郑州澍青医学高等专科学校文件

校字〔2022〕33号

郑州澍青医学高等专科学校
关于印发《郑州澍青医学高等专科学校信息技术安全事件报告与处置流程（试行）》的通知

校属各单位:

《郑州澍青医学高等专科学校信息技术安全事件报告与处置流程（试行）》已经学校研究同意，现印发给你们，请严格遵照执行。

2022年6月10日

郑州澍青医学高等专科学校
信息技术安全事件报告与处置流程（试行）

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，降低安全事件带来的损失与影响，根据国家有关法律法规和标准规范，依据《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）的有关规定，制定本流程。

第一条 信息技术安全事件定义。根据《信息安全事件分类分级指南》（GB/T 20986-2007，以下简称《指南》），本流程中所称的信息技术安全事件（以下简称安全事件）是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。

第二条 适用范围。本流程适用于我校所有单位信息技术安全事件的报告与处置工作，不含涉及信息内容安全事件的报告与处置工作。

第三条 安全事件等级划分。根据我校网络与信息系统安全突发事件的可控性、严重程度和影响范围，结合我校的实际情况分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）和Ⅳ级（一般）。

Ⅰ级（特别重大）。重要网络与信息系统发生全校性大规模

瘫痪，事态发展超出学校网络安全和信息化领导小组的控制能力，对学校安全、秩序和学校公共利益造成特别严重损害，需要跨省、市协同处置的突发事件。

II级（重大）。重要网络与信息系统全校性瘫痪，对学校安全、秩序和学校公共利益造成严重损害，需要跨地、市协同处置的突发事件。

III级（较大）。某一区域的重要网络与信息系统瘫痪，对学校安全、秩序和学校公共利益造成一定损害，但不需要跨地、市协同处置的突发事件。

IV级（一般）。重要网络与信息系统受到一定程度的损坏，对学校师生员工和一些部门的权益有一定影响，但不危害学校安全、秩序、学校公共利益的突发事件。

第四条 安全事件自主判定。一旦发生安全事件，各相关单位应根据《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，自主判定安全事件等级。

第五条 I至III级安全事件的报告与处置。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.发现安全事件，网络与信息系统运维操作人员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，并报告本单位信息技术安全分管责任

人和主要负责人。

2.信息技术安全分管责任人接到报告后，应立即组织技术人员赶赴现场进行紧急处置，同时以口头方式将相关情况报告网络安全和信息化领导小组办公室。涉及人为主观破坏事件应同时报告市公安局。

3.学校网络安全和信息化领导小组办公室接到报告后，应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，应向学校领导报告并组织力量开展应急处置，同时将有关情况报教育厅科技信息化处、省委网信办、市公安局。

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.事发单位应及时跟进事件进展情况，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8小时内以书面报告的形式进行报送（报送内容和格式见附件1）。

2.事中情况报告由事发单位信息技术安全分管责任人组织信息技术安全管理部门、系统使用单位和运维单位共同编写，由本单位主要负责人审核后，签字并加盖公章报送网络安全和信息化领导小组办公室。

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积极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 5 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件 2）。

2. 事后整改报告由单位信息技术安全分管责任人组织信息技术安全管理部门、系统使用单位和运维单位共同编写，由本单位主要负责人审核后，签字并加盖公章报送学校网络安全和信息化领导小组办公室。

3. 安全事件事后处置包括：进一步总结事件教训，研判信息安全现状、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事件应继续配合公安部门开展调查。

第六条 一般安全事件报告与处置。单位发生一般安全事件，应及时、自主组织应急处置工作，在事件处置完毕后 5 日内向学校网络安全和信息化领导小组办公室报送整改报告（内容和格式见附件 2）

第七条 预警类信息的报告与处置。各单位要认真做好网络管理中心发布的预警类信息的应急处置工作，并及时将执行情况同时报告学校网络安全和信息化领导小组办公室。

第八条 信息安全问题整改类信息的报告与处置。各单位要

认真做好发布的漏洞整改类信息的应急处置工作，并及时将整改报告同时报送学校网络安全和信息化领导小组办公室。（报送内容和格式见附件 3）

第九条 人事变更报告。各单位的信息技术安全工作主管领导、系统负责人、联络员、联络方式发生变更的，应及时将变更情况报学校网络安全和信息化领导小组办公室。

第十条 相关配套机制。信息管理中心设立应急值守电话。各单位应根据实际建立值守制度，做到安全事件早发现、早报告、早控制、早解决。各单位应建立健全本单位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。

第十一条 责任追究。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。

第十二条 本流程自发布之日起施行。

附件：1.信息技术安全事件情况报告（样式）

2.信息技术安全事件整改报告（样式）

3.信息安全隐患整改报告（样式）

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　　时　　分

<table>
<tr><td rowspan="2">联系人姓名</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>电子邮箱</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">☐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</td></tr>
<tr><td>事件分级</td><td colspan="3">☐I 级　☐II 级　☐III 级　☐IV 级</td></tr>
<tr><td>事件概况</td><td colspan="3"></td></tr>
<tr><td>信息系统基本情况
（如涉及请填写）</td><td colspan="3">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</td></tr>
</table>

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	
网络信息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学校网络安全与信息化领导小组办公室。

郑州澍青医学高等专科学校校长办公室　2022年6月10日印发