河南工学院文件

校〔2023〕98号

关于印发《河南工学院网络安全事件应急预案》的通知

各部门（单位）：

现将学校研究通过的《河南工学院网络安全事件应急预案》印发给你们，请认真组织学习，抓好贯彻落实。

2023年8月18日

河南工学院网络安全事件应急预案

第一章　总则

第一条　编制目的。为建立健全学校网络安全事件应急工作机制，规范网络安全事件应急处置流程，提高应急处置能力，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，根据国家相关法律法规和上级文件精神，结合学校实际，制定本预案。

第二条　编制依据。《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《河南省网络安全事件应急预案（2021修订版）》、《教育系统网络安全事件应急预案》、《信息安全技术信息安全事件分类分级指南》、《河南省教育系统网络安全事件应急预案（2022修订版）》等相关规定。

第三条　适用范围。学校范围内网络与信息安全事件的应急处置。

第四条　工作原则

（一）统一指挥，密切协同。河南工学院网络安全和信息化领导小组（以下简称网信领导小组）统筹协调网络安全应急指挥工作，建立与省教育厅、省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。

（二）分级管理，强化责任。按照“谁主管谁负责，谁运维谁负责，谁使用谁负责"的原则，学校各部门是本部门网络安全工作的责任主体，负责本部门网络安全应急工作，部门主要负责人是网络

安全工作的第一责任人。

（三）预防为主，平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判和预警工作，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，抓早抓小，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　网络安全事件分级

第五条　事件定义。根据《信息安全技术信息安全事件分类分级指南》(以下简称《指南》），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。

第六条　事件分类。根据《指南》，网络安全事件可划分为恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件和其他事件等十类事件。

第七条　事件分级。网络安全事件分为四级：特别重大网络安全事件(I 级）、重大网络安全事件(II 级）、较大网络安全事件(III 级）和一般网络安全事件(IV 级）。

（一）符合下列情形之一的，为特别重大网络安全事件(I 级）：

1.校园网发生全校性大规模瘫痪，90％以上用户无法正常上网，对学校正常工作造成特别严重损害。

2.关键信息基础设施或核心业务信息系统遭受特别严重损失,造

成系统大规模瘫痪，90％以上核心业务信息系统丧失业务处理能力。

3.网络病毒在全校大面积爆发。

4.关键信息基础设施或核心业务信息系统的重要敏感信息或关键数据丢失或被窃取、篡改。

5.其他对学校安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

（二）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(II 级):

1.校园网发生大面积瘫痪，50％以上用户无法正常上网，对学校正常工作造成严重损害。

2.关键信息基础设施或核心业务信息系统遭受严重系统损失，造成系统大面积瘫痪，50％以上核心业务信息系统的业务处理能力受到重大影响。

3.网络病毒在学校多个部门大面积爆发。

4.其他对学校安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（三）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(III 级):

1.校园网发生局部瘫痪，学校某一个部门的所有用户无法正常上网，对学校正常工作造成较大损害。

2.重要业务信息系统遭受较大系统损失，明显影响系统效率，业务处理能力受到影响。

3.网络病毒在学校某一个部门广泛传播。

4.重要业务信息系统的信息或数据发生丢失或被窃取、篡改、假冒。

5 其他对学校安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

（四）一般网络安全事件(IV 级）：

除（一）（二）（三）中所述情形外，对学校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

第三章　组织机构及职责

第八条　领导机构与职责。学校网信领导小组是学校网络安全事件应急处置的领导机构，统筹制定学校网络安全和信息化发展战略、宏观规划和重大决策，统筹协调学校网络安全和信息化重大问题，统筹推进学校信息化项目建设；贯彻落实上级有关部门关于网络安全和信息化建设工作的决策部署，根据学校信息化发展需要，按照“统一领导、统一规划、统一标准、分布实施”的原则，制定学校网络安全和信息化发展中长期规划、重要政策、规章制度与重大措施；贯彻落实网络意识形态工作责任制、涉密网络安全工作责任制，加强网络安全管理与监督、舆情监控及引导；指导、督促和检查各部门网络安全和信息化工作的实施；论证通过全校网络安全与信息化建设年度预算和实施计划。

第九条　办事机构与职责

（一）学校网信领导小组办公室职责

学校网信领导小组办公室（以下简称“网信办”)统筹协调学校网络安全和信息化日常工作，贯彻执行领导小组形成的各项决议；起草学校网络安全和信息化工作发展规划和实施方案；建立健全和落实网络安全和信息化建设的各项管理规章制度；组织、协调学校网络与信息安全重要活动，督促、指导学校各二级单位落实网络安全与信息化工作，对网络信息安全违规事件进行查处，并提出责任追究建议。

（二）其他部门职责

1、党委办公室牵头组织重大敏感时期、重要活动、重要会议期间发生的网络信息安全事件的协调处置；负责涉密级信息网络泄密类事件的处理。

2、党委宣传部分管学校网络信息安全，负责信息内容安全管理与监督、舆情监控及引导等工作。

3、信息化建设与管理办公室分管学校网络信息技术安全，负责建设学校网络安全防护系统、校园网络安全设备日常运维管理、组织网络安全巡查、攻防演练、渗透测试等工作。

4、学校其他各部门。按照“谁主管谁负责，谁运维谁负责，谁使用谁负责" 的原则，负责本部门网站和各类信息系统安全事件的预防、监测、报告和应急处置工作；参照本预案制定本部门有关信息系统的网络安全事件专项应急预案，承担本部门网络安全责任。

第四章　监测与预警

第十条 预警分级。学校建立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。

第十一条 安全监测。网信办统筹组织开展学校网络和信息系统的安全监测工作。各部门对本部门信息系统（网站）的运行状况进行密切监测，重要监测信息应及时向网信办报告，不得迟报、谎报、瞒报、漏报。

第十二条 预警研判。各部门组织对监测信息进行研判，认为需要立即采取防范措施的，应及时报告网信办。网信办对监测信息进行研判，对网络安全事件发生的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时通知有关部门；对可能发生较大及以上等级的网络安全事件情况，网信办应立即向学校网信领导小组报告，并由学校相关部门将有关情况向省教育厅和省市网络安全应急管理部门报告。

第十三条 预警发布。网信办可根据监测研判情况，发布橙色以下（含橙色）预警。需发布红色预警的，报学校网信领导小组批准后统一发布。对达不到预警级别但又需要发布警示信息的，网信办可发布风险提示信息。预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施、时限要求和发布部门等。

第十四条 预警响应

（一）红色预警响应

1.网信办组织预警响应工作，联系省教育厅、省市网络安全职能部门、专业机构和专家，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调调度各方资源，做好各项准备，重要情况报学校网信领导小组及省教育厅和省市网络安全应急管理部门。

2.网信办组织跟踪和分析研判，密切关注事态发展，做好监测分析和信息搜集工作；开展应急处置或准备、风险评估；密切关注舆情动态，加强教育引导，采取有效措施管控风险。

3.有关部门按照网信办要求，实行24小时值守，相关人员保持通信联络畅通。

4.网信办做好与专业机构沟通协调的准备工作；信息办及相关部门进入待命状态，研究制定应对方案，检查设备、软件工具等，确保处于良好状态。

（二）橙色预警响应

1.网信办组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

2.网信办密切关注事态发展，有关重大事项及时通报有关部门。

3.信息办及相关部门保持联络畅通，检查应急设备、软件工具等，确保处于良好状态。

（三）黄色、蓝色预警响应

网信办、信息办和有关部门根据预案，组织做好预警响应工作。

第十五条 预警解除。网信办根据实际情况，确定是否解除预

警，及时发布预警解除信息。

第五章　应急处置

第十六条　初步处置。网络安全事件发生后，事发部门网络与信息系统运维人员应第一时间采取断网等有效措施先期处置，将损害和影响降到最小范围，保留现场，立即报告本部门 CIO 和主要责任人，同时向网信办报告。网信办进行初步分析研判，初判为特别重大(I 级）、重大(II 级）和较大(III 级）网络安全事件的，由网信办负责按程序处置，同时以口头方式报告省教育厅；一般网络安全事件(IV 级)由信息办和事发部门直接处置。涉及人为主观破坏事件，应报告当地公安机关。

第十七条　应急响应。网信办组织有关部门尽最大可能收集网络安全事件相关信息，根据事件级别、事件类型和事件原因，采取科学有效的应急处置措施，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。

(一)I 级和 II 级响应

发生特别重大和重大网络安全事件，由网信办向学校网信领导小组提出启动 I 级和 II 级响应的建议，经批准后，成立应急工作组。

1.启动指挥体系

工作组进入应急状态，履行应急处置工作统一领导、指挥、协调的职责。工作组成员保持 24 小时联络畅通，网信办 24 小时值守。

信息办以及相关职能部门和二级部门进入应急状态，在工作组的统一领导、指挥、协调下组织人员开展应急处置或支援保障工作，

启动 24 小时值守。

2.掌握事件动态

（1）跟踪事态发展。事发部门与网信办保持联系，及时填写《网络安全事件情况报告》，详见附件 1,将事态发展变化情况和处置进展情况上报网信办。

（2）检查影响范围。网信办立即全面了解学校的网络和信息系统（网站）是否受到事件的波及或影响，并将有关情况及时报省教育厅。

（3）及时通报情况。网信办负责整理上述情况，重大事项及时报工作组和省教育厅，并通报学校有关部门。涉及人为破坏事件的同时报告公安机关。

3.决策部署

应急工作组组织党委办公室、党委宣传部、保卫处、信息办等部门以及校内外相关技术专家及时研究对策，制定处置方案，对处置工作进行决策部署。

4.处置实施

（1）控制事态防止蔓延。信息办应在第一时间采取各种技术措施、管控手段，包括但不限于断开网络、关闭服务器、设置黑名单、暂停账号等，最大限度阻止和控制事态蔓延。

（2）消除隐患恢复系统。根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患。对业务连续性要求高的受破坏网络与信息系统（网站）要在保证安全的前提下及时组织恢复。

（3）调查取证。事发系统的服务器等设备在学校核心机房的，由信息办负责问题定位和溯源追踪工作；不在学校核心机房的，立即将相关设备封存，由事发部门配合信息办完成问题定位和溯源追踪工作。处置时必须做好相关证据的保存工作。根据需要积极配合省教育厅和省市网络安全相关部门开展调查取证。

（4）信息发布。党委宣传部根据实际，组织网络安全突发事件的应急新闻工作，统一负责对外新闻发布和舆论引导工作。未经批准，其他部门不得擅自发布相关信息。

（5）请求支持。处置中需要技术及工作支持的，由网信办根据实际，报请工作组批准后，报请省教育厅、省教育和科研计算机网网络中心以及省市网络安全相关部门支持。

（6）次生事件处置。工作组立即组织排查和制定方案，防止发生次生事件。

(二)III 级响应

1.信息办和事发部门进入应急状态，按照相关专项应急预案做好应急处置工作。

2.事发部门及时填写《网络安全事件情况报告》，详见附件 1，报网信办。网信办将有关重大事项及时报网信领导小组，并根据情况通报有关部门。

3.信息办负责采取各种技术措施、管控手段阻止和控制事态蔓延。事发系统的服务器等设备不在学校数据中心的，由事发部门立即将相关设备封存，配合信息办完成问题定位和溯源追踪工作，处置时

必须做好相关证据的保存工作。

4.事发部门根据网信办要求，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

（三）IV 级响应

事发部门自行做好应急处置工作，尽快消除隐患、恢复系统，处置中需要其他部门和配合和支持的，由网信办予以协调。

第十八条 应急结束

（一）I 级、II 级、III 级响应结束

网信办提出建议，报网信领导小组批准后结束，相关情况及时向省教育厅和省市网络安全相关部门等有关部门报告。

（二）IV 级响应结束

由事发部门完成应急处置后，报网信办核实，核实后自行解除 IV 级响应状态。

第六章 调查与评估

第十九条 较大、重大和特别重大网络安全事件由网信办组织有关部门开展调查处理和总结评估工作，并将调查评估结果上报网信领导小组，根据网信领导小组批示报教育厅；一般网络安全事件由事发部门自行组织开展调查处理，并将调查结果报网信办。

总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施，详见附件 2。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 日内完成。

第七章 预防工作

第二十条 日常管理。信息办按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统及网站的安全保障能力。各部门要做好网络安全事件日常预防工作，根据本预案制定相关的专项应急预案和配套的管理制度，建立完善的应急管理体制。

第二十一条 监测预警和通报。网信办应全面掌握学校信息系统情况，建立学校网络安全监测预警和通报机制，并指导、监督学校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。各部门收到网信办、信息办发出的网络安全风险通报后应及时修复安全威胁，存在困难的，及时向网信办报告，由网信办组织力量及时协助修复。

第二十二条 应急演练。网信办每年组织针对特别重大或重大网络安全事件的跨部门的应急演练，检验和完善预案，提高实战能力。

第二十三条 宣传教育。充分利用各种传播媒介，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，开展网络安全知识宣传活动。

第二十四条 工作培训。学校将网络安全事件的应急知识列为领导干部和有关人员的培训内容，各部门按要求参加网络安全培训，加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

第八章 工作保障

第二十五条 机构和人员。各部门应落实网络安全应急工作责任制，明确分管网络安全的责任领导及网络安全联络员，把责任落实到具体部门、具体岗位和个人，根据要求指派人员参加学校网络安全应急培训和应急演练。

第二十六条 技术支撑。学校加强网络安全应急技术支撑队伍建设和网络安全物资保障，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。

第二十七条 信息共享与应急合作。学校各部门要加强与网信办的信息共享，保持信息畅通。学校加强与省教育厅、省市网络安全职能部门、中国教育和科研计算机网、兄弟院校、行业学会和网络安全专业机构等单位的合作，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。

第二十八条 经费保障。学校为网络安全应急工作提供必要的经费保障，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。

第二十九条 责任与奖惩。学校对网络安全事件应急管理工作中作出突出贡献的集体和个人给予表彰和奖励。对未有效落实预案各项规定（如：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、渎职行为等）的部门，依照相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。

第九章　附则

第三十条　预案管理。本预案原则上每年评估一次，根据实际情况适时修订，修订工作由网信办组织。各部门应根据本预案制定或修订本部门的网络安全事件应急预案。各预案要做好与本预案的衔接，并报网信办。

第三十一条　本预案由学校网络安全和信息化领导小组负责解释。

第三十二条　本预案自发布之日起施行。

附件：

1. 网络安全事件情况报告
2. 网络安全事件总结调查报告

附件 1

网络安全事件情况报告

部门名称：（需加盖公章）　　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	□一般网络安全事件□较大网络安全事件 □重大大网络安全事件□不能判定等级		
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	
网络安全分管负责人意见（签字）	
主要负责人意见（签字）	

附件 2

网络安全事件整改报告

部门名称：（需加盖公章）　　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	
网络安全分管负责人意见（签字）	
部门主要负责人意见（签字）	

发：各位校领导、校党委委员。

河南工学院院长办公室　　2023 年 8 月 18 日印发