郑州市教育局处室函件

郑教科信函〔2022〕565号

郑州市教育局办公室
关于印发《郑州市教育系统网络安全事件应急预案》的通知

各开发区教育局，各区县（市）教育局，局直属各学校（单位），市属事业及各民办学校：

现将《郑州市教育系统网络安全事件应急预案》印发你们，请认真贯彻执行。

2022年8月23日

郑州市教育系统网络安全事件应急预案

为建立健全全市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。依据《河南省教育系统网络安全事件应急预案（2022修订版）》（教办科技〔2022〕144号），编制本案。

一、适用范围

本案适用于郑州市各级教育行政部门及其直属机构（以下简称教育行政部门）、中初等以下学校（含幼儿园），以及郑州市教育城域网的网络安全事件应对工作。

本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。

二、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。适用于全市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。

（一）符合下列情形之一的，为重大网络安全事件

1.教育行业关键信息基础设施或统一运行的市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。

2.教育行业关键信息基础设施或统一运行的市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。

3.计算机病毒在全市教育系统大面积爆发。

4.其他对全市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。

（二）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.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。

2.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。

3.计算机病毒在全市教育系统较大范围内爆发。

4.其他对全市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。

（三）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。

三、监测与预警

（一）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。

（二）预警监测

市教育局建立教育城域网网络安全监测平台，开展网络安全的监测，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。各开发区、区（县）市教育行政部门应分别建立本地网络安全监测体系，主动监测并发布预警信息，与市教育系统网络安全监测平台对接，共享监测预警数据。

（三）预警研判和发布

各级教育行政部门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。

根据监测研判情况，可面向全市教育系统发布蓝色预警信息。

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，各级教育行政部门可发布风险提示信息。

（四）预警响应

1.红色及橙色预警响应

（1）省教育厅组织预警响应工作，启动应急预案。

（2）市、区（县）市教育行政部门、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）市、区（县）市教育行政部门、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。

2.黄色预警响应

（1）省教育厅组织预警响应工作。

（2）市、区（县）市教育行政部门、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.蓝色预警响应

市、区（县）市教育行政部门、各级各类学校启动应急预案，组织开展预警响应工作。

（五） 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。

四、应急处置

（一）事件报告

全市教育系统任何单位和个人都有义务向市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。

（二）应急响应

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

接到上级主管部门关于启动Ⅰ级和Ⅱ级响应的通知后，全市教育系统进入响应状态，开展以下工作：

（1）启动指挥体系

全市各级教育行政部门、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

①跟踪事态发展。事发区（县）市和学校（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。

②检查影响范围。各区（县）市教育行政部门和学校（单位）要全面了解本地区、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。

③及时通报情况。各区（县）市教育行政部门和学校（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

①控制事态，防止蔓延。事发区（县）市和学校（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。

②做好处置工作。事发区（县）市和学校（单位）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）。

③调查取证。事发区（县）市和学校（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。

④信息发布。各级教育行政部门按照上级统一要求，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。

2. III级响应

网络安全事件III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上级教育行政部门。

（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。

（4）有关区（县）市和学校根据上级教育行政部门通报的情况，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。

①控制事态，防止蔓延。事件发生地区（县）市实施技术措施、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。

②做好处置工作。事件发生区（县）市根据事件发生原因，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）。

③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，并及时向上级教育行政部门报告有关情况。

3.Ⅳ级响应

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

（三）应急结束

1.Ⅰ级、Ⅱ级、Ⅲ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。

2.Ⅳ级响应结束

事发市、区（县）市教育行政部门或单位完成处置后，自行解除Ⅳ级响应，并报当地网信办和上级教育行政部门备案。

五、应急保障

（一）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。

（二）组织机构

1.市教育局在市委网信委、省教育厅领导下，统筹协调全市教育系统全局性网络安全事件应急工作,指导开发区、区(县）市教育行政部门和学校网络安全事件应急处置工作。市现代教育信息技术中心负责网络安全应急管理事务性工作，向市教育局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.按照属地化管理原则，各开发区、区（县）市教育行政部门、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。

3.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。

（三）预防工作

1.日常管理

各开发区、区（县）市教育局以及学校（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。

2.演练

市教育局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。各区（县）市教育行政部门每年至少组织一次应急演练。

3.宣传教育

充分利用网络安全宣传周、网络安全攻防大赛、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。

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。

5.重要时期预防措施

在国家和我省、我市重大活动、重要会议、招生录取期间，各级教育行政部门要加强网络安全事件的防范和应急响应。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。

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