信息安全应急预案优秀6篇（信息安全应急预案优秀6篇）

作者：有故事的人 来源：范文网 www.wtabcd.cn/fanwen/

本文原地址：https://www.wtabcd.cn/fanwen/meiwen/b299173ced012eb324d4ecf71589a0e5.html

在学习、工作、生活中，难免会发生一些不在自己预期的事件，为了控制事故的发展，很有必要提前准备一份具体、详细、针对性强的应急预案。那么大家知道应急预案怎么写才规范吗？t7t8美文号为您带来了6篇《信息安全应急预案》，希望可以启发、帮助到大朋友、小朋友们。

网络与信息安全应急处置预案 篇一

一、总则

（一）编制目的

为提高我局处置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，最大程度地预防和减少网络与信息安全突发事件及其造成的损害，保障信息资产安全，特制定本预案。

（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》、公安部《计算机病毒防治管理办法》，制定本预案。

（三）分类分级

本预案所称网络与信息安全突发事件，是指我局信息系统突然遭受不可预知外力的破坏、毁损、故障，发生对国家、社会、公众造成或者可能造成重大危害，危及公共安全的紧急事件。

1、事件分类

根据网络与信息安全突发事件的性质、机理和发生过程，网络与信息安全突发事件主要分为以下三类：

（1）自然灾害。指地震、台风、雷电、火灾、洪水等引起的网络与信息系统的损坏。

（2）事故灾难。指电力中断、网络损坏或是软件、硬件设备故障等引起的网络与信息系统的损

坏。

（3）人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

2、事件分级

根据网络与信息安全突发事件的可控性、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）和Ⅳ级（一般）。

（1）Ⅰ级（特别重大）、Ⅱ级（重大）。重要网络与信息系统发生全局大规模瘫痪，事态发展超出我局的控制能力，需要由县网络与信息安全应急协调小组跨部门协调解决，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的信息安全突发事件。

（2）Ⅲ级（较大）。某一部分的重要网络与信息系统瘫痪，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但在我局控制之内的信息安全突发事件。

（3）Ⅳ级（一般）。重要网络与信息系统使用效率上受到一定程度的损坏，对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益的信息安全突发事件。

（四）适用范围

本预案是局本级网络与信息安全的专项预案，适用于本局发生或可能导致发生网络与信息安全突发事件的应急处置工作。

（五）工作原则

1、居安思危，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关系国家安全、经济命脉、社会稳定的重要信息系统，从预防、监控、应急处理、应急保障和打击犯罪等环节，在法律、管理、技术、人才等方面，采取多种措施，充分发挥各方面的作用，共同构筑网络与信息安全保障体系。

2、提高素质，快速反应。加强网络与信息安全科学研究和技术开发，采用先进的监测、预测、预警、预防和应急处置技术及设施，充分发挥专业人员的作用，在网络与信息安全突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

3、以人为本，减少损害。把保障公共利益以及公民、法人和其他组织的合法权益的安全作为首要任务，及时采取措施，最大限度地避免公共财产、信息资产遭受损失。

4、加强管理，分级负责。按照“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，加强部门间协调与配合，形成合力，共同履行应急处置工作的管理职责。

5、定期演练，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，实现网络与信息安全突发事件应急处置的科学化、程序化与规范化。

二、组织指挥机构与职责

（一）组织体系

成立局网络与信息安全领导小组，组长由分管副局长担任（特殊情况由局长担任），副组长由办公室主任、分管信息化副主任担任。成员包括：各处室负责人及联络员等。

（二）工作职责

1、研究制订我局网络与信息安全应急处置工作的规划、计划和政策，协调推进我局网络与信息安全应急机制和工作体系建设。

2、发生I级、Ⅱ级、Ⅲ级网络与信息安全突发事件后，决定启动本预案，组织应急处置工作。如网络与信息安全突发事件属于I级、Ⅱ级的，向县有关部门通报并协调县有关部门配合处理。

3、研究提出网络与信息安全应急机制建设规划，检查、指导和督促网络与信息安全应急机制建设。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。

4、指导应对网络与信息安全突发事件的科学研究、预案演习、宣传培训，督促应急保障体系建设。

5、及时收集网络与信息安全突发事件相关信息，分析重要信息并提出处置建议。对可能演变为I级、Ⅱ级、Ⅲ级的网络与信息安全突发事件，应及时向局领导提出启动本预案的建议。

6、负责提供技术咨询、技术支持，参与重要信息的研判、网络与信息安全突发事件的调查和总结评估工作，进行应急处置工作。

三、监测、预警和先期处置

（一）信息监测与报告

1、要进一步完善各重要信息系统网络与信息安全突发事件监测、预测、预警制度。按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发事件和可能引发网络与信息安全突发事件的有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发事件时，在按规定向有关部门报告的同时，按紧急信息报送的规定及时向局领导汇报。初次报告最迟不得超过4小时，较大、重大和特别重大的网络与信息安全突发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。

2、重要信息系统管理人员应确立2个以上的即时联系方式，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。

3、信息安全定期汇报。每周应向县工能局报告我局网络与信息安全自查工作进展情况：

（1）恶意人士利用我局网络从事违法犯罪活动的情况。

（2）网络或信息系统通信和资源使用异常，网络和信息系统瘫痪、应用服务中断或数据篡改、丢失等情况。

（3）网络恐怖活动的嫌疑情况和预警信息。

（4）网络安全状况、安全形势分析预测等信息。

（5）其他影响网络与信息安全的信息。

（二）预警处理与预警发布

1、对于可能发生或已经发生的网络与信息安全突发事件，系统管理员应立即采取措施控制事态，并在2小时内进行风险评估，判定事件等级并发布预警。必要时应启动相应的预案，同时向信息安全领导小组汇报。

2、领导小组接到汇报后应立即组织现场救援，查明事件状态及原因，技术人员应及时对信息进行技术分析、研判，根据问题的性质、危害程度，提出安全警报级别。

（三）先期处置

1、当发生网络与信息安全突发事件时，及时请技术人员做好先期应急处置工作并立即采取措施控制事态，必要时采用断网、关闭服务器等方式防止事态进一步扩大，同时向上级信息安全领导小组通报。

2、信息安全领导小组在接到网络与信息安全突发事件发生或可能发生的信息后，应加强与有关方面的联系，掌握最新发展态势。对有可能演变为Ⅲ级网络与信息安全突发事件，技术人员处置工作提出建议方案，并作好启动本预案的各项准备工作。信息安全领导小组根据网络与信息安全突发事件发展态势，视情况决定现场指导、组织设备厂商或者系统开发商应急支援力量，做好应急处置工作。对有可能演变为Ⅱ级或Ⅰ级的网络与信息安全突发事件，要根据县有关部门的要求，上报县政府有关部门，赶赴现场指挥、组织应急支援力量，积极做好应急处置工作。

四、应急处置

（一）应急指挥

1、本预案启动后，领导小组要迅速建立与现场通讯联系。抓紧收集相关信息，掌握现场处置工作状态，分析事件发展趋势，研究提出处置方案，调集和配置应急处置所需要的人、财、物等资源，统一指挥网络与信息安全应急处置工作。

2、需要成立现场指挥部的，局机关立即在现场开设指挥部，并提供现场指挥运作的相关保障。现场指挥部要根据事件性质迅速组建各类应急工作组，开展应急处置工作。

（二）应急支援

本预案启动后，领导小组可根据事态的发展和处置工作需要，及时向市政府相关单位申请增派专家小组和应急支援单位，调动必需的物资、设备，支援应急工作。参加现场处置工作的有关人员

要在现场指挥部统一指挥下，协助开展处置行动。

（三）信息处理

现场信息收集、分析和上报。技术人员应对事件进行动态监测、评估，及时将事件的性质、危害程度和损失情况及处置工作等情况及时报领导小组，不得隐瞒、缓报、谎报。符合紧急信息报送规定的，属于I级、Ⅱ级信息安全事件的，同时报县委、县政府相关网络与信息安全部门。

（四）扩大应急

经应急处置后，事态难以控制或有扩大发展趋势时，应实施扩大应急行动。要迅速召开信息安全工作领导小组会议，根据事态情况，研究采取有利于控制事态的非常措施，并向县政府有关部门请求支援。

（五）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，将各监测统计数据报信息安全工作领导小组，提出应急结束的建议，经领导批准后实施。

五、后期处置

（一）善后处置

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，统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，迅速组织实施。

（二）调查和评估

在应急处置工作结束后，信息安全工作领导小组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状况和总结经验教训，写出调查评估报告。

六、应急保障

（一）通信与信息保障

领导小组各成员应保证电话24小时开机，以确保发生信息安全事故时能及时联系到位。

（二）应急装备保障

各重要信息系统在建设系统时应事先预留出一定的应急设备，做好信息网络硬件、软件、应急救援设备等应急物资储备工作。在网络与信息安全突发事件发生时，由领导小组负责统一调用。

（三）数据保障

重要信息系统应建立容灾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。

（四）应急队伍保障

按照一专多能的要求建立网络与信息安全应急保障队伍。选择若干经国家有关部门资质认可的，具有管理规范、服务能力较强的企业作为我局网络与信息安全的社会应急支援单位，提供技术支持与服务；必要时能够有效调动机关团体、企事业单位等的保障力量，进行技术支援。

（五）交通运输保障

应确定网络与信息安全突发事件应急交通工具，确保应急期间人员、物资、信息传递的需要，并根据应急处置工作需要，由领导小组统一调配。

（六）经费保障

网络与信息系统突发公共事件应急处置资金，应列入年度工作经费预算，切实予以保障。

七、监督管理

（一）宣传教育和培训

要充分利用各种传播媒介，采取多种形式，加强有关网络与信息安全突发事件应急处置的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，提高我局信息安全防范意识和应急处置能力。

将网络与信息安全突发事件的应急管理、工作流程等列入各股室及各司法所主要负责人的培训内容，增强应急处置工作中的组织能力。加强对网络与信息安全突发事件的技术准备培训，提高工作人员的防范意识及技能。

（二）预案演练

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。

（三）责任与奖惩

要认真贯彻落实预案的各项要求与任务，建立分级布置、监督检查和奖惩机制。领导小组按预案的规定不定期进行检查，对未有效落实预案各项规定进行通报批评，责令限期改正，对落实到位给予相应的奖励。

八、附则

（一）预案管理与更新

本预案由局办公室制订，报局领导批准后实施。

结合信息网络快速发展的特点和我局实际状况，及时修订本预案。

（二）解释部门

本预案由网络与信息安全办公室负责解释。

（三）实施时间

本预案自发布之日起实施。

信息网络安全应急预案策划 篇二

一、活动目标：

1、认知目标：认识计算机、网络与中学生获取信息的关系；

2、情感目标：正确对待网络，不沉溺其中，自觉抵制网络的不良影响；

3、行为目标：展示新时代中学生丰富多彩的网络生活与实践成果。

二、活动内容：

1、展示学生网络成果：借助网络支持和大屏幕演示，展示学生丰富多彩的网络生活与实践成果。

2、提出诸多负面事件，通过讨论网络的负面影响，充分认识网络，为下一步正确认识、正确使用网络的讨论奠定基础。

3、树立正确网络观：在充分演示、讨论的基础之上，客观公正地认识网络。

4、讨论网络秩序的维护：确立“维护网络秩序，人人有责”的观念，并提出一些行之有效的具体措施。

三、课前准备：

1、搜集、整理班级电子图文信息，建立班级相册、ppt演示文稿展示、电子学习助手等等。

2、搜集计算机、网络负面影响的报道，并进行资料分类整理。

3、技术支持：多媒体演示教室一间，黑板一块，观众座位若干。

四、活动过程：

（一）网络并不远，就在你我身边——网聚魅力展示

1、记录精彩每一刻——班级电子相册展示

由通过扫描或数码照相存入的相片集结成册，内容包括：

（1）每位同学最满意的个人照片及一句话格言，每位教师的照片及寄语；

（2）重大集体活动，如军训、运动会、春游等具有纪念意义的相关照片。

2、一人有“难”（“难题”的“难”），八方支援——电子学习助手

从德智体各个方面概括介绍班级的情况。以word文档、ppt演示文稿的形式，总结各学科知识的重难点。

3、知识的海洋任我游——现场网络资源搜索

由观众提出有待查询的知识点，现场搜索。

（二）虚拟的世界中，我不辨南北西东——认清网络的负面性

讨论主要集中在以下几个方面：

1、不是我不想走，实在是欲罢不能——对沉迷网络游戏的讨论。

2、还我明亮的眼睛，还我健康的体魄——对损害身体健康的讨论。

3、虚拟世界中，我是谁，你又是谁？——对网恋，网上散布谣言，网络购物骗买骗卖现象的讨论，实质是对网络道德、责任的讨论。

在观众讨论的同时，用多媒体将观众搜集的视听信息播放在大屏幕上。所有讨论内容由主持人进行分类整理，并将之概括在演示黑板

（三）谁之过，网络还是我？——网络的利弊讨论

主持人：网络到底带来了些什么？为什么有人凭借着它走向成功、走向辉煌，也有人因之而走向堕落、走向毁灭？由此引发对网络本质的讨论。由主持人对讨论走向进行把握，对讨论结果进行总结。由一位计算机录入速度较快的同学，将讨论结果录入机器，并用大屏幕展示出来。

讨论结果集中为：

1、网络本善良：网络是一种媒介、一种手段、一种工具、是为我们架起的一座与外界沟通的桥梁，本身无所谓对错。

2、虚拟的世界中，我们仍旧是现实的：网络虽然是一个与现实生活截然不同的虚拟世界，但仍离不开现实的道德与规范。

3、网络面前，人人平等：网络为每个人提供了相等的资源，从中获益还是受害，全靠自己把握。

（四）将网络规则进行到底——维护网络秩序讨论

网络秩序，从我做起；网络秩序，人人有责。面对网络，应该做到：

1、提高自身素质，抵制网络诱惑；

2、发现不良信息，通知朋友共同抵制，并报告有关部门。

五、班主任讲话

通过同学们的交流反映，看来网络值得关注问题还真不少网络已深入我们每个人生活的各个方面，但它到底会成为汩汩长流的智慧泉源，抑或是上天“赐予”人类的“潘多拉盒子”，却是因人而异的。因此同学们要正确认识网络，自觉抵御诱惑。而且我们学校也规定在校生周一至周五严禁上网，请同学们自觉遵守。

信息网络安全应急预案策划 篇三

总则

1.1编制目的

为高效有序地做好机房火灾事故的应急处置工作，避免或最大程度地减轻火灾事故造成的损失，保障员工生命和企业财产安全，维护社会稳定。

1.2编制依据

《中华人民共和国安全生产法》《江苏省消防条例》

1.3适用范围

适用于机房火灾事故的现场应急处置和应急救援工作。

2、事件特征

2.1事件类型及危险性分析

2.1.1电气线路短路、过载、接触电阻过大，静电，雷击等强电侵入，机房内电脑、空调等用电设备长时间通电过热、设备故障等原因均可能引起计算机房的火灾事故。

2.1.2机房火灾事故会造成计算机设备损坏、系统故障网络中断或瘫痪，影响网络的安全运行。

2.1.3火灾产生的有毒烟雾污染机房的空气，造成人员中毒、窒息等人身伤亡事故。

3、应急组织及职责

3.1火灾应急指挥部

应急指挥部总指挥：

机房火灾应急抢险指挥：

成员：

3.2指挥部人员的职责

3.2.1指挥的职责：全面指挥突发事件应急救援工作。

3.2.2高低压专业职责：组织、协调本部门人员参加应急处置和救援工作，对发生险情机房切断电源。

3.2.3智能化专业职责：监控相关区域事故情况。

3.2.4空调专业职责：发现异常情况，及时切断空调、通风系统，做好运行方式的调整和故障设备的隔离。 4应急处置

4.1现场应急处置程序

4.1.1最早发现火情者应立即向值班长和机房负责人汇报，机房负责人到现场指挥灭火，

同时报告公司领导，启动本预案。

4.1.2机房负责人根据事故状态及危害程度做出相应的应急决定，指挥疏散现场无关人员，各应急救援队立即开展救援。

4.1.3事故扩大时，拨打119报警电话请求市消防队支援。报警内容：单位名称、地址、着火物质、火势大小、着火范围。把自己的电话号码和姓名告诉对方，以便联系。同时还要注意听清对方提出的问题，以便正确回答。打完电话后，要立即到交叉路口等候消防车的到来，以便引导消防车迅速赶到火灾现场。

4.2现场应急处置措施

4.2.1机房负责人组织人员迅速查明着火原因。

4.2.2发生火灾事故后，运行值班人员在人身安全不受危害的情况下要坚守本职岗位，确保设备运行。

4.2.3火灾初起阶段，值班人员要利用区域内常规灭火器（干粉或气体灭火器）进行扑救。控制初起火灾，防止火势蔓延。根据火势情况立即启动气体自动灭火装置。

4.2.4被困火场逃生时，应用湿毛巾捂住口鼻，背向烟火方向迅速离开。逃生通道被切断、短时间内无人救援时，应关紧迎火门窗，用湿毛巾、湿布堵塞门缝，用水淋透房门，防止烟火侵入。

4.2.5火灾发生时要采取有效措施扑灭身上的火焰，使伤员迅速脱离开致伤现场。当衣服着火时，

应采用各种方法尽快地灭火，如水浸、水淋、就地卧倒翻滚等，千万不可直立奔跑或站立呼喊，以免助长燃烧，引起或加重呼吸道烧伤。灭火后伤员应立即将衣服脱去，如衣服和皮肤粘在一起，可在救护人员的帮助下把未粘的部分剪去，并对创面进行包扎。

4.2.6在火场，对于烧伤创面一般可不做特殊处理，尽量不要弄破水泡，不能涂龙胆紫一类有色的外用药，以免影响烧伤面深度的判断。为防止创面继续污染，避免加重感染和加深创面，对创面应立即用三角巾、大纱布块、清洁的衣眼和被单等，给予简单而确实的包扎。手足被烧伤时，应将各个指、趾分开包扎，以防粘连。

4.2.7消防队到达火场时，应立即与消防队负责人取得联系并交待失火设备现状和运行设备状况，然后协助消防队灭火，并提供技术支援。

4.2.8复情况，事故应急处理全部结束，才能恢复生产秩序。

4.3火灾事故报告流程

4.3.1出现火情后，值班人员除采取有效措施扑灭初期火情外应立即想机房负责人汇报；

4.3.2火势无法控制时由机房负责人决定报火警请求辖区消防队救援。并在在火灾事故发生后1小时内向所云汇报突发事件信息。速报内容主要包括事故发生的时间、地点、人员伤亡、设备损坏情况、可能的引发因素和发展趋势等。

4.3.3联系方式

消防队：119 医务急救：120

4.4注意事项

4.4.1应急处置时注意防止中毒、窒息、触电、烫伤。

4.4.2危险区设好警戒线，并挂好标示牌。无操作权限的人员不得乱动现场设备。

4.4.3佩戴个人防护器具时注意检查防护用品合格，且在有效检验期内；正确佩戴使用正压式呼吸器、隔热服、隔热手套、绝缘靴等安全防护用具。

4.4.4现场自救和互救时不熟悉现场情况和灭火方法的人员不得盲目进入危险区域，救人前先确认自己的能力和现场情况是否能够满足对他人施救的需要。

4.4.5应急救援结束后要全面检查，确认现场无火灾隐患和建筑物坍塌的隐患。

4.4.6加强自身防护，避免救火导致人身伤害。

4.5附则

4.5.1机房应急人员的联系方式。

信息安全应急预案 篇四

信息发布登记制度

1. 在信源接入时要落实安全保护技术措施，保障本网络的运行安全和信息安全；

2. 对以虚拟主机方式接入的单位，系统要做好用户权限设定工作，不能开放
其信息目录以外的其他目录的操作权限。

3. 对委托发布信息的单位和个人进行登记并存档。

4. 对信源单位提供的信息进行审核，不得有违犯《计算机信息网络国际联网安全保护管理办法》的内容出现。

5. 发现有违犯《计算机信息网络国际联网安全保护管理办法》情形的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告。

信息内容审核制度

一、必须认真执行信息发布审核管理工作，杜绝违犯《计算机信息网络国际联网安全保护
管理办法》的情形出现。

二、对在本网站发布信息的信源单位提供的信息进行认真检查，不得有危害国家安全、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的内容出现。

三、对在BBS公告板等发布公共言论的栏目建立完善的。审核检查制度，并定时检查，防止违犯《计算机信息网络国际联网安全保护管理办法》的言论出现。

四、一旦在本信息港发现用户制作、复制、查阅和传播下列信息的：

1. 煽动抗拒、破坏宪法和法律、行政法规实施

2. 煽动颠覆国家政权，推翻社会主义制度

3. 煽动分裂国家、破坏国家统一

4. 煽动民族仇恨、民族歧视、破坏民族团结

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

7. 公然侮辱他人或者捏造事实诽谤他人

8. 损害国家机关信誉

9. 其他违反宪法和法律、行政法规

10. 按照国家有关规定，删除本网络中含有上述内容的地址、目录或者关闭服务器。并保留原始记录，在二十四小时之内向当地公安机关报告。

用户备案制度

一、用户在本单位办理入网手续时，应当填写用户备案表。

二、公司设专人按照《中华人民共和国计算机信息网络国际联网单位备案表的通知》的要求，在每月20日前，将济南地区本月因特网及公众多媒体通信网（网外有权部分）新增、撤消用户的档案材料完整录入微机，并打印两份。

三、将本月新增、撤消的用户进行分类统计，并更改微机存档资料，同时打印一份。

四、每月20日之前，将打印出的网络用户的备案资料（2份）及统计信息（1份）送至专人处。

安全制度

一、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，提高工作人员的维护网络安全的警惕性和自觉 性。

二、负责对本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。

三、对信息源接入单位进行安全教育和培训，使他们自觉遵守和维护《计算机信息网络国际 互联网安全保护管理办法》，杜绝发布违犯《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。

四、不定期地邀请公安机关有关人员进行信息安全方面的培训，加强对有害信息，特别是影射性有害信息的识别能力，提高防犯能力。

用户登记和管理制度

一、建立健全计算机信息网络电子公告系统的用户登记和信息管理制度；组织学习《计算机信息网络国际联网安全保护管理办法》，提高网络安全员的警惕性；负责对本网络用户进行安全教育和培训；建立电子公告系统的网络安全管理制度和考核制度，加强对电子公告系统的审核管理工作，杜绝BBS上出现违犯《计算机信息网络国际联网安全保护管理办法》的内容。

二、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；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；版主负责检查各版信息内容，如发现违反《计算机信息网络国际互联网安全保护管理办法》即时予以删除，情节严重者，做好原始记录，报告解决，由管理员向公安机关计算机管理监察机构报告；负责考核各版版主，如发现不能正常履行版主职责者，

三、检查时严格按照《计算机信息网络国际互联网安全保护管理办法》、及（见附页）的标准执

行；如发现违犯《计算机信息网络国际互联网安全保护管理办法》（见附页）的言论及信息，即时予以删除，情节严重者保留有关原始记录，并在二十四小时内向当地公安机关报告；负责对本网络用户进行安全教育和培训，网络管理员加强对《计算机信息网络国际互联网安全保护管理办法》的学习，进一步提高对维护的警惕性。

信息安全应急预案 篇五

为了切实做好学校校园网络突发事件的防范和应急处理工作，进一步提高学校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，结合学校工作实际，制定本预案。

一、成立安全应急领导小组

领导小组成员：

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的技能训练，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，使之保持良好的。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。

二、各级处理预案

（一）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，立刻关闭网站。

2.备份不良信息出现的目录、出现时间前后一星期的HTTP连接日志和网络连接日志。

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。

（二）网络恶意攻击事故处理预案

1.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。

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。

（三）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、确定所需要的网络设备及环境。

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，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、以及可能出现事故的影响，在事件过程中出现任何问题应立刻向领导小组组长汇报。

三、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.加强对校园网内的计算机设备的管理，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。

四、网络安全事故发生后有关行动

1.领导小组得悉网络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，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。

五、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，加强演练与熟悉，切实落实各项组织措施。

网络与信息安全应急处置预案 篇六

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各类突发事件的危害和影响，确保信息系统和网络的畅通运行。现结合我局工作实际，特制定本应急预案。

一、总则

（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。

（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。立足安全防护，加强预警，抓好预防、监控、应急处理等环节，采取各种措施，充分发挥各方作用，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，谁运维谁负责”的原则，各部门（单位）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

本预案适用于机关各科室、局属事业单位。

二、组织体系

成立工作领导小组，组长由局长担任，副组长由分管局长担任，组员由各科室、局属事业单位负责人组成。

领导小组下设办公室，办公室设在局综合科，统一协调，负责处理日常工作。

三、预案的启动

在发生网络与信息安全事故时，应根据具体情况启动相应的应急预案。

四、预防预警

（一）信息监测与报告

1、进一步完善网络与信息安全突发公共事件监测、预测和预警制度。落实工作责任制，按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发公共事件和可能引起突发网络与信息安全突发公共事件的有关信息的收集、分析、判断和持续监测。当检查到有网络与信息安全突发公共事件发生时，立即向应急领导小组报告。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建议等。

2、发现下列情况应及时向应急领导小组报告：利用网络从事违法犯罪活动；网络或信息系统通信和资源使用异常；网络或信息系统瘫痪，应用服务中断或数据篡改、丢失；网络恐怖活动的嫌疑和预警信息；其他影响网络与信息安全的信息。

（二）预警处理与发布

1、对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，制止事件的延续、蔓延，并在1小时内进行风险评估，必要时启动相应预案，同时向应急领导小组报告。

2、应急领导小组接到报告后，对可能发生或已经发生的网络与信息安全突发公共事件，迅速召开应急领导小组会议，启动本预案，研究确定处置意见。

3。对需要向上级相关部门通报的，要及时通报，并争取支援。

五、应急响应

（一）先期处置

当我局网络内计算机受到不明估计或恶意入侵时，应立刻关闭网络，并详细备案，同时向应急工作小组组长报告。处理后，应对网络进行查病毒、查木马，检测是否受到攻击，排查事件原因。

领导小组组长接到报告后，应加强与有关方面的联系，掌握最新发展动态，追查原因。对发生重大和有可能演变为重大的网络与信息安全突发公共事件，要立即报告应急领导小组，并做好启动本预案的各项准备工作；应急领导小组在接到报告后，要根据网络与信息安全突发公共事件发展态势，视情况决定是否赶赴现场指挥，组织派遣应急支援力量。

（二）应急指挥

本预案启动后，领导小组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。根据事件性质组建各类应急工作小组，开展应急处置工作，必要时，向相关部门申请应急支援。

（三）信息处理

应急工作小组应对事件进行动态监测、评估，不得隐瞒、缓报、谎报。要做好信息分析、报告和发布工作，及时提供事件动态信息给应急领导小组研究决策。应组织专家和有关技术人员研判各

类信息，研究提出处置措施，完善应急处置计划方案。

六、后期处置

（一）善后处理

在应急处置工作结束后，应急工作小组要迅速采取措施，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。统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建所需的时间、费用等进行分析评估，认真制定恢复重建计划，并迅速组织实施。最后，要将善后处置的有关情况报应急领导小组。

（二）调查评估

应急处置工作结束后，应急工作小组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。

七、保障措施

（一）应急装备保障

对于重要网络与信息系统，在建设系统时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在网络与信息安全突发公共事件发生时，报应急领导小组同意后，由应急工作小组负责统一调用。

（二）数据保障

重要信息系统均应建立容灾备份系统和相关工作机制，保证重要数据在遭到破坏后，可紧急恢复。各容灾备份系统应具有一定的兼容性，在特殊情况下各系统间可互为备份。

八、监督管理

（一）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。

（二）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。

（三）对在网络与信息安全突发公共事件应急处置中作出突出贡献的集体和个人，给予表彰奖励；对在网络与信息安全突发公共事件预防和应急处置中有玩忽职守、失职、渎职等行为，依法依规追究责任。

以上内容就是t7t8美文号为您提供的6篇《信息安全应急预案》，能够给予您一定的参考与启发，是t7t8美文号的价值所在。