重庆广播电视大学
重庆工商职业学院 文件

渝电大技〔2018〕1号

关于印发《重庆广播电视大学 重庆工商职业学院网络安全事件应急预案》的通知

各单位（部门）：

经研究，现将《重庆广播电视大学 重庆工商职业学院网络安全事件应急预案》印发给你们，请遵照执行。

重庆广播电视大学　重庆工商职业学院

2018年5月23日

重庆广播电视大学 重庆工商职业学院
网络安全事件应急预案

为健全学校网络安全事件应急响应工作机制，提高我校应对网络安全突发事件能力和水平，有效预防并科学应对网络安全突发事件，确保校园网络与信息系统正常运行，根据《中华人民共和国网络安全法》、《信息安全技术信息安全事件分级分类指南》（GB/Z 20986-2007）、《重庆市网络安全事件应急预案》等有关文件精神，结合学校实际，特制定本预案。

第一章 总 则

第一条 本预案适用于我校所属的网络与信息系统发生网络安全突发事件后的组织指挥、应急行动、后期处置。

第二条 本预案所称的网络安全事件是指校园网络、信息系统、网站、数据等遭到破坏，对学校工作、师生学习、生活秩序造成或可能造成影响的事件。

第三条 本预案所指的网络与信息系统，是指校园内信息化基础设施设备、服务器、校内各网站和信息系统。

第四条 网络安全事件应急处置依照“统一领导、密切协同、快速反应、科学处置”的组织原则，层层落实网络安全主体责任。坚持预防为主，预防与应急相结合，充分发挥全校力量共同做好我校网络安全事件的预防和处置工作。

第二章 网络安全事件分类与分级

第五条 网络安全事件依据发生过程、性质和特征不同，可分为以下四类：

（一）网络攻击事件：校园网络与信息系统因病毒感染、非法入侵或其他技术手段攻击，造成校园网络和信息系统运行异常或存在潜在威胁，或造成数据被篡改、假冒、泄露、窃取等而导致的安全事件。

（二）信息内容安全事件：利用校园网络或网站在校内外传播法律法规禁止的信息，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安全事件。

（三）设备设施故障事件：由于信息系统或软硬件设施设备故障、人为操作等，造成信息系统破坏、业务中断、系统宕机、网络瘫痪等导致的网络安全事件。

（四）灾害性事件：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素造成网络与信息系统损毁，导致业务中断、系统宕机、网络瘫痪等安全事件。

第六条 网络安全事件按照可控性、严重程度和影响范围不同，可划分为四级：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）、一般事件（Ⅳ级）。

（一）符合下列情形之一的，为特别重大网络安全事件（Ⅰ级）：

1.学校网络与信息系统发生全校性大规模瘫痪，对学校正常工作造成特别严重损害，且事态发展超出学校控制能力的网络安全事件。

2.校内重要信息系统中的敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁，对学校稳定和社会形象构成重大影响的网络安全事件。

3.利用校园网传播重要涉密信息、反动信息、煽动性信息、

谣言等情况，可能泄露国家机密，对国家安全、社会稳定构成严重危害，或引发学校大规模突发群体事件，对学校的安全稳定和正常秩序构成特别严重影响、教育教学活动无法正常进行，师生反映强烈并有过激行为的网络安全事件。

4.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、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特别重大网络安全事件（Ⅰ级）的，为重大网络安全事件（Ⅱ级）：

1.学校网络与信息系统发生全校性大规模瘫痪，业务处理能力受到极大影响，对学校正常工作造成严重损害。事态发展超出了信息技术中心控制能力，需学校各部门协同处置的网络安全事件。

2.校内信息系统中的敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全、社会稳定构成较大威胁，对学校稳定和社会形象构成重大影响的网络安全事件。

3.利用校园网传播重要涉密信息、反动信息、煽动性信息、谣言等情况，对国家安全、社会稳定构成较大危害，可能泄露学校机密，或引发学校大规模突发群体事件，对学校的安全稳定和正常秩序构成严重影响，师生反映强烈的网络安全事件。

4.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

（三）符合下列情形之一且未达到重大网络安全事件（Ⅱ级）的，为较大网络安全事件（Ⅲ级）：

1.学校网络与信息系统发生局部瘫痪，对学校正常工作造成一定影响，信息技术中心可自行处理的网络安全事件。

2.校内信息系统中的敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成一定威胁，对学校的安全稳定和正常秩序构成较大影响的网络安全事件。

3.利用校园网传播重要涉密信息、反动信息、煽动性信息、谣言等情况，对国家安全、社会稳定构成一定危害，或对学校的安全稳定和正常秩序构成一定影响，引起师生广泛关注的网络安全事件。

4.其他对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

（四）除上述情形外，对学校安全稳定、正常秩序造成一定影响、对师生权益造成危害和影响，但不危及学校整体工作的网络安全事件，为一般网络安全事件（Ⅳ级）。

第三章 监测措施

第七条 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，信息系统所属二级部门（单位）需参照本预案做好网络安全事件的监测工作，制定和完善管理制度，做好日常管理，避免和减少网络安全事件的发生和危害。

第八条 信息技术中心在校园网出入口、数据中心、重要信息系统等重要部位，安装必要的安全防御检测工具，进行实时监测和定期扫描，发现异常情况及时联系信息系统建管部门。同时做好重要信息系统升级杀毒、数据备份、安全审计等日常管理工作。

第九条 各二级部门（单位）需指定专门的信息技术安全联络员对所属的信息系统采取相关技术措施用以记录系统运行状态、访问日志等，并按照规定留存相关的日志信息不少于六个月。

第十条 信息技术中心定期对校园网信息化基础设施设备进行巡查，做好校园网基础设施设备的日常管理。工程施工须按校园管网线路图纸操作，或经由学校相关部门许可。未经许可不得直接切割或改动网络线路和设备。

第十一条 特殊时期，根据工作需要，由信息技术中心进行统一部署和安排，组织相关信息技术安全人员对校园网络和信息系统采取加强性保护措施，对校园网络安全进行24小时不间断监控。

第四章 响应及应急处置

第十二条 最先发现或接到网络安全事件信息的二级部门（单位）须第一时间通过电话、邮件、短信等方式报信息技术中心，并在12小时内提交《网络安全事件情况报告》（见附件1），信息技术中心根据监测研判情况，确定网络安全事件的类别和等级，并参照下述响应机制对突发事件进行处置：

（一）Ⅲ至Ⅳ级事件响应机制

信息技术中心和发生安全事件的网站或信息系统建管部门自行负责应急处置工作，有关情况报分管校领导。

（二）Ⅱ级事件响应机制

信息技术中心立即上报分管校领导，由分管领导统一组织、协调指挥相关部门进行应急处置。

（三）Ⅰ级事件响应机制

信息技术中心立即上报分管校领导和安全稳定工作领导小组，领导小组再上报至市教委等相关部门，由市教委相关部门会同我校安全稳定工作领导小组统一组织、协调指挥应急处置。

第十三条 各类安全事件应急处置措施

信息技术中心将根据《网络安全事件情况报告》，按照事件发生的性质将启动以下应急处置措施：

（一）网络攻击事件

1.信息技术中心立即切断出现安全事件的网站或信息系统的网络连接，如是病毒类网络安全事件，必要时隔离其相应楼层的网络，同时做好现场保护。

2.涉事部门自主或在信息技术中心协助下立即通过相关设备日志，找出导致安全事件的原因和网站或信息系统可能存在的安全漏洞，并完成系统修复、清理和数据恢复等整改工作。同时做好取证或协助公安部门做好调查取证工作。

3.在网络安全事件处理结束，网站或信息系统恢复网络连接之后48小时内，涉事部门须继续不间断对其运行情况进行监控，以避免再次发生安全事件。

（二）信息内容安全事件

1.信息技术中心立即阻断涉事网站的外网访问。

2.涉事部门自主或在信息技术中心协助下立即通过相关服务器日志，查找不良言论的发布者及发布途径，找出导致安全事件的原因和网站可能存在的安全漏洞，并完成不良信息清理、网站全面清查等整改工作。同时做好取证或协助公安部门做好调查取证工作。

3.在网络安全事件处理结束，网站恢复外网访问之后48小时内，涉事部门须继续不间断对其运行情况进行监控，以避免再次发生安全事件。

（三）设施设备安全事件

信息技术中心及时到达发生事件现场，判断事件危害范围和

程度，确定发生事件原因，迅速联系相关运维公司尽快抢修故障设施设备，优先保证校园网主干网络和重要信息系统的运转。

（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：存储设备的拔出与保存，设备的断电与拆卸、搬迁等。

第五章 总结与报告

第十四条 网络安全事件解决后，涉事部门需对事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写《网络安全事件整改报告》（见附件2），报告内容包括事件的时间、地点、规模、涉及人员情况，事件的危害影响程度和是否完成整改等基本情况，交信息技术中心备案。

第十五条 发生Ⅰ级事件，在报告学校的同时，应按照市教委《信息技术安全事件报告与处置流程（试行）》报告上级主管部门。属于特别重大事件或存在非法犯罪行为的，还须第一时间向公安机关报案。

第六章 保障措施

第十六条 信息系统所属二级部门（单位）做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，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，提高应对网络安全事件的能力。

第十七条 加强技术储备与保障工作，不断完善网络安全技术防护体系，确保信息系统的稳定与安全。适时组织相关专家和机构分析当前网络安全，对网络应急预案及实施情况进行评估，

开展现场研究。

第十八条 加强安全培训和演练，信息技术中心应定期组织相关单位网络技术安全联络员进行安全知识培训，提高有关人员的责任意识、安全意识和技术水平。开展应急处置演练，确保相关措施的有效落实。

第七章 附 则

第十九条 本预案由信息技术中心负责解释。

第二十条 本预案自发布之日起施行。本预案施行前的有关规定，凡与本预案不符的，均以本预案为准。

附 1

网络安全事件情况报告

部门名称:(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	□网络攻击事件　□信息内容安全事件 □设施设备故障事件　□灾难性事件 □其他:_____		
事件分级	□I 级　□II 级　□III 级　□IV 级		
事件概况			
信息系统的基本情况(如涉及请填写)	1.系统名称: _____ 2.系统域名和 IP 地址: _____ 3.系统主管部门: _____ 4.系统运维人员: _____ 5.系统主要用途:_____ 6.是否定级　□是　□否，所定级别:_____ 7.是否备案　□是　□否，备案号:_____ 8.是否测评　□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	
是否需要技术支持及需支持事项	
安全负责人意见（签字）	
主要负责人意见（签字）	

附 2

网络安全事件整改报告

部门名称：（需加盖公章）　　报告时间：_____年__月__日__分

联系人姓名		手机	
		电子邮箱	
事件分类	□网络攻击事件　□信息内容安全事件 □设施设备故障事件　□灾难性事件 □其他：_____		
事件分级	□I 级　□II 级　□III 级　□IV 级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统域名和 IP 地址：_____ 3.系统主管部门：_____ 4.系统运维人员：_____ 5.系统主要用途：_____ 6.是否定级　□是　□否，所定级别：_____ 7.是否备案　□是　□否，备案号：_____ 8.是否测评　□是　□否 9.是否整改　□是　□否		

事件发的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情况	
事件的安全整改措施	
存在问题及建议	
安全负责人意见（签字）	
主要负责人意见（签字）	

重庆广播电视大学办公室　　2018年5月23日印发