河南科技大学文件

河科大信〔2021〕6号

关于印发《河南科技大学信息技术安全事件报告与处置流程》的通知

校属各单位：

为加强我校信息技术安全工作，及时掌握和处置信息技术安全事件，做好信息技术安全事件应急响应处置工作，降低安全事件带来的 损失与影响，维护校园正常工作秩序和营造安全稳定健康网络环境，特制定《河南科技大学信息技术安全事件报告与处置流程》，请遵照执行。

二〇二一年一月四日

河南科技大学

信息技术安全事件报告与处置流程

为加强我校信息技术安全工作，及时掌握和处置信息技术安全事件，做好信息技术安全事件应急响应处置工作，降低安全事件带来的 损失与影响，维护校园正常工作秩序和营造安全稳定健康网络环境， 根据《教育部进一步加强直属高校直属单位信息技术安全工作的通知》 （教技〔2015〕1 号）、教育部《信息技术安全事件报告与处置流程》 （教技厅函〔2014〕75 号）、河南省教育厅《信息技术安全事件报告与处置流程（试行）》（教科技〔2017〕438 号），结合学校实际，特制定本流程。

第一章 总则

第一条 信息技术安全事件的定义。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》）， 本流程中所指网络安全事件是指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。

第二条 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。

第三条 本流程适用于我校各单位发生的信息技术安全事件

的报告与处置工作。

第二章 安全事件等级划分与判定

第四条 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）。

第五条 我校各单位一旦发生安全事件，应根据《指南》，视信息系统重要程度、损失情况以及对工作和社会造成的影响，迅速自主判定安全事件等级，并立即向学校网络安全和信息化领导小组办公室（以下简称“校网信办”）进行报告。校网信办在接到报告后，根据事件情况，进一步做出判定。必要时，校网信办组织专家组进行判定或报告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”）判定。

第三章 安全事件的报告与处置

第六条 对Ⅰ至Ⅲ级安全事件的报告与处置分为三个步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

(一)事发紧急报告与处置

1. 各单位的系统管理员一旦发现上述安全事件，应根据实际情况第一时间采取断网等有效措施进行先期处置，将损害和影响降到最小范围，保留现场，并报告本单位安全员。

2. 单位安全员接到报告后，应立即组织相关人员赶赴现场进行紧急处置，同时以口头通讯的方式将相关情况通报至校

网信办， 并书面记录安全事件发现过程及口头汇报过程。涉及人为主观破坏事 件应同时报告学校保卫处。

3. 校网信办接到报告后，应做好书面记录，并进一步判定安全事件等级，对确认属于 I 至Ⅲ级安全事件的,应向校网信领导小组报告。

4. 紧急报告内容包括：①时间地点；②简要经过；③ 事件类型与分级；④影响范围；⑤危害程度；⑥初步原因分析；⑦已采取的应急措施。

5. 对确认属 I 至Ⅲ级的安全事件，校网信办应立即组织相关技术力量赶赴现场协助开展处置工作。涉及人为主观破坏事件的，学校保卫处应组织人员赶赴现场协助处置，并协助公安机关做好相关取证和处置工作。

6. 各单位应及时跟进事件发展情况，出现新的重大情况应及时补报。

(二) 事中情况报告与处置

1. 事中情况报告应在安全事件发现后 6 小时内以书面报告的形式进行报送（报送内容和格式见附表 1)。

2. 事中情况报告由事发单位安全员组织编写，由单位党政领导班子审核后，签字并加盖公章报送校网信办。涉及人为主观破坏事件的，事中情况报告应抄送给保卫处。

3. 安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为主观破坏的安

全事件应由保卫处联系、配合公安部门开展调查。

(三)事后整改报告与处置

1. 事后整改报告应在安全事件处置完毕后 4 个工作日内以书面报告的形式进行报送（报送内容和格式见附表 2)。

2. 事后整改报告由事发单位安全员组织编写，由本单位党政领导班子审核后，签字并加盖公章报送校网信办。

3. 安全事件事后处置包括：进一步总结事件教训，研判本单位的网络和信息系统安全现状、排查安全隐患，进一步加强制度建设， 提升安全防护能力。如涉及人为主观破坏的安全事件，学校保卫处 应继续配合公安部门开展调查。

第七条 一般安全事件（Ⅳ级）报告与处置。各单位发生一般安 全事件，应及时、自主组织应急处置工作，需要技术协助的，联系校网信办予以协助。在事件处置完毕后 4 天内向校网信办报送整改报告。

第八条 预警类信息的报告与处置。各单位要按时、按要求、认 真完成国家、地方有关信息安全部门(例如教育部、公安部、省教育 厅、省公安厅、市公安局、省教育信息安全监测中心等)以及学校网 信办等信息安全部门发布的预警类信息的应急处置工作，并按要求及 时将执行情况形成书面报告报送校网信办。

第九条 信息安全问题整改类信息的报告与处置。各单位要认真 做好国家、地方有关信息安全部门(例如教育部、公安部、省教育厅、 省公安厅、省工业和信息化委员会、市公安局、省教育信息安全监测 中心等）以及学校网信办等信息安全部门发

布的漏洞整改类信息的应 急处置工作，并按要求及时向校网信办报送整改报告（报送内容和格式 见附表 3)。

第四章 配套制度与责任追究

第十条 为保障联络通畅，各单位安全员、信息员、系统员和数据管理员等人的联络方式发生变更时，应及时将变更情况向校网信办报备。

第十一条 各单位应根据实际建立本单位的值守制度，设立应急值守电话，做到安全事件早预警、早发现、早报告、早控制、早解决。各单位应建立健全本单位网络安全事件应急处置机制， 制定安全事件应急预案，定期组织应急演练。

第十二条 各单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况的，将对相关单位予以通报并追究相关人员的责任。

第十三条 发生Ⅰ至Ⅲ级安全事件后，各单位要认真做好整改落实工作，坚持做到事故原因不查清不放过、整改措施未落实不放过、责任人员未受到教育或处理不放过，尽力杜绝类似事件再次发生。

第五章 附则

第十四条 本管理办法的解释权归校网信办。

第十五条 本流程自发布之日起施行。

网络安全和信息化领导小组办公室

二〇二一年一月四日

附件 1

信息技术安全事件情况报告

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	
信息技术安全分管负责人意见（签字）	
主要负责人意见（签字）	

附件 2

信息技术安全事件整改报告

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	
信息技术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

信息技术安全隐患整改报告

单位名称：（加盖公章）　　报告时间：　年　月　日

联系人姓名		手机	
		电子邮箱	
信息安全隐患名称			
信息安全隐患类别	□安全漏洞　□暗链　□网页篡改　□弱口令 □信息泄露　□系统后门　□网页挂马 □其它_____		
隐患级别	□高危　□中危　□低危		
接收到整改通知时间			
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		

存在隐患主要原因	
简要处置过程	
处置结果	
信息技术安全主管部门审核意见（签字）	
信息技术安全分管负责人审定意见（签字）	

备注：接到安全隐患告知通知后，按规定时限将该报告提交至网络信息中心。

河南科技大学校长办公室	主动公开	2021 年 1 月 4 日