河南省教育厅办公室文件

教办科技〔2022〕144号

河南省教育厅办公室
关于印发《河南省教育系统网络安全事件
应急预案（2022修订版）》的通知

各省辖市、省直管县（市）教育局，各高等学校，厅直各单位（学校）：

现将《河南省教育系统网络安全事件应急预案（2022修订版）》印发你们，请认真贯彻执行。《全省教育系统网络安全事件应急预案》（教科技函〔2019〕113号）同时废止。

河南省教育厅办公室

2022年5月9日

河南省教育系统网络安全事件应急预案（2022 修订版）

1　总则

1.1 编制目的

建立健全全省教育系统网络安全事件应急工作机制，规范网络安全事件处置流程，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，维护国家安全、公共安全和社会稳定。

1.2 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》（GB/Z 20986—2007）等相关规定。

1.3 适用范围

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、设备设施故障、灾害性事件和其他事件。

本预案适用于河南省各级教育行政部门及其直属机构（以下简称教育行政部门）、各级各类学校（含幼儿园）、河南省教育科

研计算机网的网络安全事件应对工作。省属中等职业学校网络安全事件处置参照高校有关要求进行；信息内容安全事件的预防和处置按照《河南省互联网信息内容管理应急预案》执行。

1.4　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。适用于全省教育系统网络安全事件为三级：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，为重大网络安全事件

` 教育行业关键信息基础设施或统一运行的省级核心业务信息系统（网站）遭受严重损失，造成系统大面积瘫痪，丧失业务处理能力。

a 教育行业关键信息基础设施或统一运行的省级核心业务信息系统（网站）的重要敏感信息、关键数据丢失或被窃取、篡改、假冒，对国家安全和社会安全稳定构成严重威胁。

b 计算机病毒在全省教育系统大面积爆发。

c 其他对教育系统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。

（2）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

` 教育行业关键信息基础设施或核心业务信息系统（网站）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

理能力受到重大影响。

a 教育行业关键信息基础设施或核心业务信息系统（网站）的重要敏感信息、关键数据丢失或被窃取、篡改、假冒，对国家安全和社会安全稳定构成较大威胁。

b 计算机病毒在全省教育系统较大范围内爆发。

c 其他对全省教育系统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。

（3）一般网络安全事件

除上述情形外，对教育系统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。

1.5 工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持属地管理，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

2 组织机构与职责

2.1 领导机构与职责

省教育厅在省委网信委、教育部领导下，统筹协调全省教育系统全局性网络安全事件应急工作，指导市县教育行政部门、各高等学校网络安全事件应急处置工作。负责建立与省工信厅、省公安厅、省通信管理局、国家互联网应急中心河南分中心等职能部门、专业机构合作联动机制；根据实际情况，吸纳网络安全业

务主管单位和技术支撑部门参加应对工作。

2.2 办事机构与职责

省教育厅科学技术与信息化处（厅网信办）负责网络安全应急管理事务性工作，对接省网络安全应急办公室和教育部网络安全应急办，向厅网信领导小组报告网络安全事件情况，提出重大网络安全事件应对措施建议，做好网络安全事件的预防、监测、报告和应急工作，指导网络安全支撑单位做好应急处置的技术保障。

2.3 市县教育行政部门和学校职责

按照属地化管理原则，各市县教育行政部门、各级各类学校在属地党委政府、上级教育行政部门领导下，负责本地区、本单位网络安全事件预防、监测、报告和应急处置工作。按照“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，承担各自网络安全责任。

2.4 其他单位职责

省教科网网络中心负责指导协调全省教科网网络安全事件应急工作；省教育信息安全监测中心负责监测、报告网络安全事件和预警信息，为全省教育系统的网络安全事件应对提供决策支持；省教育系统网络安全应急支撑队伍负责配合开展事件处置和技术服务。

3 监测与预警

3.1 预警分级

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特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

省教育厅建立教育系统网络安全监测平台，开展网络安全的宏观监测，接收上级网络安全主管部门的预警信息，开展跨地区、跨部门的网络安全信息共享。各市县教育行政部门、各高等学校应分别建立本地、本单位网络安全监测体系，主动监测并发布预警信息，与省教育系统网络安全监测平台对接，共享监测预警数据。

3.3 预警研判和发布

各级教育行政部门和高校对监测信息进行研判，对发生网络安全事件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，应及时通知有关单位；对可能发生较大及以上网络安全事件的信息，应及时向当地网信办和上级教育行政部门报告。

厅网信领导小组根据监测研判情况，可面向全省教育系统发布黄色及蓝色预警信息，各市县教育行政部门和高校可发布蓝色预警信息。

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、完成时限和发布机关等。

对达不到预警级别但又需要发布警示信息的，省教育厅、各级教育行政部门和高等学校可发布风险提示信息。

3.4　预警响应

3.4.1　红色及橙色预警响应

（1）在省网络安全应急办和教育部网络安全应急办领导下，省教育厅组织预警响应工作，启动应急预案，协调调度各方资源，做好应对准备，重要情况及时报省网络安全应急办和教育部网络安全应急办。

（2）各级教育行政部门、各级各类学校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）各级教育行政部门、各级各类学校网络安全主管部门实行 24 小时值守，相关人员保持通信联络畅通，每日向当地网信办和上级教育行政部门报告一次工作进展。

（4）网络安全管理及技术支撑部门进入待命状态，研究制定应对方案，检查设备、软件工具等，时刻处于待命状态。

3.4.2　黄色预警响应

（1）省教育厅组织预警响应工作，联系有关部门、专业机构和专家，组织对事态发展情况进行跟踪研判，协调资源调度和部门联动的各项准备工作。

（2）各市县教育行政部门、各级各类学校网络安全主管部门实行 24 小时值守，相关人员保持通信联络畅通，密切关注事态发展，重要情况及时报当地网信办和上级教育行政部门。

（3）相关应急技术支撑队伍保持联络畅通，检查应急设备、软件工具等，确保处于良好状态。

3.4.3 蓝色预警响应

各市县教育行政部门和各级各类学校启动相应应急预案，组织开展预警响应工作。

3.5 预警解除

预警发布部门根据实际情况，确定是否解除预警，及时发布预警解除信息。

4 应急处置

4.1 事件报告

全省教育系统任何单位和个人都有义务向省内各级网络安全事件应急指挥机构和教育行政部门报告网络安全事件或隐患。

网络安全事件发生后，事发单位应立即启动应急预案，查清网络安全事件具体情况，实施处置并及时报送信息，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、计算机病毒等证据。经分析研判，初判为较大及以上网络安全事件的，应立即报告当地网信办和上级教育行政部门；对于人为破坏活动，应同时报当地公安机关。

事件报告信息需包括以下要素：报告时间、单位、报告人及联系方式，发生事件的网络与信息系统名称及运营使用管理单位、简要过程、采取的措施与效果等。《网络安全事件情况报告》样式详见附件 1。

对于当地网信、公安、工信等职能部门和上级教育行政部门要求核查的情况，各单位要认真调查、核对、及时报告。

4.2　应急响应

网络安全事件应急响应分为`级、a 级、b 级、c 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。`级为最高响应级别。

4.2.1 `级和a 级响应

接到省委网信委、教育部等上级主管部门关于启动`级和a级响应的通知后，省教育厅通知全省教育系统进入响应状态，开展以下工作

（1）启动指挥体系

全省各级教育行政部门、各级各类学校全面进入应急状态，在当地网信办和上级教育行政部门统一指挥、协调下，开展本地、本单位应急处置或支援保障工作。单位主要负责同志、分管负责同志保持 24 小时通信联络畅通，网络安全主管部门 24 小时值班。

（2）掌握事件动态

`跟踪事态发展。事发市县和单位密切跟踪事态发展，及时将事态发展变化情况、处置情况进行汇总整理，以《网络安全事件情况报告》的形式，报当地网信办和上级教育行政部门。

a 检查影响范围。各市县教育行政部门、各高校全面了解本地区、本单位主管范围内的网络和信息系统是否受到事件波及或影响，以《网络安全事件情况报告》的形式，报当地网信办和上

级教育行政部门。

b 及时通报情况。各地、各单位按照当地网信办和上级教育主管部门的统一部署，将相关情况通报有关单位或内设部门。

（3）处置实施

` 控制事态，防止蔓延。事发地区和单位要组织有关力量，尽快控制事态；督促运行单位有针对性地加强预防，防止事件蔓延至其他信息系统。

a 做好处置工作。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，组织恢复业务连续性要求高的受破坏网络与信息系统，提交《网络安全事件整改报告》（见附件 2）。

b 调查取证。事发单位应在保留相关证据的基础上，开展问题定位和溯源追踪工作，配合当地网信、工信、公安等部门开展调查取证。

c 信息发布。各级教育行政部门、各高校按照上级统一要求，开展对外信息发布，对受影响的用户进行解释。未经批准，不得擅自发布相关信息。

4.2.2 b 级响应

网络安全事件b 级响应由教育厅或市县网络安全主管部门根据事件性质和态势启动。

（1）事件发生地教育行政部门或高校的网络安全指挥机构进入应急状态，按照相关应急预案做好应急处置工作。

（2）事件发生地教育行政部门或高校跟踪掌握网络安全事态

发展，及时将网络安全事件的危害、影响、发展变化等情况报当地网信办和省教育厅。教育厅视情将情况通报相关地区和单位。

（3）处置中需要其他单位和网络安全应急技术支撑队伍配合和支持的，商请当地网信办或上级教育行政部门予以协调。省市两级和教育系统网络安全事件应急技术支撑队伍根据各自职责，积极配合和提供支持。

（4）有关市县和高校根据省教育厅通报的情况，结合各自实际有针对性地加强防范，防止造成更大影响和损失。

（5）处置实施。

`控制事态，防止蔓延。事件发生市县或高校实施技术措施、尽快控制事态，督促相关部门有针对性地加强防范，防止事件蔓延。

a 做好处置工作。事件发生市县或高校根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患，组织恢复业务连续性要求高的受破坏网络与信息系统，提交《网络安全事件整改报告》（见附件 2）。

b 调查取证。事发单位应在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合当地网信、工信、公安等部门开展调查取证工作，并及时向省教育厅报告有关情况。

4.2.3 c 级响应

事件发生地教育行政部门和高校按相关预案进行应急响应，做好应急处置工作，并报当地网信办和教育厅备案。

4.3 应急结束

4.3.1 Ⅰ级、a 级、b 级响应结束

由当地网信办和省教育厅按照上级要求和自身权限，将响应结束信息通报相关地方或高校。

4.3.2 c 级响应结束

事发市县教育行政部门或单位完成处置后，自行解除c 级响应，并报当地网信办和上级教育行政部门备案。

5 调查与评估

重大及以上级别网络安全事件由省级以上网络安全主管部门或教育部牵头调查处理，全省教育系统做好配合工作。较大网络安全事件由教育厅会同省辖市网信部门调查处理，并向省委网信办提交总结调查报告。一般网络安全事件由事发单位自行组织开展调查处理和总结评估工作，报当地网信办和上级教育行政部门备案。

网络安全事件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。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 30 天内完成。相关总结调查报告按照要求上报。

6 预防工作

6.1 日常管理

各地、各单位应做好网络安全事件日常预防工作，根据本预案制定完善相关的应急预案，明确职责分工，落实网络安全等级保护义务，及时更新网络安全和信息化部门人员信息，做好网络安全

检查自查，落实各项防护措施，提高应对网络安全事件的能力。

6.2 演练

省教育厅每年至少组织一次针对重大网络安全事件的应急演练，检验和完善应急预案，提高应急水平，锻炼应急队伍，完善应急机制。各市县教育行政部门和各高等学校每年至少组织一次应急演练。

6.3 宣传教育

充分利用网络安全宣传周、网络安全攻防大赛、学术研讨会、安全培训会、应急演练等各种形式，加大对有关法律、法规和政策的宣传力度，深入宣传《网络安全法》《数据安全法》《密码法》《个人信息保护法》，普及网络安全预防、预警、救助和减灾等基本知识，提高各级教育行政部门、各级各类学校的安全防护意识和应急处置能力。

6.4 工作培训

各单位应定期组织网络安全培训，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，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。

6.5 重要时期预防措施

在国家和我省重大活动、重要会议、招生录取期间，各级教育行政部门和各高校要加强网络安全事件的防范和应急响应。省教育厅将会同有关部门，加强网络安全监测和分析研判，及时预

警可能造成重大影响的风险和隐患，重点部门、重点岗位保持 24 小时值班，制定专门的应急预案，及时发现和处置网络安全事件和隐患。

7　工作保障

7.1　机构和人员

各单位应落实网络安全应急工作责任制，明确网络安全职能部门，按照“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，把网络安全应急工作责任落实到具体部门、具体岗位和个人，健全应急工作机制。

7.2　技术支撑

省教育厅将建立教育系统网络安全应急支撑保障队伍，作为省级网络安全应急支撑力量的有效补充，提供应急技术支援。各级教育行政部门要加强与网信、工信、公安、通信发展等部门的沟通协调，建立必要的网络安全信息共享机制。

7.3　基础平台

省教育厅加强省教育系统网络安全管理平台建设，通过已有“河南省教育系统网络安全监测系统”通报网络安全事件信息和网络安全威胁信息，做到早发现、早预警、早响应，增强教育系统网络安全预警和态势感知能力。各市县教育行政机构和各级各类学校应对通报的网络安全事件信息和网络安全威胁信息做到及时响应，提高应急处置能力。

7.4　物资保障

加强对网络安全应急装备、工具的储备，及时调整、升级软硬件工具，不断增强应急技术支撑能力。

7.5　经费保障

各地、各单位要利用现有政策和资金渠道，支持网络安全监测预警、应急演练、支撑队伍、值班值守、物资保障等工作开展。

7.6　责任与奖惩

省教育厅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和奖励；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，依照相关规定对有关责任人给予处分；涉嫌犯罪的，移送司法机关依法处理。

8.　附则

8.1　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。修订工作由省教育厅科学技术与信息化处负责。

各单位要根据本预案制定或修订本地区、本单位的网络安全事件应急预案。

8.2 预案解释

本预案由省教育厅科学技术与信息化处负责解释。

8.3　预案实施时间

本预案自印发之日起实施。

附件　1.网络安全事件情况报告

2.网络安全事件整改报告

3.网络安全事件分类

4.名词术语

5.网络和信息系统损失程度划分说明

附件 1

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___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

单位名称：（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）	
单位主要负责人意见（签字）	

附件 3

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 4

名词术语

一、重要网络与信息系统

所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

（参考依据：《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007））

二、重要敏感信息

不涉及国家秘密，但与国家安全、经济发展、社会稳定以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果

a) 损害国防、国际关系

b) 损害国家财产、公共利益以及个人财产或人身安全

c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等

d) 影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为

e) 干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责

f) 危害国家关键基础设施、政府信息系统安全

g）影响市场秩序，造成不公平竞争，破坏市场规律

h）可推论出国家秘密事项

i）侵犯个人隐私、企业商业秘密和知识产权

j）损害国家、企业、个人的其他利益和声誉。

（参考依据：《信息安全技术云计算服务安全指南》（GB/T31167-2014））

附件 5

网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下

a) 特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的

b) 严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的

c) 较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的

d) 较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

河南省教育厅办公室　　依申请公开　　2022 年 5 月 10 日印发