郑州工程技术学院文件

校政字〔2022〕16号

关于印发《郑州工程技术学院网络安全事件应急预案》的通知

学校各单位:

根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》等文件要求，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，现制定《郑州工程技术学院网络安全事件应急预案》，请各单位认真贯彻落实。

郑州工程技术学院

2022年3月15日

郑州工程技术学院网络安全事件应急预案

第一章 总 则

第一条 为完善学校网络安全事件应急工作机制，规范网络安全事件工作流程，提高我校网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校安全稳定和健康发展，特编制本预案。

第二条 本预案编制依据为《中华人民共和国网络安全法》《国家网络安全事件应急预案》和《教育系统网络安全事件应急预案》等文件。

第三条 按照教育部《教育系统网络安全事件应急预案》的规定，本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、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、灾害性事件和其他事件（**附件 1**）。其中信息内容安全事件，应参照有关规定和办法。

第四条 参照教育部《教育系统网络安全事件应急预案》的事件分级规定，结合我校实际，以及网络安全事件可能造成的危害、可能发展蔓延的趋势等，网络安全事件分为特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件（**附件 2**）。

第五条 为保障网络安全事件应急预案有效实施，确定以下工作原则。

1. 统一指挥、密切协同。学校网络安全和信息化领导小组统筹协调全校网络安全应急指挥工作，建立与省教育厅、郑州市网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

2. 分级管理、强化责任。按照“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，信息与网络管理中心对全校网络安全工作负主体责任，各单位、各部门对所属网站和业务信息系统的安全工作负直接责任。各级领导班子主要负责人是网络安全工作第一责任人。

3. 预防为主、防战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

第二章 组织机构与职责

第六条 学校网络安全和信息化领导小组负责统筹协调全校网络安全事件应急工作，指导学校各单位、各部门网络安全事件应急处置。当发生特别重大网络安全事件、重大网络安全事件时，在上级统一指挥下开展应急处置工作，具体参照相关规定执行。

第七条 信息与网络管理中心负责网络安全事件应急管理事务性工作，对接省教育网络安全应急办公室，向学校网络安全和信息化领导小组报告网络安全事件情况，提出较大网络安全事件、一般网络安全事件的应对措施、建议和意见，统筹组织学校网络安全监测工作，做好应急处置的技术支撑工作。

第八条 各单位、各部门负责所属网站和业务信息系统的网络安全事件应急工作，根据本预案制定有关网络和信息系统的网络安全事件专项应急预案，切实落实相关工作。

第三章 监测与预警

第九条 安全监测工作包括事件监测、威胁监测。信息与网络管理中心通过多种渠道对学校网络进行监测，发现已经发生的学校网络安全事件；通过多种途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息，应及时上报学校网络安全和信息化领导小组。

第十条 建立学校网络安全事件预警制度。按照紧急程度、发展态势和可能造成的危害程度，网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生的特别重大、重大、较大和一般网络安全事件。

第四章 应急响应及事件处置

第十一条 网络安全事件发生后，事发单位可以做初步处置，并应立即启动专项应急预案，根据不同的事件类型和事件原因，采取科学有效的应急处置措施，尽最大努力将影响降到最低，并

注意保存网络攻击、网络入侵或网络病毒等证据。同时，应立即向学校信息与网络管理中心报告，不得迟报、谎报、瞒报、漏报。

信息与网络管理中心组织研判，认定为网络安全事件的，须立即向学校网络安全和信息化领导小组报告；初判为重大及以上网络安全事件的，经学校网络安全和信息化领导小组批准后，立即向省教育网络安全应急办报告。属于人为破坏活动的，由学校保卫处确认后报当地公安机关。

第十二条 网络安全事件应急响应分为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级等四级，分别对应特别重大、重大、较大和一般网络安全事件。Ⅰ级为最高响应级别。

1. Ⅰ级和Ⅱ级响应

由上级网络安全应急办统一组织应急处置工作，具体要求以上级网络安全应急办部署为准。

(1) 掌握事态及时上报。跟踪事态发展情况，及时向学校网络安全与信息化领导小组报告，经批准后按要求将事态发展变化情况和处置进展情况上报上级网络安全应急办。

(2) 控制事态防止蔓延。根据事件发生原因，结合相应专项应急预案，采取各种技术措施，管控手段，最大限度阻止和控制事态蔓延。

(3) 消除隐患恢复系统。针对性制定解决方案，及时组织恢复受破坏的网络和信息系统。

(4)取证溯源协调配合。在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极协调配合上级部门和当地公安机关开展调查取证工作。

2. III级响应

发生较大网络安全事件，由学校网络安全和信息化领导小组确认并启动III级响应。学校网络安全和信息化领导小组履行应急处置工作统一领导、指挥、协调的职责。

(1)信息与网络管理中心负责整理、汇总相关信息、掌握事态发展变化情况和处置进展情况，掌握全校网络和信息系统受到事件涉及或影响的情况，随时向学校网络安全和信息化领导小组报告相关重要事项。

(2)及时形成《网络安全事件情况报告》（附件3），经学校网络安全和信息化领导小组同意后报上级网络安全应急办。

(3)根据事件发生原因，结合相应专项应急预案，采取各种技术措施，管控手段，最大限度阻止和控制事态蔓延。

(4)消除隐患恢复系统。针对性制定解决方案，及时组织恢复受破坏的网络和信息系统。

(5)取证溯源协调配合。在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极协调配合上级部门和当地公安机关开展调查取证工作。

3. IV级响应

由信息与网络管理中心确认并启动IV级响应。信息与网络管理中心履行应急处置工作领导、协调的职责。

(1)协助事发单位整理、汇总相关信息，掌握事态发展变化情况和处置进展情况，及时向学校网络安全和信息化领导小组报告相关重要事项。

(2)事发单位根据专项应急预案开展应急处置工作，采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

(3)协助事发单位消除隐患，恢复遭受破坏的网络和信息系统，开展问题定位和溯源追踪工作。

第十三条 各级响应按照以下权限和流程，确定响应的结束。

1. I级和II级响应结束，以上级网络安全应急办部署为准。

2. III级响应结束，经应急工作组批准报学校网络安全和信息化领导小组同意后，根据实际决定III级响应的结束，并通报有关情况。

3. IV级响应结束，由事发单位完成应急处置后，报学校信息与网络管理中心同意后，根据实际决定IV级响应的结束。

第五章 调查与评估

第十四条 特别重大网络安全事件和重大网络安全事件的调查处理和总结评估工作根据上级有关规定执行。

较大网络安全事件由信息与网络管理中心组织开展调查处理和总结评估工作，并将调查评估结果报学校网络安全和信息化领导小组。

一般网络安全事件由信息与网络管理中心会同事发单位组织开展调查处理和总结评估工作，在每年的网络安全工作总结中向学校网络安全和信息化领导小组汇总报告调查评估结果。

网络安全事件的调查处理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《网络安全事件整改报告》**（附件4）**。

第六章 预防工作

第十五条 做好网络安全事件日常预防工作，进一步细化应急操作流程，按照网络安全等级保护等相关要求，落实各项防护措施，做好网络安全检查、风险评估和数据备份，加强信息系统的安全保障能力。

第十六条 加强网络安全监测预警，及时发现并处置安全威胁，全面掌握全校网站和业务信息系统情况，建立全校网络安全监测预警和通报机制，并指导监督各单位、各部门及时修复安全威胁，全面排查安全隐患，提高发现和应对网络安全事件的能力。

第十七条 学校将网络安全教育作国家安全教育的重要内容，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。信息与网络管理中心应充分利用网络安全宣传周等各种活动，开展网络安全基本知识和技能的宣传活动，提高师生的网络安全意识。

第七章 工作保障

第十八条 按照“谁主管谁负责，谁使用谁负责”的原则，各单位、各部门应落实网络安全应急工作责任制，明确具体岗位和人员，建立健全应急工作机制。

第十九条 信息与网络管理中心作为全校网络安全应急技术支撑单位，应加强网络安全技术队伍建设，提升网络安全技术能力，做好网络安全事件的监测预警、预防防护、应急处置、应急技术等支撑工作。

第二十条 加强与周边高校、网络安全专业机构行业学会（协会）等单位的合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制。

第二十一条 学校保障每年用于网络安全等级保护测评、网络安全监测和检测评估、信息系统安全升级改造和防护加固、网络安全教育培训、网络安全事件处置和安全运维等5项重点工作的经费。

第二十二条 学校对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰；对不按照规定制定预案和组织开展演练、迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照有关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

第八章 附 则

第二十三条 本预案应根据实际情况适时修订，修订工作由学校网络安全和信息化领导小组组织。

第二十四条 本预案由学校网络安全和信息化领导小组负责解释。

第二十五条 本预案自印发之日起试行。

附件 1

网络安全事件分类

网络安全事件分为有害程序事件、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、灾害性事件和其他网络安全事件等。

（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、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（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。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络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、社会稳定和公众利益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

附件 2

事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

（1）符合下列情形之一的，为特别重大网络安全事件：

①重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

①重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

①重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

（4）除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

附件 3

网络安全事件情况报告

单位名称：（加盖公章）

事发时间：__年__月__日__分

联系人姓名		手机	
		电子邮箱	
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		

事件发现与处置的简要经过	
事件初步估计的危害和影响	
事件原因的初步分析	
已采取的应急措施	
是否需要应急支援及需支援事项	
信息与网络管理中心负责人意见（签字）	
网络安全和信息化领导小组主要负责人意见（签字）	

附件 4

网络安全事件整改报告

单位名称：　　（加盖公章）

报告事件：_____年_____月____日

联系人姓名		手机	
		电子邮箱	
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、图片及其他说明）	
事件的影响及恢复情况	
事件的安全整改措施	
存在问题与建议	
信息与网络管理中心负责人意见（签字）	
网络安全和信息化领导小组主要负责人意见（签字）	

郑州工程技术学院　　2022年3月15日印发