南京工业大学校园网络
与信息安全应急处置预案

一、总 则

第一条 指导思想

减轻和消除网络与信息安全事件突发时间造成的危害和影响，维护学校的安全稳定。

第二条 适用范围

本预案根据《江苏省教育系统网络安全事件应急预案》编制，适用于我校自建自管的网络与信息系统，尤其是校园网主干设施和重要信息系统安全突发事件的应急处置。

第三条 处置原则

快速、有效。网络与信息安全事件应急处置，依照“统一领导，快速反应，密切配合，科学处置”的组织原则和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的协调原则，充分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

二、组织指挥和职责任务

第四条　组织指挥

由学校网络安全和信息化领导小组或授权的领导组织指挥。

第五条 职责任务

全校网络与信息安全事件应急处置工作由学校网络安全和信息化领导小组统一指导，由网络与信息化建设工作小组指挥和协调。各相关单位须坚决执行学校的决定，密切配合，履行职责。

三、处置措施和处置程序

第六条 发现情况

学校信息服务部信息中心（下文简称信息中心）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 60 天访问日志保存工作,以保障及时发现并处置灾害及突发性事件。

第七条 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。

第八条 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，阻断网络连接，进行现场保护，协助调查取证，定位入侵的IP地址，对相关事件进行跟踪，密切关注事件动向。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。有关违法事件移交公安机关处理。

3．信息被篡改：这种情况，要求一经发现，第一时间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。不能处理的可以请示相关的专业人员。

第九条 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。出现灾害时，先断开外网连接，再通过消息平台把灾害信息第一时间发送至系统（网站）管理人员和部门负责人。信息中心参照《江苏省教育系统网络安全事件应急预案》对安全事件危害程度的定义，对于发生的 I、II、III 级网络安全事件，向学校网络安全和信息化领导小组汇报，由网络安全和信息化领导小组决定是否启动该预案。

一旦启动该预案，有关人员应及时到位，并按照《江苏省教育系统网络安全事件应急预案》的要求处理事件，填写《教育系统网络安全事件情况报告》（见附件 1）和《教育系统网络安全事件总结调查报告》（见附件 2）。

灾害的发生单位，必须按照学校信息中心要求，在事件发生后 24 小时内完成事件书面报告《南京工业大学网络和信息安全事件总结调查报告》（见附件 3）。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，需向上级主管部门汇报。

报告应包括以下内容：事件发生时间、地点、事件内容，涉及计算机的 IP 地址、管理人、操作系统、应用服务，损失，事件性质及发生原因，事件处理情况及采取的措施；事故报告人、报告时间等。

第十条 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。

第十一条 预案终止

灾害险情或灾情已消除，或者得到有效控制后，由学校网络安全和信息化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。

四、保障措施

第十二条 队伍保障

学校专设网络技术安全岗、信息技术安全岗和信息内容安全岗，对学校各学院、部门进行相关业务培训，提高网站及信息系统管理人员的安全意识。敏感期间，信息中心安排 24 小时专人值班。学校各学院、部门安排相关人员 24 小时监控其网站及信息系统的运行状况。

第十三条 技术保障

完善网络安全整体方案，加强技术管理，确保网络与信息系统的稳定安全。配备防火墙系统、网页内容过滤器、网络防病毒系统；网管人员可通过远程网管环境及时反应；已购网络安全产品厂家须提供稳定的技术支持；网页的互动栏目采用先审后发机制；信息系统项目立项时，在技术参数中对信息系统安全级别有明确要求；网站及信息系统正式上线前严格测试，必须安装学校统一部署的服务器安全软件。

第十四条 资金保障

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维专项资金，提出本年度应急处置工作相关设备和工具所需经费，上报至财务处纳入年度预算，由学校给予资金保障。

第十五条 物质保障

关键岗位配备有移动电话，保证24小时开机。

第十六条 训练和演练

通过校内各种宣传形式对师生员工进行正面引导、宣传并落实学校关于网络安全的各项规章制度。在学校统一部署下，按规定召开季度及年度网络安全工作会议，开展安全事件演练，定期组织自查。

五、工作要求

第十七条 所有值班人员必须坚持在岗、保证通讯畅通、工作认真负责。

附件：1.教育系统网络安全事件情况报告

2.教育系统网络安全事件总结调查报告

3.南京工业大学网络和信息安全事件总结调查报告

南京工业大学

2020年1月9日

附件 1

教育系统网络安全事件情况报告

单位名称：（需加盖公章） 事发时间：_____年__月__日__时__分

联系人姓名		电子邮箱	
手机		传真	
事件分类	☐ 有害程序事件 ☐ 网络攻击事件 ☐ 信息破坏事件 ☐ 设备设施故障 ☐ 灾害事件 ☐其他_____		
事件分级	☐Ⅰ级 ☐Ⅱ级 ☐Ⅲ级 ☐Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统网址和 IP 地址：_____ 3.系统主管单位/部门：_____ 4.系统运维单位/部门：_____ 5. 系统使用单位/部门：_____ 6.系统主要用途：_____ _____ 7.是否定级 ☐是 ☐否，所定级别：_____ 8.是否备案 ☐是 ☐否，备案号：_____		

	9.是否测评 □是　□否 10．是否整改 □是　□否
事发单位及事发网络和信息系统功能描述	
事件发生时间、事态发展与处置的简要经过。	
事件初步估计的危害和影响（影响程度、影响人数、紧急损失等情况）	
事件原因的初步分析	

已采取的应急措施和效果	
是否需要应急支援及需支援事项和工作建议	
安全负责人意见（签字）	
主要负责人意见（签字）	

备注：省教育网络安全应急办联系电话：025-83752162。

附件 2

教育系统网络安全事件总结调查报告

单位名称：（需加盖公章）　　报告时间：_____年___月__日

联系人姓名		手机	
		电子邮件	
事件分类	☐ 有害程序事件　☐ 网络攻击事件 ☐ 信息破坏事件　☐ 设备设施故障 ☐ 灾害事件　　☐其他_____		
事件分级	☐Ⅰ级　☐Ⅱ级　☐Ⅲ级　☐Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统网址和 IP 地址：_____ 3.系统主管单位/部门：_____ 4.系统运维单位/部门：_____ 5.系统使用单位/部门：_____ 6.系统主要用途：_____ _____ 7.是否定级 ☐是　☐否，所定级别：_____ 8.是否备案 ☐是　☐否，备案号：_____		

	9.是否测评 □是　　□否 10.是否整改 □是　　□否
事件发生的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情况	
事件的安全整改措施	
存在问题及建议	
安全负责人意见（签字）	
主要负责人意见（签字）	

备注：省教育网络安全应急办联系电话：025-83752162。

附件 3

南京工业大学网络和信息安全事件总结调查报告

单位名称：（需加盖公章）　　报告时间：_____年___月___日

联系人姓名		手机	
		电子邮件	
事件分类	☐ 有害程序事件　☐ 网络攻击事件 ☐ 信息破坏事件　☐ 设备设施故障 ☐ 灾害事件　　☐其他_____		
事件分级	☐Ⅰ级　☐Ⅱ级　☐Ⅲ级　☐Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统网址和 IP 地址：_____ 3.系统使用单位/部门：_____ 4.系统运维单位/部门：_____ 5.系统主要用途：_____ _____ 6.是否定级 ☐是　☐否，所定级别：_____ 7.是否备案 ☐是　☐否，备案号：_____ 8.是否测评 ☐是　☐否		

	9.是否整改 □是　　□否
事件发生的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情况	
事件的安全整改措施	
存在问题及建议	
安全负责人意见（签字）	
主要负责人意见（签字）	

备注：南京工业大学网络和信息安全联系电话：025-83172363。