# 网络安全应急预案演练方案(精选11篇)

来源：网络 作者：寂静之音 更新时间：2024-12-28

*方案在各个领域都有着重要的作用，无论是在个人生活中还是在组织管理中，都扮演着至关重要的角色。方案的格式和要求是什么样的呢？以下是小编为大家收集的方案范文，欢迎大家分享阅读。网络安全应急预案演练方案篇一为有效制止各种网络安全事件的发生，最大地...*

方案在各个领域都有着重要的作用，无论是在个人生活中还是在组织管理中，都扮演着至关重要的角色。方案的格式和要求是什么样的呢？以下是小编为大家收集的方案范文，欢迎大家分享阅读。

**网络安全应急预案演练方案篇一**

为有效制止各种网络安全事件的发生，最大地减少各种网络安全事件所造成的破坏和负面影响，特制定本预案。

一、坚持以预防、监控为主的原则，做到响应快、定位准、控制及时、措施有力，在网络安全上把握主动权。

二、学校保卫处对校园网内容进行24小时专人监控，信息与网络中心对网络安全技术问题进行24小时应急响应，结合严格的规章制度，确保网络安全的监控随时处于有序、有效状态。

三、实行多部门协作机制，发现网络安全事件的苗头后，网络中心、保卫处、学工部，必要时联合当地公安派出所，对安全事件当事人进行快速准确的目标定位、对象确定，并在适当时机实地控制当事人和相关设备等。

四、严格上网实名制，所有校园网用户均采取有详细记录的、由学校统一管理的身份认证措施；学校论坛必须实名注册。

五、重视服务器日志的保存和使用，确保发现问题时能够有效追查定位。

六、对校园网内各单位或个人因特殊需要而开设的服务采取登录备案制度，各单位服务器要求有专人负责管理，并且对管理员的联系信息进行详细备案。

网络事件的处置遵从负面影响最小化的原则。

网络内容相关事件的处理，必须遵从先固定证据、再保留证据、然后再采取措施消除影响的基本流程。

1、责任到人。

事件发生将直接追究部门主要负责人及分管领导和技术负责人的责任。

2、跟踪监控。

发生安全事件后，保卫处、信息与网络中心通过一定的技术手段，立即保持对事件的全程跟踪，同时根据事件的表现和程度，及时通知有关部门协同处理。

3、内容取证。

在采取跟踪监控措施的同时，立即对安全事件的内容进行取证，必要时请公安部门出面同时控制当事者的机器和当事人。有关通过网络远程取证的内容要注意时间、位置、涉及人员等尽量全面，注意证据保存位置可靠；现场取证的内容在必要时要求在当事人现场参与的情况下截图，并打印、签字确认。

4、切断服务。

对安全事件进行证据保全后，应当第一时间根据事件性质，分别采取勒令改正、删除内容、停止服务等果断措施。必要时学校可强行断开相关区域的网络或与安全事件相关的服务。

5、追查定位。

结合事件发生日期时间、服务器日志、用户账户等信息，对事件当事人进行快速定位，以便能够在必要时进行责任追查。

6、调查处理。

确定事件的当事人后，根据国家有关法规和学校网络管理和安全、保密要求，根据当事人的事件性质和危害程度，分别采取学院或单位内部处置、全校通报处理等措施。学生当事人联合学工部按有关规定进行处置；其他教工则联系人事处、保卫处、纪委等单位，根据有关规定给予当事人适当的处分。

7、漏洞补救。

对安全事件采取适当处置后，有关单位和个人必须认真检讨其所存在的疏忽，找出事件发生的原因，查找存在的安全漏洞，并立即采取有效的补救措施。对于某些事件，必要时必须由相关部门研究后给出适当的回应，以最快地消除负面影响。

八、网络紧急响应小组成员：

由分管校长及校办、党办、信息与网络中心、人事处、保卫处、学工部、团委各部门负责人组成。

**网络安全应急预案演练方案篇二**

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：

一、活动目的。

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。

二、组织机构。

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。

三、活动主题。

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。

四、活动时间。

11月24日至30日。

五、活动内容。

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。

六、活动形式。

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：

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”。

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。

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。

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。

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。

七、活动要求。

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。

**网络安全应急预案演练方案篇三**

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网络管理安全会议精神，结合我校校园网工作实际，特制定本预案。

从讲政治、讲大局，保证国家安全的高度，充分认识确保网络与信息安全的重要意义。要对xxx组织及其它境外敌对势力利用网络信息进行煽动和破坏活动以及进行有组织的网上大规模“黑客”与病毒攻击保持高度警惕，消除麻痹大意和侥幸思想,继续深入开展互联网有害信息的清理整治,组织实施本校园网有害信息的安全防范及应急处置工作,进一步明确责任,落实工作措施,确保校园网络信息安全。

在最短时限内，及时、果断处理在本校园网范围内传播的有害信息，遏制有害信息在校园网中扩散，最大限度减轻社会危害，并搜集掌握犯罪线索，打击网上违法犯罪活动，维护校园信息安全和政治稳定。

（一）有害信息内容：

1、攻击党和国家领导人；

2、煽动抗拒、破坏宪法和法律、行政法规实施；

3、煽动颠覆国家政权，推翻社会主义制度；

4、煽动分裂国家、破坏国家统一；

6、宣传xxx、色情、暴力、凶杀，教唆犯罪；

7、歪曲报道我区重大政治、经济、文化事件；

8、其他严重危害国家安全和社会治安秩序的信息；

9、一切对青少年成长可能产生不良影响的信息。

（二）严重违法犯罪活动：

1、利用互联网、校园网大规模进行煽动颠覆国家政权、推翻社会主义制度、破坏国家统一，煽动民族仇恨，破坏民族团结活动。

2、利用互联网、校园网组党结社，进行xxx勾联、xxx活动。

3、利用网络技术进行大规模破坏社会稳定，扰乱金融秩序的活动。

4、利用互联网、校园网大规模制作、传播计算机病毒，非法入侵，致使计算机系统及通信网络遭受重大损失的活动。

成立信息安全应急处置工作领导小组（简称信息安全应急领导小组）,负责学校网络信息安全应急处置工作。

组长：zz。

成员：zz。

各班级班主任。

（一）信息安全应急领导小组负责组织开展对校园网进行信息监控和巡查，删除、过滤有害信息，采取技术措施封堵有害信息的传播途径，控制有害信息在校园网扩散，及时上报学生动态。

（二）接入互联网的科室教师和学生，要主动与有关部门做好网络与信息安全的衔接工作，做到权责明确，应急处置渠道畅通。要根据师生使用公共网络的实际情况，制定切实可行的安全防范措施，防止有害信息通过公共网络在校内扩散。

（三）进一步加强对视频节目的监管，校园网视频不得采用通过盗版等非法途径接收、下载、录制、播放，在校园网里点播或直播的视频节目应健康向上，有利于青少年身心健康发展，有利于促进学校教育教学事业发展。

具体职责分工：

z（通讯联络）。

发生网络安全事故时迅速与学校领导、各相关处室、班主任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）对学校重大事件（如艺术节直播、检查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。

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电信部门求救。

在事件过程中出现任何问题应立刻向学校分管领导汇报。

z（网络恶意攻击事故处理）。

（2）如果攻击来自校外，立刻从路由器中查出对方ip地址并过滤，同时对路由器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。

**网络安全应急预案演练方案篇四**

为提高我校校园网应对网络与信息安全突发事件的能力，加强校园网安全保障工作，形成科学、有效、快速的应急机制，确保校园网的实体安全、运行安全和数据安全，最大限度地减轻网络基础平台与信息安全突发事件造成的危害，特制定此应急预案。

一、制定依据。

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联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《桐城师专校园计算机网络管理暂行办法》制定本预案。

二、适用范围。

本预案适用的网络和信息安全突发事件包括如下几方面。

1、网络基础平台突发事件。网络基础平台突发事件是指由自然灾害、其他事故和人为破坏引起的网络硬件设备和基础设施损坏的事件。

2、应用系统和信息安全突发事件。应用系统和信息安全突发事件是指因为黑客攻击或病毒等导致的应用系统故障、异常或拒绝服务、信息泄露或被篡改、或利用校园网传播危害国家安全、社会秩序及影响我校正常学习工作的事件。

三、组织体系。

在学校信息化工作小组的领导下，以实验实训中心为执行部门，按照“分级负责、责任到人”的原则，组织实施具体的应急预案。

实验实训中心领导负责研究制定校园网基础平台、应用系统和信息安全突发事件应急处置工作的规划、计划和政策，不断推进网络应急机制和工作体系的建设；在发生以上网络安全突发事件后，决定启动应急预案，组织实施应急处置工作。并在发生重大突发事件时汇报信息化工作小组。

四、应急流程。

1、临时处理。

在突发事件发生后，值班维护人员应做好临时应急处置工作，立即采取措施控制事态，同时向实验实训中心领导报告。并在事件处置结束前进行动态监测、评估，及时将事件现状及处置工作等情况进行汇报，不得隐瞒、缓报、谎报。

2、预案实施。

实验实训中心领导接到突发事件报告后，根据事件严重程度，进行不同的处置。对于重大突发事件，实验实训中心领导应当汇报信息化工作小组，并给出处置建议。对于一般事件，按照已有的预案实施应急处置。同时相关人员保持联系，及时了解当前状况，组织预案的实施工作。

3、信息发布。

当突发事件发生时，实验实训中心应及时做好信息发布工作，通过仍然正常工作的应用系统或者其他渠道发布当前网络安全突发事件处置的相关信息，引导舆论和公众行为，避免影响社会或学校秩序。

实验实训中心要密切关注国内外关于当前网络安全突发事件的新闻报道，及时采取措施，对媒体关于事件以及处置工作的不正确信息，进行澄清、纠正影响，接受群众咨询，释疑解惑，稳定人心。

4、应急支援。

经实施应急预案后，事态难以控制或有扩大发展趋势时。要迅速召开应急处置会议或由信息化工作小组根据事态情况，研究采取有利于控制事态的非常措施，并向相关技术部门或公安部门请求援助。

5、应急结束。

当突发事件的影响效果大幅度减小或消失，校园网恢复正常时，由实验实训中心相关人员根据监控数据给出应急结束的建议，由实验实训中心领导宣布应急结束，对于重大事件应急结束时应汇报信息化工作小组。

五、事后处置。

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或对存在问题的应用系统进行维护，以减少损失，尽快恢复正常工作。对于信息安全突发事件中的不良信息，做好日志记录，保存好证据以备日后审查。统计各种数据，查明事件原因，对事件造成的损失和影响以及恢复能力进行分析评估，认真制定恢复计划，并迅速组织实施。事后处置过程应向实验实训中心领导汇报或上报信息化工作小组。

1、硬件和网络设施保障。事先预留一定的应急硬件设备或网络设施。在突发事件发生时，可以及时替换使用。

2、重要应用系统、信息和数据均应建立异地容灾备份系统和相关工作机制，保证系统或数据在受到破坏后，可紧急恢复。

3、应急队伍保障。建立网络安全应急保障队伍。同时由实验实训中心选择技术能力较强的人员作为网站应急支援力量。

4、经费保障。优先考虑经费投入，纳入学校年度预算。

七、具体预案措施。

1、自然灾害紧急处置措施，校园网中心机房和核心交换节点因自然灾害（如潮湿、雷电等）导致设备损害无法正常工作时，值班人员应立即报告实验实训中心领导，并检查损坏程度，找出事故原因加以处理，联系设备供应商进行维修，并通知用户相关服务暂停以及预计恢复时间。

2、被盗和人为损坏紧急处置措施，校园网中心机房和核心交换节点设备被盗或者人为原因导致损坏时，值班人员应立即报告信息管理中心领导，并保护好现场，第一时间收集证据，以备公安部门进行调查或追究损坏设备的相关责任。实验实训中心应报告学校总务处或公安部门进行后续处理。

3、网络基础平台设备自然损坏紧急处置措施，服务器等关键设备因老化等原因自然损坏后，相关负责人员应立即查明原因。如果能够自行恢复，应立即用备件替换受损部件。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。如果设备一时不能修复，应向领导汇报，并告知用户受到影响的网站服务。

4、停电紧急处置措施，机房长时间停电发生时，如果能事先从学校后勤部门或供电部门得知停电信息，应做好应用系统备份工作，通过学校网站通知用户暂停部分服务的信息，提醒用户保存数据，停止网络传输。准备备用电源保障最重要的设备和应用系统继续运作，关闭次要的设备和系统。并及时报告给实验实训中心领导，保持和后勤或供电部门的联系，以期尽快恢复供电。

5、通信故障紧急处置措施，当校内网络出现严重通信故障时，信息管理中心网络管理部应立刻报告实验实训中心领导，并立即组织排除故障，同时通知网络受到影响的校园网用户。校外网络出现通信故障时，应及时通知校园网用户，并积极联系网络服务提供商，敦促排除故障。

6、校园网网站、公共资源等信息窗口和平台出现非法言论或不良信息时，网站、网页和该公共资源由值班人员随时密切监视。如果多次出现，应结合发布人和身份认证系统定位到人，并向信息管理中心领导汇报。技术人员应在接到通知后立即对非法信息进行日志记录，保留证据后进行清除。网站维护员应将记录及日志上报备案。

7、黑客攻击时的紧急处置措施，当有应用系统或者信息被篡改，或通过应用系统日志和访问记录发现有黑客正在进行攻击时,首先应将被攻击的系统和设备等从网络中隔离出来，同时向领导汇报情况。技术人员立即进行被破坏系统的恢复与重建工作。

8、病毒安全紧急处置措施，当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。对该设备的硬盘进行数据备份。启用杀毒软件对该机进行杀毒处理。如发现杀毒软件无法清楚该病毒，应立即向实验实训中心领导报告。经技术人员确认确实无法查杀该病毒后，应作好相关记录，同时立即向信息技术人员报告，并迅速研究解决办法。如果感染病毒的设备是托管服务器，经领导同意，应立即告知各下属单位做好相应的清查工作。

9、应用系统遭受破坏性攻击的紧急处置措施，重要的应用系统平时必须存有备份，与应用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。一旦系统遭到破坏性攻击，应立即向领导报告，并将系统停止运行。网站维护员立即进行软件系统和数据的恢复。

10、数据库安全紧急处置措施，各数据库系统要至少准备一个以上数据库备份，每日进行增量备份。一旦数据库崩溃，应立即向领导报告，并立即进行备份恢复。

11、关键人员不在岗的紧急处置措施。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。一旦发生关键人员不在岗的情况，首先应向领导汇报情况。经领导批准后，由备用人员上岗操作。

其他未列出的突发事件，一律需首先汇报给实验实训中心领导或信息化工作小组，并遵照领导指示进行应急处置。

**网络安全应急预案演练方案篇五**

为切实做好学校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，确保网络与信息安全，结合我校网络实际工作，特制定本预案。

第一条本预案所称突发性事件，是指自然因素或人为活动引发的危害我校网络设施及信息安全等有关的灾害。包括校园网运行及网络信息方面发生的有可能影响学校、社会和国家安全稳定的紧急事件；由于其他重大事件的发生影响到我校校园网正常运行或校园网络信息安全，并由此可能影响到学校、社会、国家安全稳定的事件。

影响或破坏网络运行及网络信息安全的事件可分为校园网络安全事件和网络信息安全事件两类：校园网络安全事件主要指校园网络实体中线路、网络设备、服务器设备等出现的被病毒和恶意攻击带来的安全事件；网络信息安全事件主要指校园网络中各信息服务设备中出现的信息安全事件，如非法信息、泄密事件等。

第二条本预案所称网络信息安全事件与网络运行事件类型

（一）网络信息安全事件：

1、特别重大的事件： 校园网上出现大面积的串联、煽动和蛊惑信息；主页出现反动、煽动分裂、破坏稳定等反动政治信息及链接的，出现较大的泄、失密事件。

2、重大事件： 校园网上出现不良信息、主页出现淫秽信息及链接的。

3、较大事件： 校园网用户邮箱出现大量非法宣传邮件；校园网用户未经审批在校园网上私自设立网站并提供非法信息 。

（二）网络运行安全事件：

1、由于病毒攻击、非法入侵等原因，校园网部分楼宇或整个校园网出现网络瘫痪。

2、由于病毒攻击、非法入侵等原因， 部分网站服务器不能响应用户请求。

3、由于病毒攻击、非法入侵等原因，校园网络中心全部dns、主web服务器不能正常工作。

4、由于病毒攻击、非法入侵、人为破坏或不可抗力等原因，造成校园网出口中断。

第三条本预案的指导思想是确保我校相关计算机网络及信息的安全。

第四条本预案适用于发生在我校网络的突发性事件应急工作。

第五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。

第六条成立学校网络信息安全管理领导小组，由分管安全与分管信息化工作领导任组长，成员包括办公室负责人、教务处负责人、思政部负责人、总务后勤负责人、网络信息中心负责人。

成立网络信息安全应急处置工作小组，工作小组办公室设在网络信息中心。工作小组的主要职责与任务是统筹全校网络信息的灾害应急工作，全面负责学校网络可能出现的各种突发事件处置工作，协调解决问题处置工作中的重大问题等。

第七条处置措施

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，网络信息中心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。网络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，要及时处理并向网络信息安全管理领导小组报告。

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。属于大型灾害的，在向领导小组报告的同时，还应向公安局网监部门报告。

（二）灾害发生后，立即启动应急预案，采取应急处置程序，判定灾害级别，并立即将灾情向网络信息安全管理领导小组报告，在处置过程中，应及时报告处置工作进展情况，直至处置工作结束。

第八条处置程序

（一）发现情况

网络信息中心要严格执行值班制度，做好校园网信息系统安全的日常巡查及其每周访问记录的备份和90天访问日志保存工作，以保障最先发现灾害并及时处置此突发性事件。

（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。

（三）应急处置方法

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。然后针对入侵方法建设或更新入侵检测设备。

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：一旦发现，可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。不能处理的可以请教相关的专业人员。

（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，首先向学校网络信息安全管理领导小组汇报。在大型灾害发生时或上级领导通知的特殊时间内发生的灾害，同时向上级主管部门报告,向公安局网监部门汇报。中、小型级别的灾害，可以只向网络信息安全管理领导小组汇报，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，或与安全相关网站发布了预警而教育网络还没有出现相应的灾害，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，由网络信息安全管理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。

第九条人员保障

重视人员的建设与保障，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的战斗力。

第十条技术保障

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强劲与安全，灾害处置过程中和灾后重建中的相关技术支撑。

第十一条物资保障

要根据近年网络信息系统安全防治工作所需经费情况，将本年度灾害应急经费纳入年度计划和预算，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。

第十二条训练和演练

加强校园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。

**网络安全应急预案演练方案篇六**

根据教育部、省高校工委关于做好20\_年国家网络安全宣传周相关工作的要求，学院决定举办2\_国家网络安全宣传周(以下简称宣传周)。为做好宣传周的相关组织工作，制订如下实施方案：

一、指导思想。

学习宣传网络强国战略思想，大力培育有高度的安全意识、有文明的网络素养、有守法的行为习惯、有必备的防护技能的新一代“四有中国好网民”，增强学院广大师生的网络安全意识，提升基本防护技能，营造安全健康文明的网络环境，共同维护国家网络安全。

二、活动时间和主题。

1.活动时间：9月19日至25日，其中9月20日为教育主题日。

2.活动主题：网络安全为人民，网络安全靠人民。

三、活动内容。

(一)举办全院大学生网络安全知识竞赛。

9月19日至10月31日，各系部组织学生参加“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：\_\_。

请各系部于9月27日前将学生参赛情况报送到学生工作处(团委)。

牵头部门：学生工作处(团委)。

1.网站和宣传橱窗宣传。

在学院网站开设网络安全宣传专栏，发布相关的安全知识、法律法规及相关案例，并组织相关资料供广大师生下载学习使用。

宣传周期间，校园各宣传橱窗张贴宣传周官方海报、相关网络安全知识海报等。

牵头部门：宣传部。

2.学院电子大屏幕播放。

宣传周期间，利用学院电子大屏幕，播放宣传周的官方海报、视频、口号标语等，积极营造网络安全文化氛围。

牵头部门：现代教育中心。

3.微信推送。

宣传周期间，利用“青春威职”,面向全院师生进行网络安全信息推送。

牵头部门：学生工作处(团委)。

4.校园广播宣传。

宣传周期间，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。

牵头部门：学生工作处(团委)。

(1)集中活动。在步行街利用宣传展板、散发宣传折页和网络安全小知识等形式，向全院师生宣传网络安全信息。

(2)分批活动。各系部利用班会、微信等渠道，宣传网络安全教育知识等。

牵头部门：学生工作处(团委)。

联系相关网络安全企业，以案例讲解、现场观摩、情景模拟等方式，组织师生进行网络安全体验，近距离感知网络安全，增强网络安全意识，提升网络安全风险防范能力。

牵头部门：现代教育中心。

四、工作要求。

(一)高度重视，加强组织领导。举办宣传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，各部门要高度重视，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。

(二)加强宣传报道和信息报送。各牵头部门和参与部门要在宣传周期间大力宣传报道。现代教育中心负责做好摄影摄像工作，留存图片影像资料。各牵头部门要指定专人根据活动情况及时向宣传部提交活动动态，活动结束后请于9月28日提交总结，提交材料要图文并茂，有条件的可配以视频资料。宣传部指定专人负责，及时向省高工委报送我院活动信息，并在活动结束后及时将总结材料报省高工委。

**网络安全应急预案演练方案篇七**

随着信息技术的飞速发展，网络的快速发展已经成为我们现代社会的必然趋势，网络已经成为我们生活中不可或缺的一部分。然而，随着网络越来越普及，网络安全问题也越来越严重，网络攻击已经成为了我们时刻面临的威胁。因此，建立网络安全应急预案非常必要。

网络安全应急预案是一份应对网络安全问题的计划，它包括预先制定的针对网络攻击和安全漏洞的应急措施，以及应急响应流程和规范。网络安全应急预案的建立是保障信息安全的必需措施之一，也是信息化建设的重要内容。它能够帮助组织对网络攻击做出正确的反应，减少攻击造成的损失，并尽快恢复到正常运行状态。

网络安全应急预案应该围绕以下几个方面展开。首先，应提前做好网络攻击和安全漏洞的预防工作，减少被攻击的可能性。其次，应该将网络安全问题纳入到组织的风险评估中，及时发现并处理安全漏洞。第三，在攻击或安全漏洞出现后，应及时启动应急响应预案，开展应急处置措施，快速恢复受害者的服务和业务。最后，应该对事件过程和处置结果进行回顾和总结，不断改进和完善应急预案。

建立网络安全应急预案需要重视以下几个方面。首先，应该对组织内部的信息系统和网络现状进行全面了解，及时发现安全漏洞。其次，在预案制定过程中，应该充分考虑组织的业务特点和安全风险情况，根据不同风险情况，采取不同措施。第三，在预案执行时，需要赋予相关人员相应的权限和职责，确保执行顺畅。最后，应建立应急演练机制，定期检验和验证应急响应预案的可行性。

总之，建立网络安全应急预案是保障信息安全、为网络应急响应提供依据和指导的重要步骤。要保证预案的实际效果，需要充分考虑组织业务特点和网络环境风险，制定合理的应急措施和流程，及时发现并修复安全漏洞，合理分配资源和职责，全面检验预案的可行性，不断完善并提高应急响应能力。只有这样才能有效应对各类网络安全问题，维护企业的信息安全。在应急预案的制定过程中，需要充分考虑组织的业务特点和网络环境风险，综合评估可能出现的安全问题。根据风险评估结果，合理分配资源和职责，建立起对应的应急响应措施和应急协作机制。在制定应急预案的过程中，需要考虑到以下几个因素：

在制定应急预案之前，需要对组织内部的网络运行环境进行全面调研和评估，识别可能存在的安全漏洞和威胁。同时也要对外部的攻击手段和技术进行研究和评估，尽量对未来可能会出现的网络安全风险做出准确的预测。在此基础上，才能更好地制定应对措施。

2.制订应急响应计划。

应急预案是制定应急响应计划的基础，要根据实际情况制定出合理的应对方案，将计划细分成多个阶段并确立阶段目标。在应急响应计划中，需要列出应急响应的程序、流程、职责和应急人员的联系方式，还要明确应急响应的.部署方案和措施。

3.建立应急协作机制。

建立应急协作机制是应急预案的重要组成部分，它涉及到与各种专业团队和机构的协作。应急协作机制应该根据组织的业务特点和风险情况，制定出合适的模式。注意到，应急协作机制的建立不仅需要内部人员的协作，还需要考虑到外部专业团队的协助。

4.加强应急物资与设备准备。

进行有效的应急响应除了应急人员的准备和熟悉应急预案外，还应该加强应急物资与设备的准备。例如:应急通讯工具、网络安全设备、备用电源设备，强化应急响应的物质保障。同时，也要确保这些物资的实时更新和配备。

5.持续性改进。

随着网络运行环境和技术的不断变化，网络安全问题也在不停地演进和变化。因此，应急预案并非一次性制定即可，需要持续性地更新和改进。同时需要对事故过程和应急响应的效果进行评估和调整，不断提高应急响应的效率和准确性。

总之，建立网络安全应急预案需要的是全面的考虑、合理的规划和全体人员的配合。应急预案的制定离不开实际情况的评估，也离不开各方面资源的支持。通过制定、完善和实践网络安全应急预案，未来可以更有效地应对各类安全问题，保障网络安全与技术创新的健康发展。网络安全是当今社会最大的挑战之一，对于一个组织而言，网络安全的重要性更是不言而喻。一旦发生网络安全事件，组织可能将面临严重的损失，比如阻碍业务运营，丢失机密信息、客户的信任等等。因此，建立完善的网络安全应急预案是组织必须做的工作之一。

首先，应急预案需要强调风险评估和分类。通过对组织的网络和业务环境进行评估，可以识别不同类型和程度的网络安全威胁，并分类建立响应机制。例如，对于内网攻击和外网入侵，需要采取不同的应急措施和协作机制。

其次，应急响应计划需要涉及全部层面。在建立应急协作机制时，不仅要考虑内部应急响应团队的配合与协作，同时还要考虑如何与外部资源及境外公司、机构协调应对一些复杂的网络安全事件，以便更快地获得第一手信息。因此，建立良好的外部沟通渠道非常重要。

第三，应急预案需要针对不同类型的事件建立不同的应急响应流程，以更好地应对复杂的安全威胁。例如，对于勒索软件攻击和恶意程序感染，需要采取不同的应急响应机制和协作方式。此外，还建议建立常用漏洞的应急预案，并配合相关的漏洞修补措施。

第四，应急预案的制定应该切合实际，其应对手段和技术应该符合组织的实际情况和业务特点。同时，应对措施还应该考虑到不同的运营环境和地理位置，以保证在面临不同的安全威胁时，可以采取最优的应急响应方式。

最后，应急预案的实施需要充分准备和培训，以确保应急响应人员具备应急实施的实际操作经验和高效应对网络安全事件的能力。同时，也需要定期应急演练来检测应急响应团队的协作和应急响应能力。

总之，建立完善的网络安全应急预案对于任何一个组织而言都是至关重要的，特别是在当前这个网络安全风险越来越高的时代，如无相关部署，不仅组织自身的安全会受到威胁，还有可能会波及到其他有关联的组织和用户。因此，成立专业的网络安全团队，制定完善的应急预案，摸清组织风险情况以及制定有效的应对计划都是非常必要的。同时，应急预案的更新升级和演练也是必备措施，以让整个组织能够更全面、更有效地应对不可预知的风险。网络安全已成为现今最为重要的挑战之一，对于任何组织而言，建立完善的网络安全应急预案是必须的。一个好的预案应该包括风险评估和分类、全面的应急响应流程、结合业务特点针对不同事件采取不同措施、考虑与外部资源协作和切合实际的应对技术方案等方面。同时，应急预案的实施还需要做好准备和培训，定期进行应急演练。只有建立了完善的预案，组织才能有效应对一些复杂的安全威胁，保证业务的顺畅运转，避免被安全威胁给带来的各种损失。而且保证网络安全不能是一成不变的，应急预案也需要定期更新升级，确保应急响应团队的能力跟上环境的变化，才能更好地强化网络安全保障技术，加强预防，降低风险。

**网络安全应急预案演练方案篇八**

为切实维护校园和谐稳定，加强我校重大突发舆情网络文化建设与管理，最大限度地避免、减少和消除因网络舆情造成的各种负面影响，营造良好的学校舆论环境，根据学校工作实际，特制定本预案。

1.准确把握、快速反应。网络舆情事件发生后，力争在第一时间发布准确、权威信息，稳定公众情绪，最大限度地避免或减少公众猜测和新闻媒体的不准确报道，掌握新闻舆论的主动权。

2.加强引导、注重效果。提高正确引导舆论的意识和工作水平，使突发事件的新闻发布有利于学校工作大局，有利于维护全体师生的切身利益，有利于社会稳定和人心安定，有利于事件的妥善处置。

3.讲究方法、提高效能。坚持网络舆情突发事件处置与新闻发布同时布置、同时落实，新闻发布依托主流强势媒体、积极引导和应用好外来媒体，处置舆情突发事件的各行政部门密切配合新闻发布工作等行之有效的做法，确保以最短的时间、最快的速度，发布最新消息，正确引导舆论。

4.严格制度、明确职责。完善新闻发布制度，加强组织协调和归口管理，健全制度，明确责任，严明纪律，严格奖惩。

1.加大学校网站，增强校园网的吸引力和感染力。配合上级部门做好网上正面宣传，唱响主旋律，打好主动仗。

2. 加强对校内网络信息内容管理，对各科室采写的信息，在负责人审核通过后，由各单位网络信息员通过学校网络信息处理平台报送，党支部进行文字审核。

3. 围绕网上热点问题，在师生访问频繁、关注度高的新闻网站、门户网站以及互动类网站等，撰写正面评论文章;对涉及本校工作的网上不实言论，适时以论坛贴文的形式主动进行引导，消除负面影响。

4. 围绕学校改革发展的重点、难点问题以及重大突发事件，在校园网上主动导贴，积极跟贴，及时发布正面观点，做好正面引导工作。

5. 针对别有用心的造谣、歪曲和攻击，开展理直气壮的舆论斗争，发表即时性评论，及时跟贴，批驳反面声音，澄清事实，抵御负面言论的渗透和传播。

一旦发生网络舆情突发事件，学校应根据网络舆情的`发生发展启动应急预案，决定各相关部门介入突发事件的处置。审定网络舆情应对方案，决定新闻发布的口径、原则和内容，确定负责新闻发布、审定新闻发布稿和接受记者采访的领导和相关部门负责人。对网络舆情处置过程中出现的新情况、新问题及时进行会商，提出解决方案及处置措施，确定相关部门进行处置。遵纪依法对当事人、责任人、责任单位提出处理和责任追究意见建议，并按有关程序移交相关部门处理。具体应对机制如下：

1. 建立网络舆情监控信息员机制。各二级学院和职能部处应确定政治素质好、责任心强、反映机敏、熟悉网络的师生担任网络舆情监控信息员，对涉及上海电力学院的网络舆情实行监控和引导，特殊时期安排专人24小时监控，加强网上舆情监测和应对。重点加强对学生、家长关心、群众关注的重点论坛的实时监控，及时了解社情民意，监测舆情发展动向。

2.建立快速报告机制。舆情监控信息员发现有关学校的不良舆情信息后要立即向主管领导汇报，经批准后，根据事件进展情况适时采取应对措施。

3. 建立网络舆情研判机制。要通过跟踪分析，把握舆论发展走向，分析判断突发及重大舆情的程度，提出合理化建议。根据事件严重程度决定是否召开会议和向上级领导汇报。

4. 建立快速查核机制。对网络反映的情况，需要调查的，要迅速组织力量开展调查，与网络抢时间，并注重周密谋划，妥善处置、严控因处置不当造成不良后果。经查证属实，并构成违纪的，按照有关规定严肃查处;与事实不符或者出入较大的，及时予以澄清。对恶意造谣、干扰学校正常学习生活开展的，依法送交有关部门处理。

5. 建立信息发布机制。加大在学校微信群有关热点事件的进展情况，完善新闻发布制度，形成权威、畅通的信息发布渠道。如发生舆情突发事件，校级领导同党办、校办迅速拟定新闻发布内容和方案，经领导小组审定后，按照统一的口径，选择合适的时机发布，并组织媒体进行报道，让正面信息先声夺人，为网民提供权威声音，营造有利舆论。按照“及时、准确、公开、透明”的原则，不论是网络舆情初步形成，还是网络舆论已成热点，都主动澄清事实真相，争取网民理解支持。

6. 学校档案馆要做好舆情突发事件的全程处置工作的文字材料、声音、影像的记录和保存保管工作。

**网络安全应急预案演练方案篇九**

为确保我院网络安全，保证各项工作高效、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。

学院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。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。

二、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）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。

（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。

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。

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，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。

文档为doc格式。

**网络安全应急预案演练方案篇十**

为科学应对网络与信息安全突发事件，建立健全我校网络与信息安全应急响应工作机制，有效预防、及时控制和最大限度消除我校信息安全各类突发事件的危害和影响，确保校园网络和重要信息系统安全，特制定本预案。

本预案适用于全校范围内自建自管的网络和信息系统，尤其是校园网主干设施和重要信息系统的突发信息安全事件的应急处置。

按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，防范为主，加强监控，统一领导，快速反应，协同工作，科学处置。采取全校统一管理和各部门分级负责的管理体制，学校主要负责人是信息技术安全工作的第一责任人，主管信息化工作的校领导为信息技术安全工作的分管责任人，各部门负责人为其部门信息安全工作的第一责任人。

遇突发的网络与信息安全事件,应及时控制事态，限制在最短时间、最小范围内，使影响和损失减少到最低程度，并尽快恢复学校正常的教学、科研和生活秩序。落实工作责任和责任追究制。凡在执行本预案过程中，因工作延误、渎职或不服从指挥、不及时处理，产生严重后果的，要追究相关人员责任。

网络与信息安全突发事件依据发生过程、性质和特征的不同，可分为以下四类：

1.网络攻击事件：校园网络与信息系统因病毒感染、非法入侵等造成学校网站或部门二级网站主页被恶意篡改，应用系统数据被拷贝、篡改、删除等。

2.设备故障事件：校园网络与信息系统因网络设备和计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪。

3.灾害性事件：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素导致网络与信息系统损毁，造成业务中断、系统宕机、网络瘫痪。

4.信息内容安全事件：利用校园网络在校内外传播法律法规禁止的信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益等。

网络与信息安全突发事件依据可控性、严重程度和影响范围的不同，可分为以下四级：

iv级（一般）：某一局部网络或信息系统受到一定程度损坏，对学校某些工作有一定影响，但不危及学校整体工作的安全事件。

（一）学校成立网络与信息安全事件应急处置工作组（以下简称工作组），工作组在网络安全与信息化领导小组指导下工作。全面负责和统一指挥校园网络与信息安全重大突发事件的应急处置工作。工作组组长由主管信息化工作的副校长和主管宣传的副书记担任，小组成员由党政机关及有关单位部门负责人和各学院主管网络安全与信息化的负责人组成。工作组下设办公室，设在网络与信息中心，办公室主任由网络与信息中心主任担任。

（二）网络与信息中心作为学校校园网建设运行的主管部门，负责校园主干网络与主要信息系统安全事件的预防、监测、报告和应急处置，负责对学校其他部门主管的网络信息系统的安全防护情况进行日常检查、指导和督促，必要时网络与信息中心协助相关主管部门完成突发事件的技术处理。

（一）按照《信息安全事件分类分级指南》，对校园网络通信平台、应用平台和信息系统采取相应安全保障措施。

（二）建立健全安全事件预警预报体系，严格执行校园网络与信息系统安全管理制度，常年坚持校园网络安全工作值班制度。加强对校园网络与学校网站等重点信息系统的监控和安全管理，做好相关数据日志记录，确定合理规则，对校园网络进出信息实行过滤及预警。实行信息网上发布审批制度，对可能引发校园网络与信息安全事件的信息，要认真收集、分析、判断，发现有异常情况时，及时防范处理并逐级报告。

（三）做好服务器的数据备份及登记工作，建立灾难性数据恢复机制。

（四）特殊时期，根据学校要求和部署，由网络与信息中心进行统一安排，组织专业技术人员对校园网络和信息系统采取加强性保护措施，对校园网络通信及信息系统进行不间断监控。

（一）预案启动。

发生校园网络与信息安全事件后，网络与信息中心和突发安全事件的信息系统建管部门应尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认突发事件的类别和等级，并参照下述响应机制对突发事件进行处置。

（二）应急响应。

1、应急响应机制。

iii级或iv级突发事件响应：网络与信息中心和突发安全事件的信息系统建管部门自行负责应急处置工作，有关情况报分管校领导。

ii级突发事件响应：网络与信息中心立即上报分管校领导和校园网络与信息安全事件应急处置领导小组，由领导小组统一组织、协调指挥进行应急处置。

i级突发事件响应：网络与信息中心立即上报分管校领导和校园网络与信息安全事件应急处置领导小组，领导小组再上报至市公安局等相关部门，由北京市相关部门会同我校校园网络与信息安全事件应急处置领导小组统一组织、协调指挥应急处置。

2、应急处理方式。

（1）网络攻击事件：判断攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的ip地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的ip地址，及时关闭入侵的端口，限制入侵的ip地址的访问。对于已经造成危害的，应立即采用断开网络连接的\'方法，避免造成更大损失和影响。

内部入侵：查清入侵来源，如ip地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（2）设备故障事件：判断故障发生点和故障原因，迅速抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（3）灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。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。

（4）信息内容安全事件：接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息的传播，根据网站相关日志记录查找信息发布人并做好善后处理；对公安机关要求我校协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（5）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理。不能处理的及时咨询信息安全公司或顾问。

（三）后续处理。

1、安全事件进行最初的应急处置后，应及时采取行动，抑制其影响进一步扩大，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、安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应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。

（四）记录上报。

网络与信息系统安全事件发生时，应及时向校领导和校园网络与信息安全事件应急处置领导小组汇报，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。

（五）结束响应。

系统恢复运行后，网络与信息中心对事件造成的损失、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网络监察部门报案。

校园网络与信息安全应急处置是一项长期的、随时可能发生的工作，必须做好各项应急保障工作。

（一）人员保障。

重视信息系统安全队伍建设，不断提高工作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。

（二）技术保障。

重视信息系统的建设和升级换代，重视网络安全整体方案的不断完善，加强技术管理，确保信息系统的稳定与安全，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。

（三）资金保障。

网络与信息中心应根据校园网络与信息系统安全预防和应急处置工作的实际需要，申报网络与信息系统关键设备及软件的运行维护专项资金，提出本年度应急处置工作相关设备和工具所需经费，并上报至财务处纳入年度财政预算，由学校给予资金保障。

（四）安全培训和演练。

举办教职工网络与信息系统安全知识培训，加强对教职工和学员的计算机操作、信息技能、网络和信息系统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。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。

**网络安全应急预案演练方案篇十一**

在平日的学习、工作和生活里，难免会突发一些事故，为了避免事情往更坏的方向发展，时常需要预先编制应急预案。写应急预案需要注意哪些格式呢？以下是小编收集整理的网络安全应急预案，仅供参考，希望能够帮助到大家。

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。

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