会商研判。

认为需要发布红色预警的，由部应急办报国家网络安全应急办公室统一发布(或转发国家网络安全应急办公室发布的红色预警)，并报部领导小组;认为需要发布橙色预警的，由部应急办统一发布，并报国家网络安全应急办公室和部领导小组;认为需要发布黄色、蓝色预警的，相关省(自治区、直辖市)通信管理局可在本行政区域内发布，并报部应急办，同时通报地方相关部门。对达不到预警级别但又需要发布警示信息的，部应急办和各省(自治区、直辖市)通信管理局可以发布风险提示信息。

发布预警信息时，应当包括预警级别、起始时间、可能的影响范围和造成的危害、应采取的防范措施、时限要求和发布机关等，并公布咨询电话。面向社会发布预警信息可通过网站、短信、微信等多种形式。

4.5预警响应

4.5.1黄色、蓝色预警响应

发布黄色、蓝色预警后，相关省(自治区、直辖市)通信管理局应当针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

(3)及时宣传避免、减轻危害的措施，公布咨询电话，并对相关信息的报道工作进行正确引导。

4.5.2红色、橙色预警响应

发布红色、橙色预警后，部应急办除采取黄色、蓝色预警响应措施外，还应当针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

(1)要求各相关单位实行24小时值班，相关人员保持通信联络畅通;

(3)组织有关单位加强对重要网络、系统的网络安全防护;

(4)要求相关网络安全专业机构、网络安全企业进入待命状态，针对预警信息研究制定应对方案，检查应急设备、软件工具等，确保处于良好状态。

4.6预警解除

部应急办和省(自治区、直辖市)通信管理局发布预警后，应当根据事态发展，适时调整预警级别并按照权限重新发布;经研判不可能发生突发事件或风险已经解除的，应当及时宣布解除预警，并解除已经采取的有关措施。相关省(自治区、直辖市)通信管理局解除黄色、蓝色预警后，应及时向部应急办报告。

5.应急处置

5.1响应分级

公共互联网网络安全突发事件应急响应分为四级：i级、ii级、iii级、iv级，分别对应已经发生的特别重大、重大、较大、一般事件的应急响应。

5.2先行处置

公共互联网网络安全突发事件发生后，事发单位在按照本预案规定立即向电信主管部门报告的同时，应当立即启动本单位应急预案，组织本单位应急队伍和工作人员采取应急处置措施，尽最大努力恢复网络和系统运行，尽可能减少对用户和社会的影响，同时注意保存网络攻击、网络入侵或网络病毒的证据。

5.3启动响应

i级响应根据国家有关决定或经部领导小组批准后启动，由部领导小组统一指挥、协调。

ii级响应由部应急办决定启动，由部应急办统一指挥、协调。

iii级、iv级响应由相关省(自治区、直辖市)通信管理局决定启动，并负责指挥、协调。

启动i级、ii级响应后，部应急办立即将突发事件情况向国家网络安全应急办公室等报告;部应急办和相关单位进入应急状态，实行24小时值班，相关人员保持联络畅通，相关单位派员参加部应急办工作;视情在部应急办设立应急恢复、攻击溯源、影响评估、信息发布、跨部门协调、国际协调等工作组。

启动iii级、iv级响应后，相关省(自治区、直辖市)通信管理局应及时将相关情况报部应急办。

5.4事态跟踪

启动i级、ii级响应后，事发单位和网络安全专业机构、网络安全企业应当持续加强监测，跟踪事态发展，检查影响范围，密切关注舆情，及时将事态发展变化、处置进展情况、相关舆情报部应急办。省(自治区、直辖市)通信管理局立即全面了解本行政区域受影响情况，并及时报部应急办。基础电信企业、域名机构、互联网企业立即了解自身网络和系统受影响情况，并及时报部应急办。

启动iii级、iv级响应后，相关省(自治区、直辖市)通信管理局组织相关单位加强事态跟踪研判。

5.5决策部署

启动i级、ii级响应后，部领导小组或部应急办紧急召开会议，听取各相关方面情况汇报，研究紧急应对措施，对应急处置工作进行决策部署。

针对突发事件的类型、特点和原因，要求相关单位采取以下措施：带宽紧急扩容、控制攻击源、过滤攻击流量、修补漏洞、查杀病毒、关闭端口、启用备份数据、暂时关闭相关系统等;对大规模用户信息泄露事件，要求事发单位及时告知受影响的用户，并告知用户减轻危害的措施;防止发生次生、衍生事件的必要措施;其他可以控制和减轻危害的措施。

做好信息报送。及时向国家网络安全应急办公室等报告突发事件处置进展情况;视情况由部应急办向相关职能部门、相关行业主管部门通报突发事件有关情况，必要时向相关部门请求提供支援。视情况向外国政府部门通报有关情况并请求协助。

注重信息发布。及时向社会公众通告突发事件情况，宣传避免或减轻危害的措施，公布咨询电话，引导社会舆论。未经部应急办同意，各相关单位不得擅自向社会发布突发事件相关信息。

启动iii级、iv级响应后，相关省(自治区、直辖市)通信管理局组织相关单位开展处置工作。处置中需要其他区域提供配合和支持的，接受请求的省(自治区、直辖市)通信管理局应当在权限范围内积极配合并提供必要的支持;必要时可报请部应急办予以协调。

5.6结束响应

突发事件的影响和危害得到控制或消除后，i级响应根据国家有关决定或经部领导小组批准后结束;ii级响应由部应急办决定结束，并报部领导小组;iii级、iv级响应由相关省(自治区、直辖市)通信管理局决定结束，并报部应急办。

6.事后总结

6.1调查评估

公共互联网网络安全突发事件应急响应结束后，事发单位要及时调查突发事件的起因(包括直接原因和间接原因)、经过、责任，评估突发事件造成的影响和损失，总结突发事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急响应结束后10个工作日内形成总结报告，报电信主管部门。电信主管部门汇总并研究后，在应急响应结束后20个工作日内形成报告，按程序上报。

6.2奖惩问责

工业和信息化部对网络安全突发事件应对工作中作出突出贡献的先进集体和个人给予表彰或奖励。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的单位或个人，由电信主管部门给予约谈、通报或依法、依规给予问责或处分。基础电信企业有关情况纳入企业年度网络与信息安全责任考核。

7.预防与应急准备

7.1预防保护

基础电信企业、域名机构、互联网企业应当根据有关法律法规和国家、行业标准的规定，建立健全网络安全管理制度，采取网络安全防护技术措施，建设网络安全技术手段，定期进行网络安全检查和风险评估，及时消除隐患和风险。电信主管部门依法开展网络安全监督检查，指导督促相关单位消除安全隐患。

7.2应急演练

电信主管部门应当组织开展公共互联网网络安全突发事件应急演练，提高相关单位网络安全突发事件应对能力。基础电信企业、大型互联网企业、域名机构要积极参与电信主管部门组织的应急演练，并应每年组织开展一次本单位网络安全应急演练，应急演练情况要向电信主管部门报告。

7.3宣传培训

电信主管部门、网络安全专业机构组织开展网络安全应急相关法律法规、应急预案和基本知识的宣传教育和培训，提高相关企业和社会公众的网络安全意识和防护、应急能力。基础电信企业、域名机构、互联网企业要面向本单位员工加强网络安全应急宣传教育和培训。鼓励开展各种形式的网络安全竞赛。

7.4手段建设

工业和信息化部规划建设统一的公共互联网网络安全应急指挥平台，汇集、存储、分析有关突发事件的信息，开展应急指挥调度。指导基础电信企业、大型互联网企业、域名机构和网络安全专业机构等单位规划建设本单位突发事件信息系统，并与工业和信息化部应急指挥平台实现互联互通。

7.5 工具配备

基础电信企业、域名机构、互联网企业和网络安全专业机构应加强对木马查杀、漏洞检测、网络扫描、渗透测试等网络安全应急装备、工具的储备，及时调整、升级软件硬件工具。鼓励研制开发相关技术装备和工具。

8.保障措施

8.1落实责任

各省(自治区、直辖市)通信管理局、基础电信企业、域名机构、互联网企业、网络安全专业机构要落实网络安全应急工作责任制，把责任落实到单位领导、具体部门、具体岗位和个人，建立健全本单位网络安全应急工作体制机制。

8.2经费保障

工业和信息化部为部应急办、各省(自治区、直辖市)通信管理局、网络安全专业机构开展公共互联网网络安全突发事件应对工作提供必要的经费保障。基础电信企业、域名机构、大型互联网企业应当安排专项资金，支持本单位网络安全应急队伍建设、手段建设、应急演练、应急培训等工作开展。

8.3队伍建设

网络安全专业机构要加强网络安全应急技术支撑队伍建设，不断提升网络安全突发事件预防保护、监测预警、应急处置、攻击溯源等能力。基础电信企业、域名机构、大型互联网企业要建立专门的网络安全应急队伍，提升本单位网络安全应急能力。支持网络安全企业提升应急支撑能力，促进网络安全应急产业发展。

8.4社会力量

建立工业和信息化部网络安全应急专家组，充分发挥专家在应急处置工作中的作用。从网络安全专业机构、相关企业、科研院所、高等学校中选拔网络安全技术人才，形成网络安全技术人才库。

8.5国际合作

工业和信息化部根据职责建立国际合作渠道，签订国际合作协议，必要时通过国际合作应对公共互联网网络安全突发事件。鼓励网络安全专业机构、基础电信企业、域名机构、互联网企业、网络安全企业开展网络安全国际交流与合作。

9.附则

9.1预案管理

本预案原则上每年评估一次，根据实际情况由工业和信息化部适时进行修订。

各省(自治区、直辖市)通信管理局要根据本预案，结合实际制定或修订本行政区域公共互联网网络安全突发事件应急预案，并报工业和信息化部备案。

基础电信企业、域名机构、互联网企业要制定本单位公共互联网网络安全突发事件应急预案。基础电信企业、域名机构、大型互联网企业的应急预案要向电信主管部门备案。

9.2预案解释

本预案由工业和信息化部网络安全管理局负责解释。

9.3预案实施时间

**网络安全应急预案应当按照事件发生后的篇五**

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六**

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七**

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。

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。

（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。

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徐汇区教育信息中心工作要求，结合我校校园网工作实际，特制定本预案。

1、领导小组及职责。

组长：马卫东。

副组长：杨海涛。

成员：王春凤、江静虹、俞莹、范显涛。

主要职责：

(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，不断提高广大师生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。

2、网站不良信息事故处理行动小组及职责。

组长：江静虹。

成员：姚雪青、卢婷芳。

主要职责：

（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，并协助向公安机关报案。

（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。

3、网络恶意攻击事故处理行动小组及职责。

组长：俞莹。

成员：陈帅奇、陈洁。

主要职责：

（2）如果攻击来自校外，立刻从防火墙中查出对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。

（3）如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台电脑，出自哪位教师或学生。接着立刻赶到现场，关闭该计算机网络连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。暂时扣留该电脑。

（4）重新启动该电脑所连接的网络设备，直至完全恢复网络通信。

（5）对该电脑进行分析，清除所有病毒、恶意程序、木马程序以及垃圾文件，测试运行该电脑5小时以上，并同时进行监控，无问题后归还该电脑。

（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。

组长：范显涛。

成员：孙鑫、陈帅奇。

主要职责：

（1）对学校重大事件（如校庆、评估等对网络安全有特别要求的事件）进行评估、确定所需的网络设备及环境。

（2）关闭其它与该网络相连，有可能对该网络造成不利影响的一切网络设备及计算机设备，保障该网络的畅通。

（3）对重要网络设备提供备份，出现问题需尽快更换设备。

（4）对外网连接进行监控，清除非法连接，出现重大问题立刻向上级部门求救。

（5）事先应向领导小组汇报本次事件中所需用到的设备、环境，以及可能出现的事故及影响，在事件过程中出现任何问题应立刻向领导小组组长汇报。

5、通讯联络小组及职责。

组长：王春凤。

成员：孙鑫、陈洁。

主要职责：迅速与学校领导、各相关处室以及相关部门取得联系，引导人员和设施进入事件地；联络有关部门、个人，组织调遣人员；负责对上、对外联系及报告工作。

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。各有关组织随时准备执行应急任务。

2、组织有关人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进行全面检查，封堵、更新有安全隐患的设备及网络环境。加强对校园网内计算机3、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。

4、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。

5、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。

6、按预案落实各项物资准备。

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、各级领导小组在上级统一组织指挥下，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,保证学校公网连接。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，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，注意做好保密工作。

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。

1、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。

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。

3、本预案从发布之日起正式施行。

**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。

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。

2.组织广大师生收看网络安全知识专题视频讲座。

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**

为了切实做好学院校园网络突发事件的防范和应急处理工作，进一步提高预防和控制网络突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保校园网络与信息安全，结合学院工作实际，制定本预案。

第一章总则。

第一条本预案所称突发性事件，是指自然因素或者人为活动引发的危害学院校园网网络设施及信息安全等有关的灾害。

第二条本预案的编制依据是学院有关计算机网络及信息安全基本要求。

第三条本预案适用于发生在学院校园网络上的突发性事件应急工作。

第四条应急处置工作原则：统一领导、统一指挥、各司其职、整体作战、发挥优势、保障安全。

第二章组织机构和主要职责。

第五条学院成立网络与信息安全应急处置工作领导小组。组长由学院行政主要负责人担任，副组长由学院办公室、图文信息中心和保卫处的主要负责人担任，成员由各副组长部门的副职及相关技术骨干组成。领导小组的主要职责是统一领导全校信息网络的灾害应急工作，全面负责学院信息网络可能出现的各种突发事件处置工作，协调解决灾害处置工作中的重大问题等。

第三章处置措施和处置程序。

处置的基本措施分灾害发生前与灾害发生后两种情况。

（一）灾害发生前，学院网络与信息安全应急处置工作小组要预先对灾害预警预报体系进行建设，开展灾害调查，编制灾害防治规划，建设专业监测网络，并规划建设灾害信息管理系统，及时处理灾害讯情信息。

加强灾害险情巡查。图文信息中心要充分发挥专业监测的作用，进行定期和不定期的检查，加强对灾害重点部位的监测和防范，发现有不良险情时，要及时处理并向工作领导小组报告。

建立健全灾情速报制度，保障突发性灾害紧急信息报送渠道畅通。

（二）灾害发生后，立即启动应急预案，按第七条拟定的应急处置程序进行处理。

第七条处置程序。

（一）发现情况。

学院图文信息中心要认真做好校园网信息系统安全的日常巡查及其日志保存工作，以保障最先发现灾害并及时处置突发性事件。

（二）预案启动。

一旦灾害发生，立即启动应急预案，进入应急预案的处置程序。

在灾害发生时，首先应区分灾害发生是否为自然灾害与人为破坏两种情况，根据这两种情况把应急处置方法分为两个流程。

流程一：当发生的灾害为自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

流程二：当人为或病毒破坏的灾害发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的ip或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照灾害发生的性质分别采用以下方案：

1．病毒传播：针对这种现象，要及时断开传播源，判断病毒的性质、采用的端口，然后关闭相应的端口，在网上公布病毒攻击信息以及防御方法。

2．入侵：对于网络入侵，首先要判断入侵的来源，区分外网与内网。入侵来自外网的，定位入侵的ip地址，及时关闭入侵的端口，限制入侵地ip地址的访问，在无法制止的情况下可以采用断开网络连接的方法。入侵来自内网的，查清入侵来源，如ip地址、上网账号等信息，同时断开对应的交换机端口。然后针对入侵方法加强入侵检测设备的建设或更新。

3．信息被篡改：这种情况，要求一经发现马上断开相应的信息上网链接，并尽快恢复。

4．网络故障：一经发现，即根据相应工作流程尽快排除。

5．其它没有列出的不确定因素造成的灾害，可根据总的安全原则，结合具体的情况，做出相应的处理。不能处理的可以向相关专业安全机构请求帮助。

（四）情况报告。

灾害发生时，一方面按照应急处置方法进行处置，同时需要判定灾害的级别，首先向学院网络与信息安全应急处置工作领导小组汇报，并及时报告处置工作进展情况，直至处置工作结束。

情况报告内容包括：灾害发生的时间、地点，灾害的级别，灾害造成的后果，应急处置的过程、结果，灾害结束的时间，以后如何防范类似灾害发生的建议与方案等。

（五）发布预警。

灾害发生时，可根据灾害的危害程度适当地发布预警，特别是一些在其它地方已经出现，或在相关安全网站发布了预警而学院信息网络还没有出现的灾害，除了在技术上进行防范以外，还应当向网络信息用户发布预警，直至灾害警报解除。

（六）预案终止。

经专家组鉴定，灾害险情或灾情已消除，或者得到有效控制后，由学院网络与信息安全应急处置工作领导小组宣布险情或灾情应急期结束，并予以公告，同时预案终止。

第四章保障措施。

灾害应急防治是一项长期的、持续的、跟踪式的、深层次的和各阶段相互联系的工作，是有组织的科学与社会行为，而不是随每次灾害的发生而开始和结束的活动。因此，必须做好应急保障工作。

第八条人员保障。

重视人员的建设与保障，确保灾害处置和灾后重建中相关人员持续在岗，并保持战斗力。

第九条技术保障。

重视网络信息安全系统的建设和更新，确保灾害发生前网络信息系统符合安全规范，信息中心和相关安全设备厂商提供灾害处置过程中和灾后重建的相关技术支撑。

第十条物资保障。

学院要根据近三年全国甚至全世界网络信息系统安全防治工作所需经费情况，购买相应的应急设施。建立应急物资储备制度，保证应急抢险救灾队伍技术装备的及时更新，以确保灾害应急工作的顺利进行。

第十一条训练和演练。

加强学院网络信息用户的防灾、减灾知识的宣传普及，增强用户的防灾意识和自救互救能力。有针对性地开展应急抢险救灾演练，确保发灾后应急救助手段及时到位和有效。

第五章附则。

第十三条本预案自发布之日起施行。

**网络安全应急预案应当按照事件发生后的篇十二**

一、指导思想：

随着互联网及相关信息通信业务的迅速发展，信息传播呈现渠道多样化、影响网络化、扩散快速化的发展趋势，网络信息安全内涵和外延已经远远突破原来的传统概念，涉及到国家的政治、经济、文化等方面，成为关系国家安全和社会稳定的重大问题，从中央到地方无不列为事务工作的重中之重。结合本园自身情况，加强监督和管理，制度本预案。

二、机构设置：

组长：

副组长：

成员：各班班主任。

三、领导小组职责：

1、强化组织机构，加强管理控制：

幼儿园成立以园长为组长的网络安全管理领导小组，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。

2、加强业务培训，提高防范水平：

积极开展相关培训提高网管员的网络管理水平，定期对教师开展互联网安全和文明上网的宣传教育，提高全体教师上网的法制意识、责任意识、政治意识、自律意识和安全意识，形成广大师幼共同抵制网上有害信息的良好氛围，保证幼儿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，网络管理员加强检查，及时发现网络本身的安全漏洞，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，尽量避免网络、病毒等的攻击事件。

3、执行审查制度，保证新闻真实健康：

园内通讯报道工作落实专人负责，经同意后方能发布或传送。未经园长同意而发布的有损于幼儿园和社会形象的言论，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，让通过安全管理小组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：

1、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。

2、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，以保障园网的安全性、稳定性和可靠性。

3、一旦发现园网上出现违反幼儿园网络安全管理制度的行为，立即停止校园网络的使用。

4、网络安全管理领导小组应在第一时间组织有关人员对违纪行为进行查处，对违纪人员依照有关法律、法规和园纪园规，作出严肃处理。

5、对有害的信息则立即删除。

**网络安全应急预案应当按照事件发生后的篇十三**

为了切实做好网络与信息安全突发事件的防范和应急处理工作，进一步提高我院预防和控制网络与信息安全突发事件的能力和水平，减轻或消除突发事件的危害和影响，保证网络的正常运行，结合本院实际，制定本预案。

一、应急处置工作的目标。

在最短时限内，及时、果断处理在本院范围内发生的\'危害网络与信息安全的突发性事件，维护网络信息安全与稳定。

1、网站、网页出现非法言论；

2、网络遭受黑客攻击；

3、计算机网络出现病毒；

4、软件系统遭受破坏性攻击；

5、数据库系统出现故障；

6、广域网外部线路中断；

7、局域网大范围中断；

8、服务器等关键网络设备故障；

9、网络中心机房外电中断。

三、组织领导成立网络与信息安全领导小组。

领导小组的主要职责与任务是统一领导全院网络与信息安全的应急工作，全面负责院内网络与信息安全可能出现的各种突发事件处置工作，协调解决灾害处置工作中的重大问题等。下设网络与信息安全应急处置工作组，由办公室、医务科、保健部成员组成，具体负责网络与信息安全应急处置工作。

四、应急预案启动时的应急处理措施。

1、网站、网页出现非法言论时的紧急处置措施。

(1)网站、网页由各相关使用部门的具体负责人员随时密切监视信息内容。每天不少于5次；非常时期，每半小时监控一次，必要时，24小时监控。

(2)发现网上出现非法信息时，负责人员应立即向应急处置工作组通报情况；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)应急处置工作组人员应在接到通知后十分钟内进行处理，作好必要的记录，清理网站上的非法信息，强化安全防范措施后方可将网站网页重新投入使用。

(4)应急处置人员应妥善保存有关记录及日志或审计记录。

(5)应急处置人员应立即追查非法信息来源，若非法信息来源于院内，则由本院保卫处和网络技术人员进行处理，同时报告网络与信息安全领导小组负责人，根据管理制度对非法传播者及时处置，并报知上级公安部门备案；若非法信息来自于院外，则立即报知上报公安部门，并由技术人员将这些信息保存、记录ip地址，以备上级公安部门互联网突发事件处置行动组调用。

2、黑客攻击时的紧急处置措施。

(1)当有关负责人员发现网页内容被篡改，或通过防火墙、入侵检测系统发现有黑客正在进行攻击时,应立即向应急处置工作组通报情况。

(2)应急处置人员应在十分钟内进行处理，首先应将被攻击的服务器等设备从网络中隔离出来，保护现场，同时向网络与信息安全领导小组汇报情况。

(3)应急处置人员负责被破坏系统的恢复与重建工作，修补漏洞、强化安全措施后方可将被攻击的服务器设备接入网络。

(4)应急处置人员追查非法信息来源。

(5)网络与信息安全领导小组会商后，如认为情况严重，则立即向公安部门汇报。

(1)当发现网络上出现病毒，并影响网络的正常运行后，应立即找出感染病毒机器。

(2)将感染病毒机器和网络隔离，待病毒彻底清除后方允许再次接入网络。

(3)网络中心技术人员要针对该款病毒进行研究，做好相应的病毒发作特征及解决方案。

4、软件系统遭受破坏性攻击的紧急处置措施。

(1)重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将它们保存于安全处。

(2)一旦软件遭到破坏性攻击，应立即停止软件系统。

(3)网络管理人员负责软件系统和数据的恢复。

(4)网络管理人员检查日志等资料，确认攻击来源。

(5)安全领导小组认为情况极为严重的，应立即向公安部门报告。

5、数据库安全紧急处置措施。

(1)各数据库系统要至少准备两个以上数据库备份，平时一份放在机房，另一份放在另一安全的建筑物中。

(2)一旦数据库崩溃，应急处置组人员应对主机系统进行维修，如遇无法解决的问题，立即向上级单位或软硬件提供商请求支援。

(3)系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。

(4)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。

(5)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，并向网络与信息安全领导小组汇报。

6、广域网外部线路中断紧急处置措施。

(1)广域网线路中断后，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。

(2)如属我院管辖范围，由网络管理员予以恢复。如遇无法恢复情况，立即向有关厂商请求支援。

(3)如属电信部门管辖范围，立即与电信维护部门联系，请求修复。

7、局域网大范围中断紧急处置措施。

(1)局域网出现大范围中断现象后，网络管理员应立即判断故障节点，查明故障原因。

(2)如属线路故障，应重新安装线路。

(3)如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调试畅通。

(4)如属路由器、交换机等网络设备故障，应立即调换备机，如无备机，立即向设备提供商联系更换设备，并调试畅通；并向网络与信息安全领导小组领导汇报。

8、服务器等关键网络设备故障安全紧急处置措施。

(1)服务器等关键设备损坏后，网络管理人员应立即查明原因。

(2)如果能够自行恢复，应立即用备件替换受损部件。

(3)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。

(4)如果设备一时不能修复，应向网络与信息安全领导小组汇报。

9、网络中心机房外电中断后的处置措施。

(1)外电中断后，机房会自动切换到备用电源。

(2)检查断电原因，如因内部线路故障，请总务科协助迅速恢复。

(3)如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

(4)如果供电局告知需长时间停电，应做如下安排：

a)预计停电1小时以内，由ups供电。

b)预计停电1-3小时，关掉非关键设备，确保各主机、路由器、交换机供电。

c)预计停电超过3小时，关掉非关键设备，确保各主机、路由器、交换机供电。ups使用4小时后，关闭所有的设备。

五、保障措施。

网络与信息安全的防治工作是一项长期的、持续的、跟踪式的、深层次的和各阶段相互联系的工作，是有组织的科学与社会行为，而不是随着每次灾害的发生而开始和结束的活动。因此，必须做好应急保障工作。

1、人员保障。

重视网络管理人员队伍的建设与保障，确保在灾害发生前的人员值班，灾害处置过程和灾后重建中的人员在岗与战斗力。

2、技术保障。

重视网络信息技术的建设和升级换代，在灾害发生前确保网络信息系统的安全与稳定，灾害处置过程中和灾后重建中的相关技术支撑。

3、物资保障网络与信息安全应急处置工作组，报请领导小组批准后，根据院财力情况及网络管理的实际需要，适当购入一些网络与信息安全保障设备。

4、训练和演练。

加强全院网络信息用户的防灾、减灾知识的宣传普及，增强这些用户的防灾意识和自救互救能力。有针对性地开展应急抢险救灾演练，确保发生灾害时的应急救助手段及时到位和有效。

组长：\_\_副组长：\_\_组员：\_\_。

组长：\_\_副组长：\_\_组员：\_\_。

**网络安全应急预案应当按照事件发生后的篇十四**

为保证我局信息系统安全，加强和完善网络与信息安全应急管理措施，层层落实责任，有效预防、及时控制和最大限度地消除信息安全突发事件的危害和影响，确保信息系统和网络的通畅运行，结合实际，特制定本应急预案。

（一）工作目标

保障信息的合法性、完整性、准确性，保障网络、计算机、相关配套设备设施及系统运行环境的安全，其中重点维护网络系统、国土资源业务系统、基础数据库服务器及国土资源网站的安全。

（二）编制依据

根据《中华人民共和国计算机信息系统安全保护条例》、《互联网信息服务管理办法》、《计算机病毒防治管理办法》等相关法规、规定、文件精神，制定本预案。

（三）基本原则

1、预防为主。根据《计算机信息安全管理规定》的要求，建立、健全国土资源计算机信息安全管理制度，有效预防网络与信息安全事故的发生。

2、分级负责。按照“谁主管谁负责，谁运营谁负责”的原则，建立和完善安全责任制。各部门应积极支持和协助应急处置工作。

3、果断处置。一旦发生网络与信息安全事故，应迅速反应，及时启动应急处置预案，尽最大力量减少损失，尽快恢复网络与系统运行。

（四）适用范围

本预案适用于局属各单位、机关各股室。

成立网络与信息安全领导组，为我局网络与信息安全应急处置的组织协调机构。

1、局网络与信息安全应急领导组组长由局长赵学崇同志担任，成员由各股室负责人及相关人员组成。负责网络与信息安全应急响应工作的整体规划、组织协调和决策指挥。

2、网络与信息安全应急领导组下设办公室。办公室主任由纪检组长郭占明同志担任。

职责：

（1）负责和处理局应急领导小组的日常工作，检查督促局应急领导组决定事项的落实。

（2）负责局网络与信息安全应急预案的管理，指导督促重要信息系统应急预案的修订和完善，检查落实预案执行情况。

（3）指导全局应对网络与信息安全突发公共事件的预案演习、宣传培训、督促应急保障体系建设。

1.信息监测与报告。

（1）按照“早发现、早报告、早处置”的原则，加强对局属各单位、各股室有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发公共事件时，按规定及时向应急领导小组报告，初次报告最迟不得超过1小时，重大和特别重大的网络与信息安全突发公共事件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。

网络恐怖活动的嫌疑情况和预警信息；其他影响网络与信息安全的信息。

2.预警处理与发布。

（1）对于可能发生或已经发生的网络与信息安全突发公共事件，立即采取措施控制事态，并向应急领导小组汇报情况。

（2）应急领导小组接到报告后，应迅速召开应急领导小组会议，研究确定网络与信息安全突发公共事件的等级，根据具体情况启动相应的应急预案，并向相关部门进行汇报。

（一）网站、网页出现非法言论时的应急预案

1、网站、网页由负责网站维护的管理员随时监控信息内容。

2、发现在网上出现非法信息时，网站管理员立即向信息安全领导小组通报情况，并作好记录。清理非法信息，采取必要的安全防范措施，将网站、网页重新投入使用；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、网站管理员应妥善保存有关记录、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。

4、事态严重的，立即向信息安全领导组组长报告，并向相关部门进行汇报。

（二）黑客攻击或软件系统遭破坏性攻击时的应急预案

1、重要的软件系统平时必须存有备份，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、当管理员通过入侵监测系统发现有黑客正在进行攻击时，应立即向局信息安全领导小组日常应急办公室报告。软件遭破坏性攻击（包括严重病毒）时要将系统停止运行。

3、管理员首先要将被攻击（或病毒感染）的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报告情况。

4、日常应急办公室负责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。

5、事态严重的，立即向信息安全领导组组长报告，并向相关部门进行汇报。

（三）数据库发生故障时的应急预案

1、主要数据库系统应定时进行数据库备份。

2、一旦数据库崩溃，管理员应立即进行数据及系统修复，修复困难的，可向县信息产业中心汇报情况，以取得相应的技术支持。

3、在此情况下无法修复的，应向信息安全领导组报告，在征得许可的情况下，可立即向软硬件提供商请求支援。

4、在取得相应技术支援也无法修复的，应及时向信息安全领导小组组长或局长报告，在征得许可、并可在业务操作弥补的情况下，由日常应急办公室信息安全岗人员利用最近备份的数据进行恢复。

（四）设备安全发生故障时的应急预案

1、小型机、服务器等关键设备损坏后，管理员应立即向日常应急办公室报告。

2、日常应急办公室网络安全岗负责人员立即查明原因。

3、如果能够自行恢复，应立即用备件替换受损部件。

4、如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

5、如果设备一时不能修复，应向信息安全领导小组汇报，并告知各股室，暂缓上传上报数据，直到故障排除设备恢复正常使用。

（五）内部局域网故障中断时的应急预案

1、局办公室平时应准备好网络备用设备，存放在指定的位置。

2、局域网中断后，网络安全岗负责人员应立即判断故障节点，查明故障原因，并向日常应急办公室汇报。

3、如属线路故障，应重新安装线路。

4、如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

5、如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

6、如有必要，应向信息安全领导组汇报。

（六）广域网外部线路中断时的应急预案

1、广域网线路中断后，管理员应向信息安全领导组日常应急办公室报告。

2、日常应急办公室网络安全岗负责人员接到报告后，应迅速判断故障节点，查明故障原因。

3、如属可即时恢复范围，由网络安全组人员立即予以恢复。

4、如属电信运营商管辖范围，应立即与电信运营商的维护部门联系，要求尽快修复。

5、如果恢复时间预计超过两小时,应立即向信息安全领导小组汇报。经领导小组同意后，应通知各股室暂缓上传上报数据。

（七）外部电中断后的应急预案

1、外部电中断后，值班室应立即向管理员汇报情况。

2、如因局内线路故障，由办公室通知维修人员迅速恢复。

3、如果是局外部的原因，由办公室立即与供电局联系，请供电局迅速恢复供电；如果供电局告知需长时间停电，应做如下安排：

（1）预计停电2小时以内，由ups供电；

（2）预计停电2-4小时，关掉非关键设备，确保各主机、路由器、交换机供电；

（3）预计停电超过4小时，白天工作时间关键设备运行，晚上所有设备停机。

（八）机房发生火灾时的应急预案

1、一旦机房发生火灾，应遵循下列原则：首先保证人员安全；其次保证关键设备、数据安全；三是保证一般设备安全。

2、人员灭火和疏散的程序是：值班人员应首先切断所有电源，同时通过119电话报警。值班人员戴好防毒面具，从最近的位置取出灭火器进行灭火，其他人员按照预先确定的路线，迅速从机房中有序撤出。

1.先期处置。

（1）当发生网络与信息安全突发公共事件时，值班人员应做好先期应急处置工作，立即采取措施控制事态，同时向局应急办公室报告。

（2）应急办公室在接到网络与信息安全突发公共事件发生或可能发生的信息后，应立即向应急领导小组汇报，并加强与有关方面的联系，并做好启动本预案的各项准备工作。

2.应急指挥。

预案启动后，要抓紧收集相关信息，掌握现场处置工作状态，分析事件发展态势，研究提出处置方案，统一指挥网络与信息应急处置工作。

3.应急支援。

预案启动后，立即成立由应急领导小组领导带队的应急响应先遣小组，督促、指导和协调处置工作。局应急领导小组根据事态的发展和处置工作需要，及时增派专家小组，调动必需的物资、设备，支援应急工作。

4.信息处理。

（1）应对事件进行动态监测、评估，将事件的性质、危害程度和损失情况及处置工作等情况，及时报应急领导小组，不得隐瞒、缓报、谎报。

（2）应急领导小组要明确信息采集、编辑、分析、审核、签发的责任人，做好信息分析、报告和发布工作。

5.应急结束。

网络与信息安全突发公共事件经应急处置后，由事发单位向应急领导小组提出应急结束的建议，经批准后实施。

1.善后处理。

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。

2.调查评估。

在应急处置工作结束后，局应急领导小组办公室应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，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。

1.数据保障。

重要信息系统均应建立备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。

2.应急队伍保障。

按照一专多能的要求建立网络信息安全应急保障队伍。

3.经费保障。

落实网络与信息系统突发公共事件应急处置资金。

1.宣传教育。

要充分利用各种传播媒介及有效的形式，加强网络与信息安全突发公共事件应急和处置的有关法律法规和政策的宣传，开展预防、预警、自救、互救和减灾等知识的宣讲活动，普及应急救援的基本知识，提高公众防范意识和应急处置能力。

要加强对网络与信息安全等方面的知识培训，提高防范意识及技能，指定专人负责安全技术工作。并将网络与信息安全突发公共事件的应急管理、工作流程等列为培训内容，增强应急处置工作的组织能力。

2.责任与奖惩。

网络与信息系统的管理部门要认真贯彻落实预案的各项要求与任务，建立监督检查和奖惩机制。应急领导小组将不定期进行检查，对各项制度、计划、方案、人员等进行实地验证。

**网络安全应急预案应当按照事件发生后的篇十五**

为提高我校处理网络与信息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，确保我校校园网络重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网络信息安全突发事件的危害，保护师生权益，维护正常社会秩序、教学秩序，促进学校的和谐发展。

2、编制依据。

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互联网管理暂行规定》等有关法规、规定，制定本预案。

3、适用范围。

本预案适用于我校校园网络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。

本预案启动后，我校以前制定的网络与信息安全应急预案与本预案相冲突的，按照本预案执行。而法律、法规和规章另有规定的从其规定。

4、分类分级。

本预案所指的网络信息安全突发事件，是指我校校园网等重要网络信息系统突然遭受不可预知外力的破坏、毁损或故障，不良信息在我校校园网乃至整个互联网的传播，发生对国家、社会、公众、学院造成或者可能造成危害的紧急网络安全事件。

事件分类根据网络信息安全突发事件的发生过程、性质和特征，网络信息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，互联网攻击、病毒攻击、恐怖主义活动等事件。

事件分级。

根据我省对网络信息安全突发事件的可控性、严重程度和影响范围，将网络信息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）：造成我校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、公共利益或教育形象造成特别严重损害的突发事件。

（2）ii级（重大）：造成我校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、公共利益或教育形象造成严重损害，需要上级政府或公安部门协助，乃至需跨地区协同处置的突发事件。

（3）iii级（较大）：造成我校网络与信息系统瘫痪，对国家安全、社会秩序、公共利益或教育形象造成一定损害，但只需在本区政府或区信息中心协同处置的突发事件。

（4）iv级（一般）：造成我校校园网络重要网络与信息系统受到一定程度的损坏，对师生、家长或其他人员和单位的权益有一定影响，但不危害国家安全、社会秩序和公共利益，可由我区教育主管部门或学校处置的突发事件。

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，构筑我校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，进一步提高师生的信息安全意识。

3、落实措施、确保安全。要对机房、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；在国际互联网上已建立网站的分院单位，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、依靠科学、平战结合。各办学单位应根据本预案的标准，建立本单位的应急处置预案，并加强技术储备、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。

（1）当发生网络信息安全突发事件时，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信息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。

发生信息安全事件的部门应当在发生信息安全事件后，首先以口头方式立即向我校信息安全管理办公室报告。

发生信息安全事件的部门应当立即对发生的事件进行调查核实、保存相关证据，并在事件被发现或应当被发现时起5小时内将有关材料报至我校信息安全管理办公室。

对于信息安全事件，我校信息安全管理办公室接到报告后，应当立即上报院领导，并负责组织人员对事件进行调查和处理。

发生信息安全事件的部门应当在事件处理完毕后5个工作日内将处理结果报院办备案。

我校信息安全管理办公室负责组织对事件进行分析和研究，并将结果通报院领导。

（2）学院信息安全管理办公室负责人和院领导应确立两个以上的即时联系方式，公众可通过固定电话、移动电话、互联网等多种联系方式进行报警，避免因信息网络突发事件发生后，必要的信息通报与指挥协调通信渠道中断。

（1）对于可能发生或已经发生的网络信息安全突发事件，应立即采取措施控制事态，并在2小时内进行相应的风险评估，并及时按规定向校长和有关部门报告。

（2）发现网络信息安全突发事件或事故时，区教育网络管理中心配合对突发事件或事故进行风险评估，并把评估信息及时反馈给区应急小组。

应急响应应急结束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院领导，由院领导向区应急小组提出应急结束的建议，经批准后实施。

保障措施应急技术队伍保障按照一专多能的要求建立我校网络与信息安全应急技术保障队伍。并定期参加信息安全配训。

1、宣传教育我校将充分利用学校各种传播媒介及有效的形式，比如校园网络、校园广播、校园电视台、教职工大会、班会等形式，加强对计算机信息网络安全的宣传和教育工作，提高师生的防范意识和应急处置能力。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。并将网络与信息安全突发事件的应急管理、工作流程等列为学校行政管理干部的培训内容，增强应急处置工作中的组织能力。

2、演练建立应急预案定期演练制度。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。

3、责任与奖惩要认真贯彻落实预案的各项要求与任务，建立监督检查制度。学校将不定期进行检查，对各项制度、计划、方案、人员等进行实地督察，对未有效落实预案各项规定的进行通报批评，责令限期改正。

文档为doc格式。

**网络安全应急预案应当按照事件发生后的篇十六**

根据教育局要求，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，确保突发事件“发现的早、化解的了、控制的住、处置的好，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。

学校全体行政人员及全体网络管理员组成网络安全应急领导小组。

1.领导小组成员：

组长：曹懿副组长：赵丽萍梅艳杰

成员：袁飞、何龚兰、沈朝香、吴永红、陶裕彬、汤晓菊、龚慧叶、李芳

责任人：学校领导网络管理员

2.领导小组主要职责：

（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，不断提高广大师生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。

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。

（3）如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台电脑，出自哪位教师或学生。接着立刻赶到现场，关闭该计算机网络连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。暂时扣留该电脑。

（4）重新启动该电脑所连接的网络设备，直至完全恢复网络通信。

（5）对该电脑进行分析，清除所有病毒、恶意程序、木马程序以及垃圾文件，测试运行该电脑5小时以上，并同时进行监控，无问题后归还该电脑。

（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.学校重大网络事件处理预案

（1）对学校重大事件（如校庆、评估等对网络安全有特别要求的事件）进行评估、确定所需的网络设备及环境。

（2）关闭其它与该网络相连，有可能对该网络造成不利影响的一切网络设备及计算机设备，保障该网络的畅通。

（3）对重要网络设备提供备份，出现问题需尽快更换设备。

（4）对外网连接进行监控，清除非法连接，出现重大问题立刻向上级部门求救。

（5）事先应向领导小组汇报本次事件中所需用到的设备、环境，以及可能出现的事故及影响，在事件过程中出现任何问题应立刻向领导小组组长汇报。

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。

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，注意做好保密工作。

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。

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。

本文档由范文网【dddot.com】收集整理，更多优质范文文档请移步dddot.com站内查找