河南科技大学文件

河科大信〔2021〕5号

关于印发《河南科技大学网络安全事件应急预案》的通知

校属各单位：

为了建立健全河南科技大学网络安全事件应急工作机制，有效预防并科学应对网络安全突发事件，提高网络安全事件处置能力，最大限度地预防和减少网络安全事件造成的损失和危害，确保校园网络和信息系统的正常运行和安全稳定，维护校园正常秩序，保护公众利益，维护国家安全、公共安全和社会秩序，特制定《河南科技大学网络安全事件应急预案》，请遵照执行。

二〇二一年一月四日

河南科技大学网络安全事件应急预案

为了建立健全河南科技大学网络安全事件应急工作机制，有效预防并科学应对网络安全突发事件，提高网络安全事件处置能力，最大限度地预防和减少网络安全事件造成的损失和危害，确保校园网络和信息系统的正常运行和安全稳定，维护校园正常秩序，保护公众利益，维护国家安全、公共安全和社会秩序。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》、《中华人民共和国计算机信息系统安全保护条例》、《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）、《信息技术安全事件报告与处理流程》、《教育系统网络与信息安全类突发公共事件应急预案》等国家和教育行业有关法律法规，特制定本预案。

第一章　总则

第一条 本预案适用于学校范围内网络安全事件的应急处置。

第二条 坚持统一领导、分级负责；积极防御、综合防范；快速响应、密切协同；强化能力、科学处置；定期演练、常备不懈；坚持“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，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。

第二章　网络安全事件分级

第三条 根据《信息安全技术信息安全事件分类分级指南》（GB/T 20986-2007，以下简称《指南》），本预案中所指网络安全事件是由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或对社会造成负面影响的事件。

第四条 根据《指南》,网络安全事件可划分为有害程序事件、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七个基本分类。

第五条 根据《指南》，将安全事件划分为四个等级：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级）。

第三章　组织机构与职责

第六条 学校网络安全和信息化领导小组（以下简称“校网信领导小组”） 是网络安全事件应急处置领导机构，校网络安全和信息化领导小组办公室（以下简称“校网信办”）统筹协调组织校内网络安全事件应对工作，建立健全跨部门联动处置机制，校党委办公室、校党委宣传部、网络信息中心等相关单位按照职责分工负责相关网络安全事件应对工作。必要时成立河南科技大学网络安全事件应急办公室（以下简称“应急办”），负责特别重大事件（Ⅰ级）、重大事件（Ⅱ级）和较大事件（Ⅲ级）处置的组织指挥和协调。

第七条 学校各单位按照职责和权限，负责本单位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。

（一） 校网信办职责：① 负责网络安全工作的组织、协调和监督，制定相关制度和应急方案；② 根据网络安全事件等级制定相应级别的处理方案，组织协调责任单位落实，共同做好处置工作；③ 负责及时收集、通报和上报网络安全事件处置的有关情况；④ 对校内各单位贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办。

（二） 校党委办公室职责：① 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安全事件的协调处置；② 负责涉密级网络信息泄密类事件的处理。

（三） 校党委宣传部职责：① 负责学校网络和信息系统的舆情监测；② 负责学校信息内容安全类事件的处置，对于涉及师生政治思想方面的倾向性、苗头性的问题，要加强分析研判，妥善有效应对。

（四） 网络信息中心职责：① 负责校园基础网络设施安全；② 负责网络信息中心运维管理的信息系统安全；③ 负责为全校网络安全事件处置提供技术支持。

（五） 其他部门职责：各院系、职能单位、附属单位负责本单位所运维管理的网站和各类信息系统网络安全事件的处置，对照本预案，建立本单位应急处置机制。

第四章 监测与预警

第八条 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。

第九条 校网信办统筹组织开展对学校网络和信息系统的安全监测工作。各单位按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，组织对本单位信息系统开展网络安全监测工作。各单位要将重要监测信息及时上报校网信办。

第十条 各单位组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知校网信办，校网信办可根据监测研判情况，发布蓝色预警。对可能发生较大及以上等级的网络安全事件情况，校网信办应向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网信办、省公安厅、 市公安局等部门通报。预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布机关等。

第十一条 预警响应

（一） 对红色、橙色、黄色预警的响应：校网信办组织预警响应工作，启动相应应急预案，加强网络安全事件监测，对事态发展情况进行跟踪研判，组织指导应急支撑队伍、相关运行单位开展应急准备、风险评估和控制工作，研究制定防范措施和应急工作方案，并根据需要实行 24 小时值班，保持通信联络畅通。 重要情况报省教育厅网信办、省公安厅、市公安局等部门。

（二） 蓝色预警响应：各单位启动相应应急预案，组织开

展预警响应。

第十二条　预警解除：校网信办根据实际情况，确定是否解除预警，并及时发布预警解除信息。

第五章　应急处置

第十三条　网络安全事件发生后，校网信办应立即启动应急预案，组织指导实施处置并及时报送信息。校党委宣传部和网络信息中心的责任单位领导及相关人员应第一时间到达现场，采取断网等先期应急处置措施，控制事态，消除隐患，将损害和影响降到最低，同时组织研判，保存证据，做好信息通报工作。对于初判为较大及以上等级的网络安全事件，校网信办应立即报告校网信领导小组，并研究决定将相关情况向省教育厅网信办、省公安厅、市公安局等部门报告。

第十四条　网信办组织有关单位尽最大可能收集网络安全事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认事件的类别和等级，并根据事件等级采取相应的应急响应。

（一）Ⅰ级、Ⅱ级、Ⅲ级网络安全时间的响应：学校成立应急办，进入应急状态，按照相关应急预案做好应急处置工作，履行应急处置工作的统一领导、指挥、协调职责。应急办 24 小时值班，跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急办，应急办将有关重大事项及时通报省教育厅网信办、省公安厅、市公安局等部门。处置中需要

上级部门网络安全应急技术支撑队伍配合和支持的，应急办予以协调。各单位根据应急办的通报信息，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。

（二）Ⅳ级响应：各单位及时、自主按相关预案进行应急处置，做好处置记录，并报校网信办。

第十五条 根据网络安全事件分类采取不同的应急处置方式：

（一） 网络攻击事件：判断攻击的来源与性质，关闭影响安全的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案： ① 病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助进行杀毒处理。 ② 外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。③ 内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于

无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（二） 信息内容安全事件：检测或接到校内网站出现不良信息报告后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息传播，查找信息发布人并做好善后处理。对上级部门或公安机关要求我校协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（三） 设备故障事件：判断故障发生点和故障原因，迅速联系网络信息中心尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（四） 灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

第十六条 应急结束

（一）Ⅰ级、Ⅱ级、Ⅲ级响应结束：应急办提出建议，报领导小组批准后，及时通报省教育厅网信办、省公安厅、市公安局等部门。

（二） Ⅳ级响应结束：由事发单位决定，报校网信办。

第六章 调查与评估

第十七条 较大、重大和特别重大网络安全事件由校网信办（应急办）组织协调有关部门进行调查处理和总结评估，并按程序上报。一般网络安全事件由事发单位自行组织调查处理和

总结评估，并将相关总结调查报告报校网信办。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。事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。

第七章　预防工作

第十八条　网络安全日常管理

（一）　加强校园网络与信息系统安全管理，建立预警监测体系，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高网络安全事件的应对能力；

（二）　不断健全学校网络和信息系统的技术防护体系，在校园网出口、数据中心、重要信息系统等边界，加强安全防御，发现异常及时处置并逐级报告；

（三）　学校各单位按职责做好网络安全事件日常预防工作，加强各单位的网站和各类信息系统安全管理，制定完善的相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份；

（四）　建立安全巡查制度。党委宣传部、网络信息中心及各单位安全员应密切监视信息系统内容，执行值班制度，做好校园网络与信息系统安全的日常巡查及日志保存等工作，以便及时应对突发性事件。

第十九条　建立应急预案定期演练制度。通过定期组织演练，

发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置实战能力。

第二十条　充分利用各种传播媒介及其他有效的宣传形式，加强网络安全突发事件预防和处置的有关法律、法规和政策宣传，开展网络安全基本知识和技能的宣传活动。

第二十一条　加强学校各单位和相关人员的网络安全事件应急知识特别是网络安全应急预案的培训，提高防范意识及技能。

第二十二条　重要活动期间的预防措施。在国家重要活动、会议期间，加强网络安全事件的防范和应急响应，确保校园网络安全。领导小组统筹协调网络安全保障工作，加强校园网络安全监测，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，及时发现和处置网络安全事件隐患。

第八章　保障措施

第二十三条　各单位要落实网络安全应急工作责任制，把责任落实到具体部门、 具体岗位和个人，并建立健全应急工作机制。

第二十四条　加强网络安全应急技术支撑队伍建设，不断提高信息安全防范意识和技术水平，提高应急处置能力，做好网络安全事件的监测预警、 预防防护、应急处置、应急技术支援工作。

第二十五条　建立学校网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。加强专家队伍建设，充分发挥专家在应急处置工作中的作用。

第二十六条　从教育科研机构、企事业单位、协会中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。

第二十七条　加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。

第二十八条　加强对网络安全应急装备、工具的储备，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

第二十九条　为网络安全事件应急处置提供必要的资金保障，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、预案演练、物资保障等工作开展。

第三十条　网络安全事件应急处置工作实行责任追究制。要求各单位认真贯彻落实预案的各项要求与任务，对未有效落实预案各项规定（如迟报、谎报、瞒报、漏报网络安全事件重要情况或者应急管理工作中有失职、渎职行为等）的单位进行通报批评，相关责任人给予处分，责令限期改正，对落实到位的给予相应的奖励。

第九章　附则

第三十一条　本预案原则上每年评估一次，根据实际情况适时修订。修订工作由校网信办负责。

第三十二条　预案由校网信办负责解释。

第三十三条　本预案自印发之日起实施。

网络安全和信息化领导小组办公室

二〇二一年一月四日

河南科技大学校长办公室　　主动公开　　2021 年 1 月 4 日