# 企业网络安全应急预案(10篇)

来源：网络 作者：梦回江南 更新时间：2024-08-04

*人的记忆力会随着岁月的流逝而衰退，写作可以弥补记忆的不足，将曾经的人生经历和感悟记录下来，也便于保存一份美好的回忆。那么我们该如何写一篇较为完美的范文呢？下面是小编帮大家整理的优质范文，仅供参考，大家一起来看看吧。企业网络安全应急预案篇一（...*

人的记忆力会随着岁月的流逝而衰退，写作可以弥补记忆的不足，将曾经的人生经历和感悟记录下来，也便于保存一份美好的回忆。那么我们该如何写一篇较为完美的范文呢？下面是小编帮大家整理的优质范文，仅供参考，大家一起来看看吧。

**企业网络安全应急预案篇一**

（一）编制目的

提高处置突发事件的能力，促进互联网应急通信、指挥、调度、处理工作迅速、高效、有序地进行，满足突发情况下互联网通信保障应急和通信恢复工作的需要，维护企业利益，为保障生产的顺利进行创造安全稳定可靠的网络环境。

（二）编制依据

《中华人民共和国电信条例》、《国家通信保障应急预案》、《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《非经营型互联网信息服务备案管理办法》、《互联网ip地址资源备案管理办法》和《中国互联网域名管理办法》等有关法规和规章制度。

设立信息网络安全事故应急指挥小组，负责信息网络安全事故的组织指挥和应急处置工作。总指挥由主要领导担任，副总指挥由分管领导担任，指挥部成员由信息中心运行。

（一）危险源分析及预警级别划分

1.1危险源分析

根据网络与信息安全突发公共事件的发生过程、性质和机理，网络与信息安全突发公共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，网络精英攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

2.2预警级别划分

1、预警级别划分

根据预测分析结果，预警划分为四个等级:ⅰ级（特别严重）、ⅱ级（严重）、ⅲ级（较重）、ⅳ级（一般）。

ⅰ级（特别严重）：因特别重大突发公共事件引发的，有可能造成整个学校互联网通信故障或大面积骨干网中断、通信枢纽设备遭到破坏或意外损坏等情况，及需要通信保障应急准备的重大情况；通信网络故障可能升级为造成整个学校互联网通信故障或大面积骨干网中断的情况。计算机房发现火情或其他重大自然灾害或存在重大自然灾害隐患的。

ⅱ级（严重）：因重大突发公共事件引发的，有可能造成学校网络通信中断，及需要通信保障应急准备的情况。

ⅳ级（一般）：因一般突发公共事件引发的，有可能造成局域网内某个交换点所属局部网通信故障（不影响正常一般通信）的情况。

（二）预防机制

信息网络安全事故应急指挥小组应加强对各级通信保障机构及全网通信网络安全防护工作和应急处置工作的监督检查，保障通信网络的安全畅通。

（三）预警监测

各重要信息系统重要负责人和主管科室要进一步完善网络与信息安全突发公共事件监测、预测、预警制度。要落实责任，制定信息通报工作制度。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公共事件和可能引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。

（四）先期处置

当发生网络与信息安全突发公共事件时，发现事故的人员在按规定向相关系统管理员报告的同时，及时向信息网络安全事故应急指挥小组相关领导报告。负责人员在接手事故报告后要向信息网络安全事故应急指挥小组进行应急工作进程报告和事故分析报告。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等。

（一）应急处置分级和应急处置程序

突发事件发生时应急通信保障工作和通信恢复工作，按照快速、机动、灵活的原则，根据响应的预警级别分别进行处置。

ⅰ级：突发事件造成全学校通信故障或大面积骨干网中断、通信枢纽设备遭到破坏等情况，及接到学校下达的通信保障任务，由信息网络安全事故应急指挥小组负责组织和协调。负责人员要迅速准确的定位故障源，如果是核心设备故障要及时切换到备用核心设备上并测试调通；如果是骨干网物理链路故障要第一时间通知相关部门（通信公司）进行抢修并切换到备用线路上测试调通。面对网络精英攻击或恶意破坏等人为造成的网络故障，要及时通知公安机关，同时采取紧急行动如切断数据源等将损失控制在最小范围。对于发现的重大自然灾害隐患，要及时汇报信息网络安全事故应急指挥小组并迅速通知消防局等相关部门，准备好临时处理灾情需要用到的工具。火灾属于常见灾情，发现火情后按如下步骤处置：

（1）发现火情要立即切断电源，值班员及时应用消防器材进行处理。

（2）立即上报领导做好事故处理记录。

（3）如切断电源并使用机房消防器灭火都不能控制火情，要及时报警（报警电话：119），报警时要准确说清火灾的地点和火灾状况，并留下联系电话。

（4）出现危急情况要利用各种手段及时逃生。

ⅱ级：突发事件造成本学校多个下属分公司网络通信中断或接到学校有关部门下达的通信保障任务时，由信息网络安全事故应急指挥小组负责组织和协调。负责人员要迅速准确的定位故障源，如果是关键部位网络设备故障要及时切换到备用设备上并测试调通；如果是骨干网物理链路故障要第一时间通知相关部门（通信公司）进行抢修并切换到备用线路上测试调通。如果是业务系统发生故障按如下办法处置：

二、趋势防病毒服务器：

1、当趋势防病毒服务器出现以下情况时，值班员应负责重启趋势防病毒服务器

（1）双击ie安装页面，出现“该页无法显示”时。

（2）大量用户申告客户端无法连接服务器。

2、重启服务器后系统仍然不能正常应用，则立即通知系统管理员，并及时做好故障现象及处理过程记录。

3、当系统管理员经过一小时处理仍未排除故障时，应通知科长协调处理。

（二）应急保障任务结束

事故现场得以控制，网络环境符合有关标准，导致次生、衍生事故隐患消除后可确认网络通信保障和通信恢复应急工作任务完成。由信息网络安全事故应急指挥小组下达解除任务通知书，现场应急指挥机构收到通知书后，任务正式结束。

（三）调查、处理、后果评估与监督检查

信息网络安全事故应急指挥小组负责对重大通信事故原因进行调查、分析和处理，对事故后果进行评估，并对事故责任处理情况进行监督检查。

（四）信息发布

信息网络安全事故应急指挥小组负责有关信息的发布工作。

（五）通讯

在突发事件的应急响应过程中，要确保应急处置系统内部机构之间的通信畅通。通信联络方式主要采用固定电话、移动电话、卫星电话。

五、后期处置

（一）情况汇报和经验总结

在突发事件应急响应过程中，信息网络安全事故应急指挥小组应做好突发事件中网络设施损失情况的统计、汇总、原因分析、应急处置情况总结等，并按程序上报。如有需要维护修理的设备要及时处理。

（二）奖惩评定及表彰

为提高通信保障应急工作的效率和积极性，对于在应对突发事件过程中表现突出的单位和个人应给予通报表扬；对保障不力，给企业造成损失的单位和个人按有关规定进行处理。

六、保障措施

（一）物资保障

信息网络安全事故应急指挥小组应建立必要的通信保障应急资源的保障机制，根据通信保障应急工作要求，配备必要的通信保障应急装备，加强对应急资源及装备的管理、维护和保养，以备随时紧急调用。

（二）人员保障

通信保障应急队伍主要由信息中心相关人员组成。信息网络安全事故应急指挥小组人员要不断提高自身专业水平并听从组长的指挥。

（三）宣传、培训和演习

信息网络安全事故应急指挥小组应加强对通信网络安全和通信保障应急的宣传教育工作，定期或不定期地对信息网络安全事故应急指挥小组主要技术人员进行技术培训和应急演练，保障应急预案的有效实施，不断提高通信保障应急的能力。

（五）通信保障应急工作监督检查制度

信息网络安全事故应急指挥小组应加强对通信保障应急工作的监督和检查，做到居安思危、常备不懈。

3、经费保障

由信息网络安全事故应急指挥小组根据通信应急保障需要，提出项目支出预算申请，报学校批准后执行。

一、信息中心配备诺顿企业版网络防火墙软件和防病毒软件，及时升级，及时清除杀灭网络病毒，一旦发生黑客入侵事件，部署的入侵检测系统（ids），将向管理员发出警报，管理员将在第一时间处理黑客入侵事件，并报有关部门。

二、对来往电子邮件及网络下载文件用防病毒软件过滤，确保不被木马类黑客病毒侵入并在无意中协助传播病毒。一旦发生类似冲击波、震荡波等类似的网络蠕虫风波，管理员将在第一时间升级病毒防火墙，给系统打布丁，防止病毒的恶意破坏。

三、信息中心对服务器重要信息定时做好备份，提高信息存储安全应急响应能力。一旦发生严重的因黑客、病毒侵入，造成网络无法正常运行时，管理员将在第一时间恢复服务器备份，保证网络的正常运行。

四、管理员对定期检查的运转情况，做好设备维护纪录，保证设备高效稳定的运行。一旦服务器出现硬件设备故障，管理员将在第一时间启用备份服务器，保证网络的正常运行，并对原服务器进行及时的检修，在修复后将替换备份服务器继续运行，保证网络的正常运行。一旦其它网络设备出现故障，管理员将在第一时间用备件替换故障设备，保证网络的正常运行。

五、定期升级操作系统补丁程序，配备顿企业版网络防火墙软件和防病毒软件，及时升级，及时清除杀灭网络病毒，防止被他人恶意侵入。对来往电子邮件及网络下载文件用防病毒软件过滤，不运行可疑程序，确保不被木马类黑客病毒侵入并在无意张协助传播病毒。

六、学校严格控制网络信息密码、管理权限、知情范围，妥善管理密码，并按照满足需求、方便使用、加强管理的原则，进一步完善密码管理制度，建立健全适应教育信息化发展的科学的密码管理体系。

七、凡是上网人员，都能通过防火墙记录在日志里，日志的保留时间为3个月。关闭一些反动、不健康的网站，保障了校园文化的干净。在邮件系统方面，我们安装了第三方插件，能起到过滤关键字的作用。信息中心对服务器重要信息定时做好备份，提高信息存储安全应急响应能力。并定期检查设备的运转情况，做好设备维护记录，保证设备高效稳定的运行。

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、发生计算机硬件（系统）故障、通信线路中断、路由故障、流量异常等，网络管理员经初步判断后应立即上报应急领导小组组长，由应急领导小组组长通知做好各部门做好检测车辆的场内秩序维护工作；

（1）、属于计算机硬件（系统）故障；就立即组织电脑公司技术人员进行抢修，属于计算机系统问题的应第一时间利用备份系统进行系统还原操作；还原操作无效的，如无大面积计算机停机现象，应排除隐患，除待处理的检测线外，立即逐步恢复能正常工作的检测线工位机、计算机，尽快恢复车辆检测工作；

（2）、属于计算机网络连接问题的，能通过拉接临时线解决的，应立即拉接临时线缆，再逐步查找连接故障；由于连接交换机故障的，应立即更换上备用交换站；站内各部门有义务配合网络管理员做好排故工作；

（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。

（4）、由网络攻击或病毒、木马等引起的网络堵塞等现象，应立即拨掉网线，将故障计算机（服务器）脱离网络，并关闭计算机后重新开机，下载安装最新的杀毒软件对故障计算机逐一进行杀毒处理；对连接交换进行断电处理；

（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。

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。

适用范围，预案适用于公司接入互联网的服务器，虚拟主机以及内部工作电脑等信息系统上的突发性事件的应急工作。

在公司发生重大突发公共事件或者自然灾害或上级部门通知时，启动本应急预案，上级有关部门交办的重要互联网通讯保障工作。那原则上要统一领导，统一指挥，分类管理，分级负责，严密组织，协作配合，预防为主，防处结合，发挥优势，保障安全。应急领导小组，公司信息管理总监，运行维护经理以及网络管理员组成的网络安全应急处理小组。

领导小组我主要职责加强领导，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。

充分利用各种渠道进行网络安全知识的宣传教育，组织直到集团网络安全常识的普及教育，广泛开展网络安全和有关技能的训练，不断提高公司员工的防范意识和基本技能。人生做好各项物资保障，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。要采取一切必要手段，组织各方面力量，全面进行网络安全事故处理工作，将不良影响和损失降到最低点。

调动一切积极因素，全面保障和促进公司网络安全稳定的运行。

灾害发生之后，网络管理员判定灾害级别抽波，估计灾害造成的损失，保留相关证据，并且在十分钟内上报信息管理总监，由信息管理总监决定是否请启动应急预案。一旦启动应急预案，信息管理中心运行维护组进行应急处置工作状态，阻断网络连接，进行现场保护协助。调查取证和系统恢复等工作，对相关事件进行跟踪，密切关注事件动向，协助调查取证有关违法事件移交公安机关处理。处置措施，网站不良信息事故处理医院一旦发现公司网站上出现不良信息，或者是被黑客攻击，修改了网页，立即关闭网站。

**企业网络安全应急预案篇二**

校园网络安全管理应急预案

一、信息中心配备诺顿企业版网络防火墙软件和防病毒软件，及时升级，及时清除杀灭网络病毒，一旦发生黑客入侵事件，部署的入侵检测系统（ids），将向管理员发出警报，管理员将在第一时间处理黑客入侵事件，并报有关部门。

二、对来往电子邮件及网络下载文件用防病毒软件过滤，确保不被木马类黑客病毒侵入并在无意中协助传播病毒。一旦发生类似冲击波、震荡波等类似的网络蠕虫风波，管理员将在第一时间升级病毒防火墙，给系统打布丁，防止病毒的恶意破坏。

三、信息中心对服务器重要信息定时做好备份，提高信息存储安全应急响应能力。一旦发生严重的因黑客、病毒侵入，造成网络无法正常运行时，管理员将在第一时间恢复服务器备份，保证网络的正常运行。

四、管理员对定期检查的运转情况，做好设备维护纪录，保证设备高效稳定的运行。一旦服务器出现硬件设备故障，管理员将在第一时间启用备份服务器，保证网络的正常运行，并对原服务器进行及时的检修，在修复后将替换备份服务器继续运行，保证网络的正常运行。一旦其它网络设备出现故障，管理员将在第一时间用备件替换故障设备，保证网络的正常运行。

五、定期升级操作系统补丁程序，配备顿企业版网络防火墙软件和防病毒软件，及时升级，及时清除杀灭网络病毒，防止被他人恶意侵入。对来往电子邮件及网络下载文件用防病毒软件过滤，不运行可疑程序，确保不被木马类黑客病毒侵入并在无意张协助传播病毒。

六、学校严格控制网络信息密码、管理权限、知情范围，妥善管理密码，并按照满足需求、方便使用、加强管理的原则，进一步完善密码管理制度，建立健全适应教育信息化发展的科学的密码管理体系。

七、凡是上网人员，都能通过防火墙记录在日志里，日志的保留时间为3个月。关闭一些反动、不健康的网站，保障了校园文化的干净。在邮件系统方面，我们安装了第三方插件，能起到过滤关键字的作用。信息中心对服务器重要信息定时做好备份，提高信息存储安全应急响应能力。并定期检查设备的运转情况，做好设备维护记录，保证设备高效稳定的运行。

**企业网络安全应急预案篇三**

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。

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。

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。

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。

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。

**企业网络安全应急预案篇四**

为切实做好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，确保我局网络与信息安全，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联网安全保护管理办法》等有关法规文件精神，结合我局实际情况，特制定本应急预案。

认真落实“教育在先，预防在前，积极处置”的工作原则，牢固树立安全意识，提高防范和救护能力，以维护正常的工作秩序和营造绿色健康的网络环境为中心，进一步完善网络管理机制，提高突发事件的应急处置能力。

成立计算机信息系统安全保护工作领导小组

组长：\_\_

副组长：\_\_

成员：\_\_

主要职责：负责召集领导小组会议，部署工作，安排、检查落实计算机网络系统重大事宜。副组长负责计算机网络系统应急预案的落实情况，处理突发事故，完成局领导交办的各项任务。

1.负责人：\_\_

2.信息安全技术人员：\_\_

1.各处室要加强对本部门人员进行及时、全面地教育和引导，提高安全防范意识。

2.网站配备信息审核员和安全管理人员，严格执行有关计算机网络安全管理制度，规范办公室、计算机机房等上网场所的管理，落实上网电脑专人专用和日志留存。

3.信息所要建立健全重要数据及时备份和灾难性数据恢复机制。

4.采取多层次的有害信息、恶意攻击防范与处理措施。各处室信息员为第一层防线，发现有害信息保留原始数据后及时删除；信息所为第二层防线，负责对所有信息进行监视及信息审核，发现有害信息及时处理。

5.切实做好计算机网络设备的防火、防盗、防雷和防信号非法接入。

6.所有涉密计算机一律不许接入国际互联网，做到专网、专机、专人、专用，做好物理隔离。

**企业网络安全应急预案篇五**

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。

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。

（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。

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。

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。

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。

**企业网络安全应急预案篇六**

我校为有序引导，有效预防、减少和消除突发重大舆情造成的负面影响，切实提升应对网络等媒体的能力，依据已有相关规定，特制定本预案。

(一）统一领导，统筹组织。将突发重大舆情应对处置工作纳入我校应急管理工作统筹安排，成立专门领导小组加强组织协调。

(二）分级负责，依法处置。按照谁主管谁负责的原则，依法依规组织实施突发重大舆情应对处置工作和应急处置工作。

(三）监测预警，及早防范。及时发现和掌握社会及互联网上动态性、苗头性和预警性信息，加强分析研判，有针对性地采取防范和控制措施，及时预防和消除不良影响。

(一)领导机构及职责

成立许昌实验中学突发重大舆情应急处置工作领导小组，负责审定我校突发重舆情应急处置预案、工作方案并组织实施；督导、考核有关单位突发重大舆情应急处置工作，研判“网络问政”形势，有序引导舆论。学校宣传科负责舆情处理，电教网络中心负责提供技术支持。

(二）岗位职责

宣传科：统筹协调有关单位落实突发重大舆情应急处置工作及其他相关工作。

各相关科室：负责组织实施本科室突发重大舆情的应急处置工作。建立舆情监管机制，在单位干部职工中培养一批政治素质高、责任心强、懂政策法规、善应对网络的网民队伍，确保一旦发生重大舆情能够得到及时有效处置。有技术上问题的及时与电教网络中心联系。

(一)研判预警

对学校可能引发重大舆情的突发事件、热点敏感问题，要及时搜集掌握有关真实信息，做好应对处置准备，增强工作前瞻性和时效性。

(二）快速反应

发现重大舆情后，要按照应急管理规定时限及时将情况报告学校宣传科，同时立即启动应急预案，组建专门工作组，制定并落实应急处置措施，于发现后三小时内以单位或网络新闻发言人的名义跟帖依法依规告知事实真相、事件处置情况或答疑释惑，及时、有效控制事态，正面、有序引导网络舆论。在应急处置过程中，要及时续报有关情况。

(三）分类处置

对网络媒体出现的突发重大舆情，在严格执行保密法律法规、新闻宣传纪律等规定的基础上，按以下办法分类处置：

1.对于询问、置疑、诉求类的，学校及时提出答复意见，能当即回复的要当即回复， 需要一段时间办理后才能回复的，要在发现当日内回复处理意见并在办结之日内回复处理结果。

2.对某一突发事件或社会热点、敏感问题恶意传播或炒作类的，要依法告知事实真相或事件处置情况；对于造成重大负面影响或严重损失，告知事实真相、事件处置情况后仍继续恶意传播或炒作的，商请执纪执法部门依纪依法查处。

3.对于捏造、歪曲或夸大事实，恶意攻击、诽谤，煽动网民闹事或涉嫌网上违法犯罪活动类的，要依法澄清事实真相，并商请执纪执法部门依纪依法查处。

4.对推动改革、发展、稳定工作有重要积极意义类的，要积极采纳建议并按要求予以回复。

(四）动态跟综

专人负责对突发重大舆情及处置后的事态实行动态跟踪，适时釆取应对处置措施，坚决防止网络舆情危机发生。

(五）总结评估

在网络舆情被消除或趋于平稳后，要根据舆情的发生、传播和处置情况及时进行总结、梳理、反思，将应对处置工作书面报告上报市教育局，并健全完善工作机制，不断提高应对网络媒体的能力。对玩忽职守、造成严重损失的，要报公安机关依法给予责任人行政处分，违反法律的，依法追究法律责任。

为快速妥当处置全市民族宗教突发重大网络舆情，有序引导网络舆论，有效预防、减少和消除突发重大网络舆情造成的负面影响，切实提升应对网络媒体的能力，营造我市民族宗教良好网络舆论环境，依据有关规定，制定本预案。

一、适用范围

本《预案》适用于我市民族宗教系统被国内外网络媒体登载舆情信息，或对本系统正常工作秩序可能产生重大影响的相关信息等突发网络舆论情况的应对处置工作。

二、工作原则

（一）统一领导，统筹组织。将突发重大网络舆情应对处置工作纳入全市民族宗教系统应急管理工作统筹安排，成立专门领导小组加强组织协调。

（二）分级负责，依法处置。按照辖区负责和谁主管谁负责的原则，依法依规组织实施突发重大网络舆情应对处置工作和应急处置工作。

（三）监测预警，及早防范。建立网络信息监测、报告、通报制度，及时发现和掌握互联网上动态性、苗头性和预警性信息，加强分析研判，有针对性地采取防范和控制措施，及时预防和消除不良影响。

（四）服务发展，防止危机。立足于服务发展、保障民生、维护稳定，采取法律、管理、技术、舆情疏导等综合措施加强突发重大网络舆情应对处置工作，有效防止网络舆情危机发生。

三、组织体系及工作职责

（一）领导机构及职责

成立市民族宗教系统突发重大网络舆情应急处置工作领导小组，由主要领导任组长，分管办公室工作的领导任副组长，有关科室主要负责人为成员，主要负责审定全市民族宗教系统突发重大网络舆情应急处置预案、工作方案并组织实施；督导、考核有关单位突发重大网络舆情应急处置工作，研判“网络问政”形势，有序引导网络监督。领导小组下设办公室于机关办公室，负责日常工作。

（二）主要职责

办公室：统筹、协调有关单位落实突发重大网络舆情应急处置工作及其他相关工作。

各科室：负责组织实施本单位突发重大网络舆情的应急处置工作。

四、处置程序及办法

（一）研判预警

各科室对所可能引发重大网络舆情的突发事件、热点敏感问题，要及时搜集掌握有关真实信息，做好应对处置准备，增强工作前瞻性和时效性。

（二）快速反应

各科室发现重大网络舆情后，应立即向重大网络舆情应急处置工作领导小组办公室报告,最迟不得超过2小时,同时向有关部门通报。应急处置过程中,要及时续报事件处置进展和可能衍生的新情况。紧急情况下，可电话口头报告突发事件信息，并在30分钟内报送书面信息。在重大网络舆情应急处置过程中，要及时续报有关情况。

（三）分类处置

对网络媒体出现的突发重大网络舆情，在严格执行保密法律法规、新闻宣传纪律等规定的基础上，按以下办法分类处置：

1、属询问、置疑、诉求类的，安排相关科室、直属单位依法依规进行办理、提出答复意见，经各科室和直属单位负责人审定后统一回复；能当即回复的要当即回复，需要一段时间办理后才能回复的，要在发现当日内回复处理意见并在办结之日内回复处理结果。

2、属对某一突发事件或社会热点、敏感问题恶意传播或炒作类的，要依法告知事实真相或事件处置情况；对于造成重大负面影响或严重损失，告知事实真相、事件处置情况后仍继续恶意传播或炒作的，商请执纪执法部门依纪依法查处。

3、属捏造、歪曲或夸大事实，恶意攻击、诽谤，煽动网民闹事或涉嫌网上违法犯罪活动类的，要依法澄清事实真相，并商请监察执法部门依纪依法查处。

4、属对推动改革、发展、稳定工作有重要积极意义类的，要积极采纳建议并按要求予以回复。

（四）动态跟踪

各相关科室、二级单位要落实专人对突发重大舆情及处置后的事态实行动态跟踪，适时采取应对处置措施，坚决防止网络舆情危机发生。

（五）总结评估

在网络舆情被消除或趋于平稳后，各相关科室和二级单位要根据舆情的发生、传播和处置情况及时进行总结、梳理、反思，将应对处置工作书面报告三日内报送办公室，并健全完善工作机制，不断提高应对网络媒体的能力。

五、工作保障

各科室和二级单位指定专门的舆情监控人员，建立网络舆情监管机制，在单位干部职工中培养一批政治素质高、责任心强、懂政策法规、善应对网络的网民队伍，确保一旦发生重大网络舆情能够得到及时有效处置。

六、责任追究

重大网络舆情应急处置工作实行行政领导负责制和责任追究制。各科室、二级单位应当建立健全奖励及责任追究机制，对迟报、漏报、谎报和瞒报突发事件重要情况或者应急处置工作中有其他失职、渎职行为的，依法对有关责任人给予行政处分，构成犯罪的，依法追究刑事责任；对突发事件应急处置工作中作出突出贡献的集体和个人，应给予表彰和奖励。

为快速妥当处置市档案局(馆)突发重大网络舆情，有序引导网络舆论，有效预防、减少和消除突发重大网络舆情造成的负面影响，切实提升应对网络媒体的能力，营造建设文化强市的良好网络舆论环境，依据有关法律法规，制定本预案。

一、适用范围

本《预案》适用于市、区县档案局(馆)被国内外网络媒体登载有对本地区经济发展、社会稳定、公共安全、人民群众生产生活可能产生重大影响的档案方面信息，或对本单位正常工作秩序可能产生重大影响的相关信息等突发网络舆论情况的应对处置工作。

二、工作原则

(一)统一领导，统筹组织。将突发重大网络舆情应对处置工作纳入全市档案系统应急管理工作统筹安排，成立专门领导小组加强组织协调。

(二)分级负责，依法处置。按照辖区负责和谁主管谁负责的原则，依法依规组织实施突发重大网络舆情应对处置工作和应急处置工作。

(三)监测预警，及早防范。建立网络信息监测、报告、通报制度，及时发现和掌握互联网上动态性、苗头性和预警性信息，加强分析研判，有针对性地采取防范和控制措施，及时预防和消除不良影响。

(四)服务发展，防止危机。立足于服务发展、保障民生、维护稳定，采取法律、管理、技术、舆情疏导等综合措施加强突发重大网络舆情应对处置工作，有效防止网络舆情危机发生。

三、组织体系及工作职责

(一)领导机构及职责

成立黄山市档案系统突发重大网络舆情应急处置工作领导小组，由局党组书记、局长任组长，分管安全工作的领导任副组长，各区县档案局(馆)、局机关各科室主要负责人为成员，主要负责审定全市档案系统突发重大网络舆情应急处置预案、工作方案并组织实施;督导有关科室突发重大网络舆情应急处置工作，研判“网络问政”形势，有序引导网络监督。领导小组下设办公室于市局科教编研科，负责日常工作。

(二)主要成员单位职责

市局科教编研科:统筹、协调有关单位落实突发重大网络舆情应急处置工作及其他相关工作。

各县(区)档案局(馆):负责组织、协调、督导本单位突发重大网络舆情的应急处置工作。

四、处置程序及办法

(一)研判预警

对本单位可能引发重大网络舆情的突发事件、热点敏感问题，要及时搜集掌握有关真实信息，做好应对处置准备，增强工作前瞻性和时效性。

(二)快速反应

发现重大网络舆情后，要按照应急管理规定时限和逐级报告、双重报告等要求，及时将情况报告市局科教编研科，由市局科教编研科报告分管领导、主要领导。同时立即启动应急预案，组建专门工作组，制定并落实应急处置措施，于发现后三小时内以单位或网络新闻发言人的名义跟帖依法依规告知事实真相、事件处置情况或答疑释惑，及时、有效控制事态，正面、有序引导网络舆论。在应急处置过程中，要及时续报有关情况。

(三)分类处置

对网络媒体出现的突发重大网络舆情，在严格执行保密法律法规、新闻宣传纪律等规定的基础上，按以下办法分类处置:

1、属询问、置疑、诉求类的，安排相关职能科(股)室位依法依规进行办理、提出答复意见，经各县(区)局负责人审定后统一回复;能当即回复的要当即回复，需要一段时间办理后才能回复的，要在发现当日内回复处理意见并在办结之日内回复处理结果。

2、属对某一突发事件或社会热点、敏感问题恶意传播或炒作类的，要依法告知事实真相或事件处置情况;对于造成重大负面影响或严重损失，告知事实真相、事件处置情况后仍继续恶意传播或炒作的，商请执纪执法部门依纪依法查处。

3、属捏造、歪曲或夸大事实，恶意攻击、诽谤，煽动网民闹事或涉嫌网上违法犯罪活动类的，要依法澄清事实真相，并商请执纪执法部门依纪依法查处。

4、属对推动改革、发展、稳定工作有重要积极意义类的，要积极采纳建议并按要求予以回复。

(四)动态跟踪

落实专人对突发重大舆情及处置后的事态实行动态跟踪，适时采取应对处置措施，坚决防止网络舆情危机发生。

(五)总结评估

在网络舆情被消除或趋于平稳后，根据舆情的发生、传播和处置情况及时进行总结、梳理、反思，将应对处置工作书面报告报送市局科教编研科，并健全完善工作机制，不断提高应对网络媒体的能力。

五、工作保障

要配备必要的设施设备和网管技术人员，保障必要的工作经费，建立网络舆情监管机制，在单位干部职工中培养一批政治素质高、责任心强、懂政策法规、善应对网络的网民队伍，确保一旦发生重大网络舆情能够得到及时有效处置。

一、突发舆情事件应对的基本方法

1.快速及时的回应舆论关切问题：在这个过程中，需要明确回应责任，通过线上（官微、官博、官网）与线下（发布会）相结合的方式及时回应，双管齐下，消解舆情热度。

2.利用网络媒体，抢占舆论制高点：在第一时间回应舆论关切问题后，还应该加强与网络媒体的合作，有助于提升对外发布信息的权威和说服力。

3.把握舆情关注重点：主要目的在于发布的信息要尽可能的满足网民的关注点，在这个过程中可以利用一些网络舆情监测系统，对舆情进行实时的跟踪监测，把握舆情态势。

4.尊重网络舆情传播规律：舆情删除是不现实的，要善于利用网络传播规律然后积极的引导舆情，如引导网络舆论转移关注点、发布与传递一些正面的声音等。

5.积极寻找网络意见领袖：这种网民引导网民，用网民自己的声音进行引导、感染网民，实现网民自我教育、自我引导的方式，在舆情引导的过程中可以达到事半功倍的效果。

二、突发舆情事件处置办法

由于网络舆情传播速度快，传播载体众多，在应对突发舆情的过程中，时效性很重要。为此，通过采购舆情监测公司的网络舆情监测系统加强网上舆情监控，以及时发现舆情信息并监测舆情的发展趋势，已成为突发舆情事件处置的主要解决办法。

以识微商情这样的网络舆情监测系统为例，可对全网舆情进行实时监控，及时发现舆情信息并监测舆情的发展趋势，负面舆情自动识别第一时间告警通知，挖掘舆情传播演化过程中的传播网站、传播媒体、关键传播节点以及传播溯源、网民情感分析等，自动生成舆情分析统计图表简报，供突发舆情事件应对工作决策参考。

为认真落实县委关于加强意识形态工作的一系列部署，增强政治意识、大局意识、核心意识、看齐意识，加强网络舆情处置工作的规范化、制度化建设，及时回应网民关切问题，有序化解网络舆论危机，有效预防、缩小和消除网络舆情造成的负面影响，切实维护社会和谐稳定，特制定本预案。

一、适用范围

本预案适用于各类敏感网络舆情的处置工作。

二、工作原则

1、快速反应，妥善处置。要第一时间发现、研判、处置网络舆情。要坚持“双处置”，即网下网上同步处置，网下治本、网上治标，积极解决自身存在的现实问题，积极妥善做好社会舆论层面的回应。要按照“三同步”的原则，切实做到事情应急与新闻应急同步部署、处置工作和对外发布同步研究、处置授权与发布授权同步安排。

2、分级响应，有序应对。根据网络舆情可能造成社会影响的大小，针对不同等级的奧情，坚持分级应对的原则， 采取不同应对措施，提高效率，注重效果。

三、组织体系

成立重大意识形态舆情事件应急处置工作领导小组(以下简称领导小组)，组成人员如下:

组 长:\_\_

副组长:\_\_

成员:各科室主要负责人

领导小组下设办公室，办公室主任由王加志同志兼任,具体负责网络舆情的监测、研判、提出处置建议。

四、应对方案

(一)应对原则

1、黄金24小时法则。力争第一时间发布新闻，赢得话语权。信息要真实透明，报道要统一开放，沟通要亲民坦诚。

2、信息公开原则。新闻发言人要充分发挥媒体优势,根据网民的质疑和提出的问题，有节奏地抛出系统化的专业信息，不断引导民众舆论。

3、主动沟通原则。突发事件中，要主动组织与积极策划新闻宣传活动，邀请第三方媒体(地方电视台、权威专业纸媒或网站等)及时发布信息，主动与民众沟通并适时进行权威讨论，通过释疑贏得公众信任。

(二)重要措施

1、启动新闻发言人机制。新闻发言人应选择熟悉媒体运作，具有丰富的公关宣传经验的工作人员，在突发事件应对处置中，根据必要性，有计划分阶段地开展新闻发布会，或者联系媒体接受专题采访等方式主动回应。

2、培养和发挥意见领袖的舆论影响力。通过内部培养、外部挖掘，寻找懂业务、新闻素养高的专业媒体人士，作为领域内意见领袖。在突发事件应对中，由意见领袖在论坛、微博等舆论活跃地带设置话题，发布专业、权威、客观的评论性内容，引导负面情绪趋于平和与理性。

3、完善网络舆情信息员制度。各科室配备一名舆情信息员，实时监控舆论发展动向，负责舆情信息的采集上报工作。

4、适时利用第三方成员应对舆论震荡。在网络平台设置议题后，可组织网络水军发布价值性评论、回帖，扭转“一边倒”的敌我情势。

(三)具体方法

1、迅速调查核实，及时上报，积极沟通。迅速组织调查，核查事实，及时上报县委党政办。同时，组织涉事各方加强内外部沟通。

2、适时跟贴回应。全面监控以“网易、搜狐、新浪、搜狐、凤凰网”为核心的商业门户网站和以天涯论坛为首的全国和地方综合性论坛，着重观察负面舆论的发展动向，发现舆论发酵的苗头，及时主动应对，由涉事主体迅速组织人员(意见领袖、网络信息员、网络水军),统一口径，以第三者身份更贴回应，放大正面声音，稀释负面影响。

3、快报事实，慎填原因，重报进展。快报事实，即在着重解决线下现实问题的同时，通过政务微博、微信和手机报等渠道，第一时间告知事实。慎报原因，即不仅要基于严格、全面和深入的调查，还要注重原因公布的时间选择，过早易引发群众的不信任感，过晚会有“执行不力”之嫌。重报进展，即通过上述“两微一端”或第三方媒体介入，阶段性公布调查和解决实况，助推舆论平复。

4、对不实贴文，即刻上报，对相关网站迅速采取有效惜施进行管控，消除负面影响。同时，可邀请主流媒体采访，正面回应网民关切。

5、对诽谤、造谣等涉嫌违法违规信息，报请公安机关衣法处置。

6、主动设置议题。在领导小组的统一指导下，认真分析研判，紧扣网民关心的热点、焦点问题，设置相关议题(着重选择事实澄清、主体问责、权威观点等话题范围),组织网络宣传，化解网上疑虑，有序引导网络舆论。

五、处置流程

结合实际，整合资源，互动融合，灵活处置，有效化解舆情情危机。

（一）全面监测

采取人工和技术相结合、网上与网下相结合的方式，对重点领域、重要人物、重大事件进行24小时检测，确保第一时间发现舆情。

(二)研判预警

对发现的舆情，各涉事主体要迅速对舆情走势、风险级别进行评估，及时报告党政办、上级业务部门和同级网信部门。特别重大舆情务必1小时内上报，重大舆情务必2小时内上报，较大和一般舆情酌情适时上报。

(三)分级处置

1、一般网络舆情。指网民在网络论坛/社区、微博、维权网站等平台对某项政策或某类问题进行询问、提出质疑、表达诉求，仅有少量围观的舆情(阅读量、跟帖量、舆情总量等均在50篇/条),且未有主流媒体(电视、报刊)介入报道，评论量也是零星分布，由涉事主体及时解决网民诉求，回应网民关切。

2、较大网络舆情。指涉及有损\_\_县形象的敏感信息在不同网站出现的(阅读量、跟帖量、舆情总量等均在100-500篇/条),评论量也有数十条，且负面声音有所上升，

发酵趋势明显的舆情。由涉事主体密切关注，及时调查核实，

及时跟帖回应，妥善处置。

3、重大网络舆情。指涉及重点领域、重要节点、重要事件、重要人物的敏感信息迅速发酵，或有主流媒体(电视、报刊等)介入报道，可能造成重大影响的舆情。由派出所及时提请领导小组研究制定奥情处置方案，组织网上网下同时实施，及时有效化解网上危机。

4、特别重大网络舆情。指突发事件引起的、严重影响社会稳定、扰乱社会秩序、造成重大负面影响的舆情(安全生产过程中发生人员伤亡等)。在党政办统一协调下，分级响应，及时有效处置。

(四)舆论引导

按照“及时准确、公开透明、有序开放、有效管理、正确引导”和“攻防兼备、疏堵结合”的原则，主动设置议题，第一时间发布信息，认真回应质询议题，适时进行权威评论、积极开展民意互动，根据舆论形势、事件进展等情况，采取“新闻发布会”“背景说明会”“组织记者集体采访或单独采访”“发布新闻公报、声明”“利用电话、传真、电子邮件答记者问询”等形式，通过新闻发言人专业、快速、准确地引导网上舆论，减少和消除负面影响。

**企业网络安全应急预案篇七**

校园网络安全管理事故应急预案

1、多媒体专用教室及其它配有计算机设备的教室、办公室。

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。

**企业网络安全应急预案篇八**

为贯彻落实中央、省、市有关网络安全工作的精神，进一步完善我局网络安全保障体系，切实提高网络安全防护能力和水平，根据《福州市审计局关于进一步加强网络安全工作的意见》，结合我局实际，制定应急预案如下：

（一）指导思想

为保障我局网络和信息安全，预防和遏制网络突发事件的发生，消除突发事件造成的危害和影响，根据有关要求，按照“统一领导、统一指挥、各司其职、整体作战、保障安全”的原则，建立健全信息安全应急响应机制，有效预防和及时控制网络安全事件的危害和影响，制定我局的网络信息安全应急处置预案。

本预案以《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》《国家网络安全事件应急预案》和《福建省审计厅网络安全事件应急预案》等为指导思想，总结工作中行之有效的经验，以构建预防为主、防治结合的网络信息安全长效管理与应急处理机制为根本，以保证系统安全稳定运行为目标，努力将网络安全工作纳入制度化、科学化和规范化的轨道，提高快速反应和应急处理能力。

（二）适用范围

本应急处置预案适用于福州市审计局各网的网络信息安全应急处置。根据事件分级原则，我局网络安全事件分为四级：一般（iv级）、较大（iii级）、重大（ii级）和特别重大（i级）。

（三）处置原则

1、预防为主。通过建立健全网络及信息安全管理制度，组织较好的安全设施建设，开展网络安全日常监测，组织网络安全测评，加强信息系统安全教育，预防网络信息系统安全事故的发生。

2、分级负责。建立局领导统一指挥、计算机审计处、办公室等各处室（中心）和值班人员积极配合的审计网络信息系统应急机制。

3、果断处置。一旦发生网络信息系统安全事故，应迅速启动应急措施，尽最大努力减少损失，尽最快速度恢复网络信息系统的安全运行。

及职责

（一）组织机构

局网络安全工作领导小组负责统筹领导网络安全事件应急处置工作，具体通过网络安全领导小组办公室协调组织局网络安全事件应对工作，建立健全全局联动处置机制。值班人员、办公室、计算机处和相关处室单位按照职责分工负责相关网络安全事件应对工作。

（二）主要职责

1、督促落实局网络安全与信息化领导小组的决定和措施；

2、全面开展网络安全事件的预防、监测、报告、应急准备、应急处置和事后恢复与重建工作；

3、拟订网络安全事件相关工作规划和应急预案；

4、督促检查各处室、单位，指导各县（市）区审计机关信息安全工作；

5、汇总有关网络安全事件的各种重要信息，进行综合分析，并提出建议。

（一）监测及报告

1、加强信息安全监测、分析和预警工作，建立网络安全事件报告制度。当网络安全事件发生后，值班人员或相关处室单位等立即报告网络安全工作领导小组办公室(计算机处)。

2、网络安全工作领导小组办公室立即组织断开网络，并启动应急预案，控制事态，消除隐患。及时向网络安全工作领导小组组长报告，对于初判为较大及以上网络安全事件的，立即报告市网安部门和上级审计机关。

（二）预警机制

网络安全工作领导小组办公室接到网络安全事件报告后，立即组织调查核实，并将有关情况及时向组长报告。组织人员进一步进行情况综合分析，研究可能造成损害的程度，提出解决问题的对策。组长视情况召集协调会，研究制定行动方案，发布指示和命令。

（三）预防机制

积极推行信息安全等级保护，逐步实行信息安全风险评估。各基础信息网络和重要信息系统建设要充分考虑抗毁性与灾难恢复，制定并不断完善信息安全应急处理预案。针对基础信息网络的突发性、大规模安全事件，各相关部门建立制度化、程序化的处理流程。

（一）级别的确定

网络安全事件分级的参考要素包括信息密级、公众影响和资产损失三项。各参考要素分别说明如下：

1、信息密级是衡量因信息失窃或泄密所造成的信息安全事件中涉及信息的重要程度的要素；

2、公众影响是衡量信息安全事件所造成的负面影响范围和程度的要素；

3、资产损失是衡量恢复系统正常运行和消除信息安全事件负面影响所需付出资金代价的要素。

网络安全事件级别分为四级：一般（iv级）、较大（iii级）、重大（ii级）和特别重大（i级）。

iv级：审计局机关各处室、下属单位范围内出现并可能造成损害其他网络安全的事件。

iii级：审计局机关各处室、下属单位范围内的信息系统、重点网站等正常运作受到大面积影响和冲击。

ii级：审计局机关各处室、下属单位范围内的基础网络、重要信息系统、重点网站瘫痪，并且纵向或横向延伸可能造成严重社会影响或较大经济损失。

i级：敌对分子利用信息网络进行有组织的大规模的宣传、煽动和渗透活动；或者局机关各处室、下属单位范围多地点或多地区基础网络、重要信息系统、重点网站瘫痪，并且已经造成或可能造成严重社会影响或巨大经济损失的网络安全事件。

（二）预案启动

发生网络安全事件（i级～iv级）后，网络安全工作领导小组办公室启动相应预案，并负责指挥和进行应急处置工作。

（三）现场应急处理

事件发生单位和现场应急处理工作，应尽最大可能收集事件相关信息，区别事件类别，确定事件来源，保护证据，以便缩短应急响应时间。

检查威胁造成的结果，评估事件带来的影响和损害：如检查系统、服务、数据的完整性、保密性或可用性，检查攻击者是否侵入了系统，以后是否能再次随意进入，损失的程度，确定暴露出的主要危险等。

抑制事件的`影响进一步扩大，限制潜在的损失与破坏。可能的抑制策略一般包括：关闭服务或关闭所有的系统，从网络上断开相关系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登录账号，阻断可疑用户得以进入网络的通路，提高系统或网络行为的监控级别，设置陷阱，启用紧急事件下的接管系统，实行特殊“防卫状态”安全警戒，反击攻击者的系统等。

1、审计管理系统等出现异常，无法正常服务时，首先由计算机审计处与福建省审计厅oa服务办联系联系沟通，确定故障原因，配合福建省审计厅oa服务办解决问题。（福建省审计厅oa服务办联系电话\_\_）。

2、东部办公区电子政务云平台存储设备与云平台网络发生故障时，首先与东部办公区电子政务云平台值班电话联系沟通，确定故障原因，配合东部办公区电子政务云平台解决问题。（东部办公区电子政务云平台值班联系电话\_\_）。

3、计算机、服务器硬件设备无法正常运行时，首先检查服务器设备故障报警指示灯状态，初步确定故障原因，使用配套系统硬件检测软件检查确定具体部位。如果不能自行排除，应立即与各设备服务商联系排除故障。（惠普官方维修电话\_\_；戴尔官方维修电话\_\_）

4、网络设施或安全设备发生故障时，首先检查分析故障原因，初步判断故障性质，采取重启设备、已备份配置启动设备等方法排除故障。对不能排除的，区分故障设备，审计专网防火墙及时联系网神科技有限公司福建省分公司，互联网防火墙及时联系网康科技有限公司福建省分公司，确保网络畅通。（网神科技有限公司福建省分公司维修电话\_\_；网康科技有限公司福建省分公司维修电话\_\_）

5、门户网站、微信公众号等政务新媒体出现非法信息或无法正常运行等异常，要立即通过计算机审计处向福州市网站管理部门反映情况，并积极会同相关部门及时追查非法信息来源并及时处理。紧急情况下，可在保全证据的前提下，采取先删除非法信息，再按程序报告的处置措施。（网站管理部门值班电\_\_）

（四）后续处理

1、安全事件进行最初的应急处置以后，应及时采取行动，抑制其影响的进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

2、安全事件被抑制之后，通过对有关事件或行为的分析结果，找出其根源，明确相应的补救措施并彻底清除。

3、在确保安全事件解决后，要及时清理系统、恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

（五）记录上报

网络安全事件发生时，应及时向网络安全工作领导小组汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

（六）结束响应

系统恢复运行后，网络安全工作领导小组办公室对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；属于重大事件或存在非法犯罪行为的，第一时间向公安机关相关部门报案。

（一）技术支撑保障

重视网络信息系统的建设和升级换代，加强技术管理，确保网络安全整体方案的不断完善，聘请信息安全顾问为应急处置过程和重建工作提供咨询和技术支持，确保网络信息系统的稳定与安全。

网络安全工作领导小组办公室不定期组织有关专家和科研力量，开展应急运作机制、应急处理技术、预警和控制等研究，推广和普及新的应急技术。

（二）应急队伍保障

重视信息安全队伍的建设，并不断提高审计人员的信息安全防范意识和技术水平，确保安全事件应急处置过程和重建工作中技术人员的在岗与防护能力。

（三）资金保障

根据网络及信息系统安全预防和应急处置工作的实际需要，提出年度应急处置工作相关设备、工具软件和技术支撑服务所需经费，并纳入年度部门预算，给予资金保障。

（一）安全宣传

不定期举办网络与信息安全知识培训，加强干部职工的计算机操作、信息技能、网络和信息安全等相关知识的宣传普及，增强预防意识和简单应急处置能力。

（二）人员培训

为确保信息安全应急预案有效运行，不定期地举办不同层次、不同类型的培训班或研讨会，以便不同岗位的应急人员都能全面熟悉并掌握信息安全应急处理的知识和技能。

（三）应急演习

为提高网络安全事件应急响应水平，不定期组织预案演练；检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求。通过演习，进一步明确应急响应各岗位责任，对预案中存在的问题和不足及时补充、完善。

（一）预案执行监督

网络安全工作领导小组办公室对预案实施的全过程进行监督检查，督促各单位按本预案指定的职责采取应急措施，确保及时、到位。

发生重大网络安全事件的处室、单位应当按照规定及时如实地报告事件的有关信息，不得瞒报、缓报或者授意他人瞒报、缓报。任何单位或个人发现有瞒报、缓报、谎报重大信息安全事件情况时，有权直接向网络与信息安全小组举报。

应急行动结束后，网络安全工作领导小组办公室对相关成员单位采取的应急行动的及时性、有效性进行评估。

（二）责任追究

在发生重大网络安全事件后，有关责任单位、责任人有瞒报、缓报、漏报和其它失职、渎职行为的，将予以通报批评；对造成严重不良后果的，将视情节由有关主管部门追究责任领导和责任人的行政责任；构成犯罪的，由有关部门依法追究其法律责任。

本预案所称网络安全事件，是指由于自然灾害、设备软硬件故障、内部人为失误或破坏、黑客攻击、无线电频率干扰和计算机病毒破坏等原因，关系到国计民生的基础性网络及重要信息系统的正常运行受到严重影响，出现业务中断、系统破坏、数据破坏或信息失窃或泄密等现象，以及境内外敌对势力、敌对分子利用信息网络进行有组织的大规模的宣传、煽动和渗透活动，或者对国内通信网络或信息设施、重点网站进行大规模的破坏活动，在国家安全、社会稳定或公众利益等方面造成不良影响以及造成一定程度直接或间接经济损失的事件。网络安全事件的主体是指网络安全事件的制造者或造成网络安全事件的最终原因。网络安全事件的客体是指受信息安全事件影响或发生信息安全事件的计算机系统或网络系统。依据计算机系统和网络系统的特点，信息安全事件的客体可分为信息系统、信息内容和网络基础设施三大类。

本预案通过演习、实践检验，以及根据应急力量变更、新技术、新资源的应用和应急事件发展趋势，及时进行修订和完善。

本预案自印发之日起实施，原《福州市审计局网络及信息安全应急预案》（榕审〔20\_\_〕67号）同时废止。

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、发生计算机硬件（系统）故障、通信线路中断、路由故障、流量异常等，网络管理员经初步判断后应立即上报应急领导小组组长，由应急领导小组组长通知做好各部门做好检测车辆的场内秩序维护工作；

（1）、属于计算机硬件（系统）故障；就立即组织电脑公司技术人员进行抢修，属于计算机系统问题的应第一时间利用备份系统进行系统还原操作；还原操作无效的，如无大面积计算机停机现象，应排除隐患，除待处理的检测线外，立即逐步恢复能正常工作的检测线工位机、计算机，尽快恢复车辆检测工作；

（2）、属于计算机网络连接问题的，能通过拉接临时线解决的，应立即拉接临时线缆，再逐步查找连接故障；由于连接交换机故障的，应立即更换上备用交换站；站内各部门有义务配合网络管理员做好排故工作；

（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。

（4）、由网络攻击或病毒、木马等引起的网络堵塞等现象，应立即拨掉网线，将故障计算机（服务器）脱离网络，并关闭计算机后重新开机，下载安装最新的杀毒软件对故障计算机逐一进行杀毒处理；对连接交换进行断电处理；

（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。

适用范围，预案适用于公司接入互联网的服务器，虚拟主机以及内部工作电脑等信息系统上的突发性事件的应急工作。

在公司发生重大突发公共事件或者自然灾害或上级部门通知时，启动本应急预案，上级有关部门交办的重要互联网通讯保障工作。那原则上要统一领导，统一指挥，分类管理，分级负责，严密组织，协作配合，预防为主，防处结合，发挥优势，保障安全。应急领导小组，公司信息管理总监，运行维护经理以及网络管理员组成的网络安全应急处理小组。

领导小组我主要职责加强领导，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。

充分利用各种渠道进行网络安全知识的宣传教育，组织直到集团网络安全常识的普及教育，广泛开展网络安全和有关技能的训练，不断提高公司员工的防范意识和基本技能。人生做好各项物资保障，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。要采取一切必要手段，组织各方面力量，全面进行网络安全事故处理工作，将不良影响和损失降到最低点。

调动一切积极因素，全面保障和促进公司网络安全稳定的运行。

灾害发生之后，网络管理员判定灾害级别抽波，估计灾害造成的损失，保留相关证据，并且在十分钟内上报信息管理总监，由信息管理总监决定是否请启动应急预案。一旦启动应急预案，信息管理中心运行维护组进行应急处置工作状态，阻断网络连接，进行现场保护协助。调查取证和系统恢复等工作，对相关事件进行跟踪，密切关注事件动向，协助调查取证有关违法事件移交公安机关处理。处置措施，网站不良信息事故处理医院一旦发现公司网站上出现不良信息，或者是被黑客攻击，修改了网页，立即关闭网站。

一、信息中心配备诺顿企业版网络防火墙软件和防病毒软件，及时升级，及时清除杀灭网络病毒，一旦发生黑客入侵事件，部署的入侵检测系统（ids），将向管理员发出警报，管理员将在第一时间处理黑客入侵事件，并报有关部门。

二、对来往电子邮件及网络下载文件用防病毒软件过滤，确保不被木马类黑客病毒侵入并在无意中协助传播病毒。一旦发生类似冲击波、震荡波等类似的网络蠕虫\_\_\_\_，管理员将在第一时间升级病毒防火墙，给系统打布丁，防止病毒的恶意破坏。

三、信息中心对服务器重要信息定时做好备份，提高信息存储安全应急响应能力。一旦发生严重的因黑客、病毒侵入，造成网络无法正常运行时，管理员将在第一时间恢复服务器备份，保证网络的正常运行。

四、管理员对定期检查的运转情况，做好设备维护纪录，保证设备高效稳定的运行。一旦服务器出现硬件设备故障，管理员将在第一时间启用备份服务器，保证网络的正常运行，并对原服务器进行及时的检修，在修复后将替换备份服务器继续运行，保证网络的正常运行。一旦其它网络设备出现故障，管理员将在第一时间用备件替换故障设备，保证网络的正常运行。

五、定期升级操作系统补丁程序，配备顿企业版网络防火墙软件和防病毒软件，及时升级，及时清除杀灭网络病毒，防止被他人恶意侵入。对来往电子邮件及网络下载文件用防病毒软件过滤，不运行可疑程序，确保不被木马类黑客病毒侵入并在无意张协助传播病毒。

六、学校严格控制网络信息密码、管理权限、知情范围，妥善管理密码，并按照满足需求、方便使用、加强管理的原则，进一步完善密码管理制度，建立健全适应教育信息化发展的科学的密码管理体系。

七、凡是上网人员，都能通过防火墙记录在日志里，日志的保留时间为3个月。关闭一些反动、不健康的网站，保障了校园文化的`干净。在邮件系统方面，我们安装了第三方插件，能起到过滤关键字的作用。信息中心对服务器重要信息定时做好备份，提高信息存储安全应急响应能力。并定期检查设备的运转情况，做好设备维护记录，保证设备高效稳定的运行。

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。

**企业网络安全应急预案篇九**

为了进一步增强全区教育系统网络安全意识，提高网络安全防护技能，按照陕西省教育厅办公室《关于开展陕西省教育系统网络安全宣传周活动的通知》要求(陕教保办〔〕15号)，区教体局决定在全区教育系统开展网络安全宣传周活动。现将有关事项通知如下：

目前，全区各中小学、幼儿园全部达到了光纤网络校校通，实现了网络校园全覆盖，部分学校还建设了无线网络应用环境。为进一步推动我区教育网络建设，提升教育网络安全教育管理水平，深入开展网络安全宣传周活动，培养广大师生绿色上网、文明上网意识和良好习惯，增强师生网络安全防护能力，加强网络安全教育宣传，强化各项管理措施，全面构建全区教育系统文明、安全、和谐的网络环境。

为了搞好本次活动，区教体局成立了网络安全宣传周活动领导小组：

组 长：安建利

副组长：赵小东 杨 刚

成 员：各乡镇(街道)教育助理员;各中小学校长、幼儿园园长。

本次活动主题为“网络安全知识进校园”，旨在提高青少年网络安全自我保护意识，提升其网络安全问题甄别能力。

11月24日至30日。

开展网络安全宣传周活动，旨在引导广大师生和家长正确认识互联网，依法管理和使用互联网，自觉抵制网络危害，远离网络违法犯罪陷阱，带动全社会共同营造良好的网络环境。各学校通过开展形式多样的网络安全宣传活动，积极倡导师生文明上网、安全上网、绿色上网，大力宣传涉网案件防范基本知识，使广大师生成为积极参与活动、主动教育宣传、坚决抵制恶习、养成良好上网习惯的网络安全践行者，使学校率先成为我区文明、安全、和谐的网络育人基地。

1、学习网络安全方面的相关政策、法规、文件，了解目前网络安全方面的动态信息。

2、召开学校网络安全工作会，总结本校在网络安全维护工作方面所采取的措施和取得的成效。

3、采用多种形式进行网络安全宣传，普及基本的网络安全知识，使教师、学生增强网络安全防范意识，具备识别和应对网络危险的基本能力。

各学校可结合各自实际情况，充分利用校园网络、电子屏、板报、校刊、手抄报等多种媒体，采用专题会议、主题班会、演讲比赛、安

全征文等多种形式，开展网络安全主题宣传活动。本次网络安全宣传周活动建议采取以下形式开展：

1、悬挂网络安全宣传横幅。

各学校应在宣传活动期间在本单位人流量较多的场所悬挂横幅，横幅内容为“共建网络安全，共享网络文明”。

2、开办网络安全宣传专栏。

各学校应在本单位宣传栏上开辟一个网络安全宣传专栏，结合黑板报、手抄报等多种形式，编写一期网络安全黑板报，对网络安全相关知识进行宣传。

3、举办网络安全宣传讲座。

各学校可根据本单位情况，邀请网络安全方面的专家为师生开办一期专题讲座;或利用“班班通”设备收看一场网络安全宣传片;或在“校园电视台”组织一次网络安全讲座或广播;或组织各班召开一次网络安全主题班会，学习网络安全相关知识。

4、开展网络安全知识竞赛。

为调动师生的积极性，各学校应组织师生开展网络安全知识竞赛或测试，竞赛内容应紧扣本次活动主题。

5、发放网络安全宣传传单。

各学校应制作电子版或纸质版网络安全宣传传单，采取“致家长、学生一封信”、开展网络安全问卷调查等方式，向学生及其家长发放，引导和带动师生、家长全面了解和积极参与本次活动。

1、本次活动时间紧、任务重。各乡镇要认识到新形势下网络安全进校园工作的紧迫性，认认真真、扎扎实实地组织学校开展此项活动。要落实专人负责，尽快制定活动方案，安排部署该项工作，确保网络安全宣传活动走进每一所学校。

2、各学校要高度重视此次宣传活动，落实工作责任。要结合活动主题，认真组织有关人员全面准备宣传内容。要精心谋划、创新形式开展系列宣传教育活动，提前做好每项活动的人员、时间安排。要动员和组织广大师生和家长积极参与，各个学校要按照活动计划，分阶段、分层次推进网络安全宣传活动，让每一名在校师生都普遍接受一次网络安全教育。

同时，各校要开展一次清理清查活动，全面掌握学校网络设备、网络接入点、上网计算机的管理情况(特别是无线接入点的管理)，了解师生网络安全防范基本信息。各校要认真查找薄弱环节，不断完善管理措施，改进宣传教育方法，全面提升网络安全管控能力，并建立长效机制。

3、本次活动中要统一使用“国家网络安全宣传周”标识，突出宣传周主题，积极利用多种媒体开展线上、线下宣传，活动形式可灵活多样，鼓励创新。

3、要坚决执行中央八项规定有关要求，严格按照勤俭节约、务实高效原则，着力在提高活动实效上下功夫，严禁铺张浪费、大讲排场和各种形式主义。/p>

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

1.按照市委网信办指导，全区学校集中开展网络安全资料进学校、进课堂活动。通过张贴海报、发放宣传材料，组织学生认真学习网络安全知识手册;

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

1.各校通过邀请专家围绕网络安全态势、网络安全新技术新应用、重点领域网络安全保障能力、个人及重要数据保护等开展专题讲座;

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。

为增强校园网络安全意识，提高网络安全防护技能，按照中央网信办、教育部等6部委联合制定的《国家网络安全宣传周活动方案》(中网办发文〔20\_\_〕2号)及省委高校工委相关通知要求，特制定出我院校园网络安全宣传周活动方案：

一、活动主题

网络安全为人民，网络安全靠人民

二、活动时间

9月19—25日，其中9月20日为教育主题日。

三、活动安排

(一)举办全校大学生网络安全知识竞赛

9月9日至10月31日，各系组织学生参加“全国大学生网络安全知识竞赛”，通过网络答题方式普及网络安全知识。激发学生学习网络安全知识兴趣，提升网络安全防护技能。

竞赛网址：

任务单位：院团委

(二)开展网络安全教育专题活动

1、网站宣传

在学院网站首页开辟网络安全专题，发布相关安全知识、法律法规及学院相关活动，并组织相关资料供广大师生下载学习使用。

负责部门：宣传部

2、设计网络安全宣传橱窗、电子标语及摆放宣传板

在学校\_\_区设计放置宣传橱窗，\_\_区主干道及学生主要活动区域发送电子宣传标语、摆放宣传板，积极营造网络安全文化氛围。

任务部门：宣传部

3、微信推送

通过学校公众号面向全校师生进行网络安全信息推送。

任务部门：宣传部

4、校园广播宣传

活动期间，校园广播站广播有关网络安全的常识，提高师生网络安全意识。

任务部门：宣传部

5、团日主题班会

各系部根据实际情况，组织开展“网络安全宣传周”团日教育活动，以视频、实例、线上线下互动交流等方式，组织学生学习网络安全知识，提升网络安全意识。

任务部门：学生处、院团委

四、工作要求

1、高度重视，加强组织领导。举办网络安全周活动是贯彻落实中央关于网络安全和信息化战略部署的重要举措，各系部要高度重视，组织师生积极参与宣传教育活动，充分调动学生的积极性、主动性和创造性，推动活动形成声势。

2、突出主题，注重工作实效。要紧紧围绕活动主题，将网络安全教育与学生思想政治教育、文明校园建设、维护校园稳定等工作有机结合，提升工作的针对性与实效性，营造校园安全上网、依法上网的良好氛围。

3、加强协作，建立长效机制。以安全周为契机，探索建立青少年学生网络安全教育长效机制。推动相关内容纳入新生教育、课程教育、团日活动和课外实践活动，完善网络安全教育工作体系，切实增强教育实效。

4、严守规定，务实高效。要坚决贯彻执行中央八项规定有关要求，严格按照勤俭节约、务实高效原则，着力在提高活动实效上下功夫，严禁铺张浪费、大讲排场和各种形式主义。

一、时间和主题

时间：9月19日至25日

主题：网络安全为人民，网络安全靠人民

宣传周活动重点内容是，深入学习贯彻重要讲话、重要批示精神和总体国家安全观，通过网站、电视、电台、报刊杂志、会议、展览等多种渠道和形式，通过全体网民的广泛参与，大力宣传倡导依法文明上网，增强全社会网络安全意识，普及网络安全知识，营造健康文明的网络环境，维护网络安全。

二、主要活动安排

(一)主题日活动

根据中央网信办统一部署，宣传周活动期间，分别组织开展主题日活动：9月20日教育日、9月21日电信日、9月22日法制日、9月23日金融日、9月24日青少年日、9月25日公益宣传日。

(二)具体活动要求

各中小学校要结合青岛市“共筑网络安全共享网络文明”安全教育活动的组织开展，通过组织主题班会、家长会、教师会等形式，通过学校网站、学校教师和班级家长微信群等途径，利用学校的班班通设施结合微机课等方面，在广大学生、家长、教师中开展网络安全知识专题教育。加强与网信、公安等部门协作，探索建立网络安全教育长效机制，完善网络安全教育工作体系。

1.各学校和教体局机关要在9月16日之前完成网络安全宣传周主形象海报的制作，并在学校宣传栏、微机教室等特殊场地醒目位置进行张贴宣传，营造良好的宣传氛围。

2.各学校要认真组织部署工作要求，通过组织主题班会等形式，教体局通过办公室组织机关工作会议，利用学校班班通设备、多媒体、网站等，广泛宣传网络安全口号标语、卡通漫画，播放收看附件中的安全教育视频和平度市“共筑网络安全共享网络文明”安全教育活动推进会报告。

3.各学校要与已经开展的青岛市“共筑网络安全共享网络文明”活动融合在一起，通过已经组建完成的各类宣传渠道以及通过官方网站、公安微博、微信群等形式积极转发打击网络违法犯罪典型案例、推送公益广告、发送宣传教育材料等，通过线上、线下多渠道、多形式充分发挥团委、少先队的作用，广泛组织集中开展主题宣传教育活动。

4.结合国家网络安全宣传周活动安排，各学校要积极组织学生、教师观看科普视频、研讨交流、争当网络安全宣传员监督员以及开展新媒体主题宣传等活动，在青少年中广泛开展网络安全宣传教育。

5.各校要了解省级部门活动安排的时间节点，积极组织学习并参与。9月19日至25日，在山东共青团官方微博开设话题#青少年与网络安全#，加强与青少年网民互动。积极组织全省高中学生参加网络安全知识竞赛，选拔优秀人才赴湖北武汉参加全国中学生网络安全夏令营暨知识竞赛全国复赛。联合大众网、齐鲁网开展网络安全公益广告有奖征集活动。9月24日，组织全省青少年在线观看湖北武汉市“青少年日”主场活动直播、与演讲嘉宾远程互动等。9月19日至25日宣传周期间，省重点新闻网站在pc端首页显著位置和移动端首屏统一开设“国家网络安全宣传周活动”专题，对我省各有关部门活动情况和现场宣传进行采访报道，转发中央新闻网站关于国家网络安全宣传周武汉开幕式相关报道和现场视频，集纳展示网络安全宣传公益广告、图片、动漫等各类相关作品，在论坛、微博等平台主动设置“网络安全”相关议题、话题，利用手机报、微信公众号推送有关稿件、视频和h5作品。大众网联合山东艺术学院制作动漫作品;9月1日至9月30日开展网络公益广告征集活动;9月12日至9月25日开展网络安全在线答题活动;邀请相关领导、专家、学者开展视频访谈。齐鲁网推出“一图教你如何安全上网”漫画;制作“文明上网”系列公益广告;组织小记者探营网络安全公益活动。舜网组织《新闻调查——网络暴力离我有多远》系列视频街访等采访报道;携手17市网媒联动倡议建立“反对网络暴力”网媒接力联盟。中华泰山网开设网络安全课堂，邀请教育、公安、团委、通讯等部门单位的专家授课。水母网开设网络金融安全知识在线答题栏目。

三、组织协调

教体局信息中心负责组织协调我市中小学校和教体局机关网络安全宣传周活动。宣传办协助做好宣传周活动的宣传报道工作。

四、总结报告

教体局信息中心负责此次活动的总结工作并要求各学校在9月30日前，将各自活动开展情况通过数字校园平台消息中心报教体局信息中心马玉民老师。

一、活动主题

共建网络安全，共享网络文明

二、重点活动及任务安排

1、校园网主页宣传学校网站标识。

任务单位：网络中心

完成要求：按国家规定

2、学校官方微博、微信宣传首届国家网络信息安全宣传周活动的主题、主要内容、网络安全知识、文明上网要求等。

任务单位：\_

完成时间：20\_\_年11月24日至30日

3、教学楼、实验楼电子屏宣传首届国家网络信息安全宣传周活动主题内容标语。

任务单位：有室外电子屏的学院

完成时间：20\_\_年11月26日至30日

4、召开教职工会、主题班会，学习宣传国家有关网络安全法规。

任务单位：\_

完成时间：20\_\_年11月25日—12月31日

5、组织学生参加全国大学生网络安全知识竞赛活动。

任务单位：学工部、校团委、各学院

完成时间：20\_\_年11月25日—12月31日

**企业网络安全应急预案篇十**

（一）网站、网页出现非法言论时的应急预案

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。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找