企业网络安全方案通用

企业网络安全方案通用 1

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。

一、指导思想

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。

二、组织领导及职责

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。

三、安全保护工作职能部门

1、负责人：__

2、信息安全技术人员：__

四、应急措施及要求

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。连接国际互联网的计算机绝对不能存储涉及国家秘密、工作秘密、商业秘密的文件。

企业网络安全方案通用 2

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，进一步提高我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，确保我校校园网络与信息安全，结合学校实际工作，特制定本预案。

第一章总则

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

第二条本预案的指导思想是确保学校有关计算机网络及信息的安全。

第三条本预案适用于发生在无锡市洛社高级中学校园网络中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。

第二章组织指挥和职责任务

第五条学校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校信息网络的灾害应急工作，全面负责学校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

第六条处置措施

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，学校网络与信息安全主管部门及网管中心要预先对灾害预警预报体系进行建设，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。网管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。属于大型灾害的，在向领导小组报告的同时，还应向市公安局计算机信息安全监察处报告。

（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与信息安全领导小组报告，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。

第七条处置程序

（一）发现情况

学校网管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、上网帐号等信息，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、网络设备故障：一旦发现，应及时联系设备供应商。

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。不能处理的可以请示相关的专业人员。

（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，首先向学校网络与信息安全应急处置工作小组汇报。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，可以同时向公安局相关部门汇报。中、小型级别的`灾害，可以只向学校的网络与信息安全应急处置领导小组汇

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，或在安全相关网站发布了预警而学校信息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，由学校的网络与信息安全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。

第九条技术保障

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。

第十条物资保障

学校要根据近三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财政计划和预算，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。

第十一条训练和演练

加强全学校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，确保发灾后应急救助手段及时到位和有效。

企业网络安全方案通用 3

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。

企业网络安全方案通用 4

为提高处理医院信息网络系统安全突发事件的应对能力，及时应对网络突发故障，维护正常的门诊、住院工作流程和医疗程序，保障患者正常就医，特制定医院信息系统应急规划。

一、组织机构：

略

二、应急范围

范围：单个计算机、外围设备、服务器、网络设备、电脑病毒感染、停电

三、报告程序及规划启动

a、报告程序

如出现网络安全问题，网管员应立即上报主任与分管院长或总值班室，请求一定的协助。

b、规划启动

当整个网络停止使用时，各科室采取以下方式进行运行

1、各医生工作站采取手式开处方。

2、门诊收费处应随时准备发票，进行手工收费。

3、门诊西药房与中药房采取手工发药，并应备用药品价格表（如价格有调整药剂科应及时通知各药房更改）

4、住院科室用药，查阅处方后到住院西药房采取借药方式进行。

5、住院西药房采取手工方式发药操作，并做好各科室药品的登记。

6、住院收费处，如当日有病人需出院，告知病人原因并留下病人电话，等系统恢复后通知病人来院进行结算

四、预防措施

1、软件系统故障：操作员可以关闭计算机并拔除电源插座，过一分钟后重新启动计算机将自动修复错误。同时信息科应做好软件操作系统的快速备份，在最短的时间内恢复计算机运行。（如不能正常关闭计算机，可直接按主机电源 5 秒强行关闭，此操作对计算机有损害请尽量避免）

2、硬件系统故障：如发现在鼠标、键盘、显示器或不能启动计算机，请与信息科联系，经网管员检测不能立即修复

好备用计算机的.工作。

3、打印机系统故障：如打印机在工作中出现异常（打印头温度过高、打印头发出异响、进纸器卡纸），操作员应立即关闭打印机电源与信息科联系，网管员经检测不能修复，可采用备用打印机替换，计算机操作员不能带电拆解打印机与计算机外部器件。

4、网络：网线、交换机、光纤模块、ups 电源故障，由信息科进行检修，如不能在立即修复采用备用设备进行更换，保证网络的正常运行。

5、服务器

a、ups 电源故障：我们现有两台服务器电源是接入 1kv 的 ups 电源，保证在停电状态下医院数据库的安全，如 ups 出现故障，服务器暂时接入市电启动服务器运行。

b、软件系统故障：当软件系统出现故障，网管员应采取相应的方法尽快解决，如不能立即解决应立即起用报告制度与手工操作方式（见后）。

c、硬件系统故障：当硬件系统出现故障，不能修复应立即起用备用服务器，替代主服务器进行工作。

d、数据安全与病毒防范：网管员应每天检查服务器的数据备份与实时数据的运行状况，如出现异常应立即停止工作站操作查找原因，并对实时数据采取备份保留。网管员应定时升级服务器病毒数据库，定时手工查杀病毒并打开服务器实时病毒监控系统，如工作站受到病毒感染应立即关闭计算机，等待网管员通知开机。

企业网络安全方案通用 5

（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。