安徽理工大学文件

校政〔2022〕104号

关于印发《安徽理工大学网络安全事件应急预案》的通知

各单位:

《安徽理工大学网络安全事件应急预案》已经学校研究通过，现予印发，请认真遵照执行。

安徽理工大学

2022年7月7日

安徽理工大学网络安全事件应急预案

第一章　总　则

第一条　编制目的

为提高学校应对网络安全事件的应急处置能力，建立健全科学、有效、反应迅速的网络安全应急工作机制，预防和减少校园网突发类网络安全事件及其造成的影响、损害，保障校园网络与信息系统稳定运行。

第二条　编制依据

依据《中华人民共和国网络安全法》《国家网络安全事件应急预案》《教育系统网络安全事件应急预案》《安徽理工大学网络安全管理办法》等文件，结合学校实际制定本预案。

第三条　适用范围

本预案适用于预防和处置学校范围内自建自管的网络设施与信息系统，尤其是校园网主干网络设施和重要信息系统安全事件的应急处置。

第四条　事件分类与分级

（一）网络安全事件分类

1.有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件。如系统感染勒索病毒、网站被上传 webshell、系统被渗透或控制等。

2.网络攻击事件分为拒绝服务攻击事件、后门攻击事件、

漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。如系统遭 DDOS 攻击、SQL 注入攻击、尝试爆破密码等。

3.信息破坏事件分为信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件。如发现网络上存在与系统数据高度雷同的数据，或发现业务数据被篡改等。

4.信息内容安全事件是指通过网络发布、传播法律法规禁止信息，炒作敏感问题并危害国家安全、社会稳定和公共利益的事件。如网站被悬挂反动标识，或有人在网站互动区发布非法内容等。

5.设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障。如服务器硬件故障，机房供电中断等。

6.灾害性事件是指由于自然灾害等其他网络安全事件导致的网络安全事件。如机房遭遇火灾、地震等。

7.其他信息安全事件是指不能归为以上分类的网络安全事件。

网络安全事件依据影响范围、严重程度，可分为以下四级:

（二）网络安全事件分级

应急响应级别	响应条件	影响范围	控制事态的能力
Ⅰ级（特别重	发生严重有害程序事件、网络攻击事件、	对学校正常工作造	事态发展超出学校控制能力

大）	设备设施故障、灾害性事件造成全校大规模网络与信息系统瘫痪；发生严重信息内容安全事件和信息破坏事件。	成特别严重损害。	的安全事件。
II级（重大）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成全校性网络与信息系统瘫痪；发生信息内容安全事件和信息破坏事件。	对学校正常工作造成严重损害。	事态发展超出技术部门控制能力，需要学校各部门协同处置的安全事件。
III级（较大）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成学校某一区域网络与信息系统瘫痪。	对学校正常工作造成一定损害。	学校技术部门及事发部门可处理的安全事件。
IV级（一般）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成学校某一局部网络与信息系统故障。	对学校某项工作造成影响，但不危及学校整体工作。	学校技术部门及事发部门可处理的安全事件。

第五条　工作原则

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、谁运维谁负责、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。

第二章　组织机构与职责

第六条　领导机构与职责

安徽理工大学网络与信息安全领导小组（以下简称“领导小组”）负责指挥协调学校网络安全事件应急处置工作。

第七条　办事机构与职责

网络与信息安全领导小组办公室（以下简称“领导小组办公室”，设在现代教育技术中心）依据网络安全事件的性质、影响范围、严重程度等因素确定事件等级，向领导小组和分管校领导报告，提出应对措施和建议，并为网络安全应急处置提供技术支持。

第八条　各内设机构职责

内设机构承担本单位网络安全主体责任，负责本单位的网络与信息安全的管理和网络安全事件应急处置工作。

第三章　应急处置

第九条　预案启动

发生校园网络安全事件后，现代教育技术中心进行最初的应急处置，抑制其影响进一步扩大，限制潜在的损失与破坏，同时会同事发部门尽最大可能收集事件相关信息，初步评定事

件的类别和等级，向领导小组报送《安徽理工大学网络安全事件情况报告》(附件 2)，并参照下述响应机制对网络安全事件进行处置。

第十条　应急响应

网络安全事件应急响应分为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级四个等级，分别对应特别重大、重大、较大和一般网络安全事件。

发生Ⅰ级网络安全事件时，现代教育技术中心先行通过技术手段紧急处置，同时将具体情况上报领导小组和分管校领导，领导小组会商后将事件详细情况上报至省教育厅、淮南市公安局等相关部门，由上级部门会同学校统一协调指挥应急处置工作。

发生Ⅱ级网络安全事件时，现代教育技术中心先行通过技术手段紧急处置，同时将具体情况上报领导小组和分管校领导，由领导小组统一协调指挥党政办公室、现代教育技术中心、党委宣传部、保卫处等相关职能部门和事发单位开展应急处置工作。

发生Ⅲ级网络安全事件时，现代教育技术中心会同事发单位开展应急处置工作，将有关情况备案后报分管校领导。

发生Ⅳ级网络安全事件时，现代教育技术中心会同事发单位开展应急处置工作。

第十一条　详细应急处置流程见附件 1

第十二条　应急响应结束

消除安全隐患、系统恢复正常运行后。

Ⅰ级网络安全事件由上级网络安全应急处置部门决定应急

响应结束。

II级网络安全事件由领导小组根据应急处置结果决定应急响应结束。

III级、IV级网络安全事件由事发单位填写《安徽理工大学网络安全事件总结调查报告》(附件3)，报送领导小组办公室。

第四章　调查与评估

第十三条　调查与评估

特别重大、重大网络安全事件由领导小组组织开展调查和总结评估工作，并将调查评估结果汇总上报教育厅相关部门。

较大网络安全事件由领导小组办公室会同事发单位开展调查和总结评估工作，并将调查评估结果汇总报领导小组。

一般网络安全事件由事发单位自行组织开展调查和总结评估工作，并将调查评估结果汇总报领导小组办公室。

网络安全事件的调查和总结评估工作应在应急响应结束后5天内完成，应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施，并填报《安徽理工大学网络安全事件总结调查报告》(附件3)。

网络安全事件中存在违法犯罪行为的，应及时向公安机关报案。

第五章　预防与保障措施

第十四条　日常管理

预防网络安全事件是一项长期、持续的工作。各部门应落实网络安全等级保护制度，做好日常网络安全检查、重要数据

的容灾备份，提高信息系统的安全保障能力。

第十五条　宣传教育

加强网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣讲活动。

第十六条　经费保障

现代教育技术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，提出年度经费预算，由学校给予资金保障。

第十七条　定期培训和演练

网络安全技术人员要定期参加专业知识培训，增强防范意识和应急处置能力，有针对性地开展应急演练，确保相关措施有效落实。

第六章　附　则

第十八条　预案实施时间

本预案自印发之日起实施。

第十九条　预案解释

本预案由网络与信息安全领导小组办公室负责解释。

附件 1

安徽理工大学网络安全事件应急处置工作流程

第一章　总　则

第一条　为切实做好网络安全事件应急处置工作，特制订应急处置工作流程。

第二章　有害程序事件处置流程

第二条　有害程序事件主要指计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网络内嵌恶意代码和其他有害程序事件等。一旦发现感染有害程序，应执行以下应急处置流程:

1.立即切断感染有害程序计算机与网络的连接，同时对该计算机的重要数据进行数据备份;

2.对事件进行初步处置，进行事发情况报告（填写附件 2，下同);

3.利用防病毒软件对该计算机进行杀毒处理，并对同一局域网内其他计算机进行有害程序扫描和清除工作；若感染有害程序的设备是服务器或者主机系统，经技术人员研判，如有必要，应告知有关单位做好相应的清查工作；同时进行事中情况报告;

4.如果满足下列情况之一的，事件应升级响应;

（1）现行防病毒软件无法清除该有害程序的;

（2）信息系统在 1 小时内无法处理完毕的;

（3）有害程序不断通过网络扩散的;

5.有害程序清理完毕后，恢复系统和相关数据，检查数据的完整性;

6.有害程序事件处理完毕，将计算机重新接入网络;

7.进行事后整改报告（附件 3，下同），总结防范经验，进行安全加固。

第三章　网络攻击事件处置流程

第三条　网络攻击事件主要包括拒绝服务事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他攻击事件等。

第四条　一旦发现网络非法入侵（远程控制、后门攻击等）行为，应执行以下应急处置流程:

1.发现有关服务器被网络非法入侵后，应立即切断服务器与网络的连接;

2.对事件进行初步处置，进行事发情况报告;

3.技术人员对入侵行为进行鉴定，做好必要的记录，妥善保存有关日志和审计信息;

4.通过技术手段进行分析，追查攻击源，修改防火墙等设备的安全配置阻断入侵渠道；分析后台数据操作日志，判断是否发生数据失窃；同时进行事中情况报告;

5.事态无法控制或造成严重后果，事件应升级响应；情节严重的、构成违法犯罪的，需及时上报公安机关立案侦查;

6.修复或重建被攻击或破坏的系统，重新将恢复后的系统接入网络;

7.进行事后整改报告，强化安全防范措施，总结防范经验，进行安全加固。

第五条 拒绝服务攻击（系统访问流量异常、无法正常访问等现象）事件处置流程。一旦发现遭受拒绝服务攻击而导致系统无法正常访问时，应执行以下应急处置流程:

1.发现可能遭受拒绝服务攻击时，首先对事件进行初步处置，进行事发情况报告;

2.技术人员对受攻击行为进行鉴定，做好必要记录，妥善保存有关日志和审计信息;

3.通过技术手段进行分析，追查攻击源，修改路由器、防火墙等设备的安全配置阻断攻击源，缓解、消除事件的影响，同时进行事中情况报告;

4.事态无法控制或持续造成影响，事件应升级响应;

5. 消除攻击隐患，提取相关攻击证据后，恢复系统正常运行;

6.进行事后整改报告，强化安全防范措施，总结防范经验。

第四章 信息破坏安全事件处置流程

第六条 信息破坏事件主要包括业务数据非法篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

一旦发现信息破坏事件应执行以下应急处置流程:

1.首先对事件进行初步处置，进行事发情况报告;

2.立即组织技术人员对事件进行勘察，做好必要记录，妥善保存有关日志和审计信息;

3.通过技术手段进行分析，阻断信息破坏的渠道消除安全隐患，实施备份数据恢复工作，有关工作实施同时进行事中情况报告;

4.事态无法控制或造成恶劣影响，事件应升级响应；情节严重的、构成违法犯罪的，需及时上报公安机关立案侦查;

5.事件处理完毕强化安全防范措施，系统恢复正常运行。

6.进行事后整改报告，总结防范经验。

第五章　信息内容安全事件处置流程

第七条　信息内容安全事件是指通过网络发布、传播法律法规禁止信息，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、社会稳定和公共利益的事件。

一旦发现信息内容安全事件，按照学校关于意识形态和舆情管理工作的相关文件进行处置。

第六章　设备设施故障事件处置流程

第八条　设备设施故障事件主要指IT设备和与之配套设备设施的软硬件发生故障等。

第九条　数据中心机房物理环境发生相关事件时，应进行事发情况报告，同时执行以下应急处置流程:

1.外部供电中断：工作人员应立即查看是否切换到UPS供电，同时联系总务部了解具体情况，若停电时间在1小时内，

关注 UPS 电源供电状态即可；若停电时间超过 1 小时，及时发布暂停网络服务公告后，按相关流程关闭网络、服务器等设备，等待供电恢复后再按规范逐步恢复网络与信息服务。

2. 火灾：火势较小可以控制，应立即切断有关部位的非消防电源，利用现场配置的手提二氧化碳灭火器进行灭火。

火势已起无法控制，机房内人员应迅速撤离，关闭发生火灾的机房大门，切断有关部位的非消防电源，启动相应机房的七氟丙烷气体喷射装置进行灭火。同时向保卫处报告火警，请求支援。

3. 渗水：切断电源，更换浸水设备，及时清除机房积水，采取措施消除渗漏水隐患。

4. 机房精密空调故障：立即联系空调售后进行处理。

机房软硬件设备、设施故障排除后，系统恢复正常运行，进行事后总结报告，采取措施防止类似事件发生。

第七章　灾害性事件处置流程

第十条　灾害性事件主要包括：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素导致的网络与信息系统损毁，造成业务中断系统、系统宕机、网络瘫痪等。有关应急处置流程如下：

1. 首先对事件进行初步处置，进行事发情况报告；

2. 发生的灾害为自然灾害时，根据当时的实际情况，在保障人身安全的前提下，首先保障数据安全，其次是核心设备、普通设备安全。具体方法包括：硬盘的拔出（同步在硬盘上做

好标识）与保存，设备的断电与拆卸、搬迁等;

3.发生灾害性事件后，立即组织技术人员对事件进行勘察，做好必要记录，妥善保存有关日志和审计信息；涉及设备损坏的须详细梳理并评估硬件和软件受损程度，若能够自行修复，应立即用备件替换受损部件实施修复；对于不能自行恢复的，应尽快联系相关供应商、技术部门或售后服务部门，详细说明受损情况，及时寻找安全可靠的地点，拆卸并搬迁未受损设备，重新构建新的系统和网络，并将相关数据迅速予以恢复；若相关备份均无法恢复，须立即向有关厂商请求紧急支援；有关工作实施同时进行事中情况报告;

4.情节严重乃至事态无法控制的，事件应升级响应;

5.处理完毕后及时恢复系统或网站运行;

6.事后进行总结报告。

第八章　其他信息安全事件处置流程

第十一条　其他信息安全事件发生后，有关应急处置流程如下:

1.首先对事件进行初步处置，进行事发情况报告;

2.根据实际情况，与事发涉及的相关单位协商后妥善处理具体问题;

3.情节严重乃至事态无法控制的，事件应升级响应;

4.处理完毕后及时恢复相关服务;

5.进行事后整改报告，总结防范经验，强化安全防范措施。

第九章　附　则

第十二条 本流程自发布之日起施行；未尽事宜，由网络与信息化安全领导小组办公室负责解释。

附件 2

安徽理工大学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

联系人姓名		电子邮箱	
手机号码		传真	
事件分类	□有害程序事件　□网络攻击事件 □信息破坏事件　□信息内容安全事件 □设备设施故障事件　□灾害性事件 □其他信息安全事件		
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			
事发时间、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	
单位主要负责人意见	（签字）

附件 3

安徽理工大学网络安全事件总结调查报告

单位名称:（需加盖公章）　事发时间:　　年　　月　　日

联系人姓名		电子邮箱	
手机号码		传真	
事件分类	□有害程序事件　□网络攻击事件 □信息破坏事件　□信息内容安全事件 □设备设施故障事件　□灾害性事件 □其他信息安全事件		
事件分级	□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级		
事件概述			
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	
存在的问题及建议	
单位主要负责人意见	（签字）

安徽理工大学党政办公室　　2022年7月7日印发