西 南 大 学 文 件

西校〔2020〕316 号

关于印发《西南大学
网络安全事件应急预案（试行）》的通知

各单位：

《西南大学网络安全事件应急预案（试行）》已经党委常委会审定通过，现印发给你们，请遵照执行。

西南大学

2020 年 12 月 17 日

西南大学
网络安全事件应急预案（试行）

第一章　总　则

第一条　为健全和完善学校网络安全事件应急工作机制，规范网络安全事件工作流程，提高学校网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校安全稳定，根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》（中网办发文〔2017〕4号）、《信息安全技术 信息安全事件分类分级指南》(GB/Z 20986-2007)、《教育系统网络安全事件应急预案》（教技〔2018〕8号）和学校有关管理规定，特制定本办法。

第二条　本预案适用于西南大学各机关职能部门、直附属单位、企业单位、各学院（部）和校管科研机构（以下简称各单位）的网络安全事件的应对工作，处置对象包括学校IP公网地址段和域名（swu.edu.cn）包含的所有网络资源以及互联网域名解析到学校校内IP地址段的信息化资源。

第三条　本预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，对学校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、信息内容安全事件、设备设施故障、灾害性事件和其他事件（详见附件1）。其中信息内容安全事件的应对，参照有关规定和办法。

第四条 根据网络安全事件可能造成的危害、可能发展蔓延的趋势等，结合学校特点，网络安全事件分为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、一般网络安全事件四级。

（一）符合下列情形之一的，为特别重大网络安全事件（I级）。

1.关键信息基础设施或重要信息系统（网站）遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

2.关键信息基础设施或重要信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改、假冒，对系统安全稳定和正常秩序构成特别严重威胁。

3.网络病毒在全校大面积爆发，严重影响全校信息系统正常运行和业务处理。

4.其他对全校信息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特别重大网络安全事件的，为重大网络安全事件（II级）。

1.全校范围的网络用户24小时以上无法访问校内或互联网信息资源。

2.关键信息基础设施或重要信息系统（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。

3.关键信息基础设施或重要信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改、假冒，对系统安全稳定和正常秩序构成重大威胁。

4.网络病毒在学校局部爆发，对全校信息系统正常运行和业务处理构成重大威胁。

5.其他对全校信息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）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（III 级）。

1.学校关键信息基础设施或重要信息系统（网站）遭受系统损失，明显影响系统效率和业务处理能力。

2.学校关键信息基础设施或重要信息系统（网站）的关键数据或重要敏感信息发生丢失或被窃取、篡改、假冒，对系统安全稳定和正常秩序构成威胁。

3.其他对全校系统安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

（四）一般网络安全事件（IV 级）。除上述情形外，对学校系统安全稳定和正常秩序构成一般威胁，造成一定影响的网络安全事件。

第二章　工作原则

第五条　网络安全事件应急处理遵循以下原则：

（一）统一指挥、密切协同。学校网络安全和信息化领导小

组（以下简称“网信领导小组”）统筹协调全校网络安全应急指挥工作，建立主管部门、专业机构和有关单位等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

（二）分级管理、强化责任。实施校院两级管理，学校统筹组织和协调部署，并按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各单位对本单位网络安全工作负主体责任，领导班子主要负责人是本单位网络安全工作第一责任人。

（三）预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

第三章　组织机构及职责

第六条　领导机构与职责。学校网信领导小组统筹指导网络安全事件应急工作，研究网络安全事件处置中的重大问题；因网络安全事件应急处置而成立的应急工作组统筹指挥和部署网络安全事件应急处置工作。

第七条　办事机构与职责。网信领导小组办公室作为下设办事机构，负责网络安全应急管理事务性工作，向学校网信领导小组和应急工作组报告网络安全事件情况，提出应对措施建议和意见，统筹组织学校网络安全监测工作，指导有关部门和单位做好

应急处置工作。

第八条 各单位职责。网信领导小组成员单位按照职责分工参与网络安全应急工作；各单位按照“谁主管谁负责、谁运维谁负责”的原则，负责所建网络和业务信息系统（网站）的网络安全事件具体应急工作，制定有关网络和信息系统的安全事件应急响应和信息通报工作机制，承担主体责任并切实落实相关具体工作。

第四章 监测与预警

第九条 网络安全监测。网信领导小组办公室通过多种渠道和技术手段，监测和及时发现网络安全事件以及漏洞、病毒、网络攻击等网络安全威胁；各单位对所建网络和信息系统（网站）的运行状态进行密切监测、及时发现网络安全事件和威胁。

第十条 网络安全事件预警按照紧急程度、发展态势和可能造成的危害程度，由高到低分为红色、橙色、黄色和蓝色四个等级，分别对应发生或可能发生的特别重大、重大、较大和一般网络安全事件。

第十一条 研判和预警发布。

（一）网信领导小组办公室对监测信息进行研判，认为发生或可能发生重大或特别重大网络安全事件的，立即向学校网信领导小组报告；认为需要立即采取防范措施的及时通知有关部门和事发单位。

（二）各单位对监测信息进行研判，认为发生或可能发生较

大、重大或特别重大网络安全事件的信息，应立即向学校网信领导小组办公室报告，不得迟报、谎报、瞒报、漏报。

（三）网信领导小组办公室负责预警信息发布，其中红色和橙色预警报网信领导小组批准后发布；对达不到预警级别但又要发布警示信息的，可发布风险提示信息。

（四）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、时限要求和发布机关等。

第十二条 预警响应。

（一）红色和橙色预警响应

1.网信领导小组办公室按照网信领导小组的统一部署，密切关注事态发展，研究制定防范措施，协同有关部门和事发单位做好各项应急处置的准备工作。

2.相关人员保持通信联络畅通，其中红色预警实行网信领导小组办公室及有关单位24小时值守。

3.网信领导小组办公室按照应急响应预案开展预警响应工作，做好风险评估、应急准备、风险控制和系统恢复准备工作。

4.信息化建设办公室部署技术支撑队伍进入待命状态，检查设备、软件工具等，确保其处于良好状态。

（二）黄色预警响应

1.网信领导小组办公室根据应急需要联系有关部门或技术人员，研究确定防范措施，协助调度各种资源，做好各项应急处置的准备工作。

2.事发单位按照应急响应工作机制开展预警响应工作，做好风险评估、应急准备、风险控制和系统恢复准备工作。

3.信息化建设办公室安排技术支撑队伍支持，保持联络畅通，协助事发单位检查设备、软件等，确保其处于良好状态。

（三）蓝色预警响应。事发单位按照应急响应工作机制开展预警响应工作，做好风险评估、应急准备、风险控制和系统恢复准备工作；根据需要报请网信领导小组办公室协助。

（四）预警解除。网信领导小组办公室根据实际情况，对已经处置结束和解除威胁的网络安全事件解除预警，及时发布预警解除信息。

第五章　应急处置

第十三条　初步处置。事发单位应立即采取科学有效的应急处置措施，必要时寻求有关部门帮助，将影响降到最低，保存网络攻击、网络入侵或网络病毒等安全事件和威胁的证据。

第十四条　应急响应。网络安全事件应急响应按照紧迫程度由大到小分为 I 级、II 级、III 级、IV 级四个等级，分别对应特别重大、重大、较大和一般网络安全事件。

（一）I 级和 II 级响应

1.启动应急指挥。成立应急工作组，分管校领导为组长，网信领导小组办公室主任为副组长，网信领导小组有关成员单位和事发单位负责人为成员。应急工作组履行应急处置工作统一指挥、部署和协调的职责。

2.跟踪事态发展。网信领导小组办公室协同有关部门和事发单位，及时关注跟踪事态发展变化和处置进展情况，掌握网络和信息系统受影响的范围和程度，随时向网信领导小组和应急工作组报告重要事项，及时填报《西南大学网络安全事件情况报告》（附件 2）。

3.控制事态蔓延。网信领导小组办公室根据需要联合有关部门、事发单位，分析事件发生原因，采取各种科学有效的技术措施、管控手段，最大限度阻止和控制事态蔓延。

4.恢复网络系统。根据事件发生的原因组织技术力量及时消除隐患，恢复遭受破坏的网络和信息系统，优先恢复业务连续性要求高的重要网络和信息系统。

5.调查溯源追责。在保留相关证据的基础上，开展问题定位和溯源追踪工作，防止类似事件的再次发生，对于人为破坏活动，由学校保卫处确认后移送当地公安机关。

6.协调校外支持。应急处置过程中需要校外技术及工作支持的，由网信领导小组办公室根据实际需要，协同事发单位，联系校外有关单位（企业）予以支持。

7.次生事件处置。对于引发或可能引发其他安全事件的，网信领导小组办公室应及时按程序上报，并做好相关部门应急处置的配合工作。

（二）III 级和 IV 级响应

1.跟踪事态发展。事发单位及时关注跟踪事态发展变化和处

置进展情况，掌握网络和信息系统受影响的范围和程度，随时向网信领导小组办公室报告重要事项，及时填报《西南大学网络安全事件情况报告》（附件2）。

2.控制事态蔓延。事发单位认真分析事件发生原因，采取各种科学有效的技术措施、管控手段，最大限度阻止和控制事态蔓延。

3.恢复网络系统。事发单位根据事件发生的原因组织技术力量及时消除隐患，恢复遭受破坏的网络和信息系统。

4.调查溯源追责。在保留相关证据的基础上，开展问题定位和溯源追踪工作，防止类似事件的再次发生，对于人为破坏活动，应向学校保卫处报告，根据实际情况严重程度进行处理。

5.协调外部支持。应急处置过程中需要其他部门和校外技术工作支持的，可联系网信领导小组办公室和校外有关单位（企业）予以支持。

6.次生事件处置。对于引发或可能引发其他安全事件的，事发单位应及时按照程序上报，并做好相关部门和单位的应急处置的配合工作。

第十五条 应急结束。I级和II级响应经应急工作组批准同意后，网信领导小组办公室根据实际情况决定响应的结束；III级和IV级响应由事发单位完成应急处置后，报网信领导小组办公室同意，根据实际情况决定响应的结束。

第十六条 信息发布。未经宣传部批准，任何单位不得发布

网络安全应急处置的相关新闻和消息。

第六章　调查评估

第十七条　重大和特别重大网络安全事件由网信领导小组办公室组织开展调查处理和总结评估工作，结果报网信领导小组和应急工作组；较大和一般网络安全事件由事发单位组织开展调查处理和总结评估工作，结果报网信领导小组办公室。

第十八条　调查处理和总结评估工作应在应急响应结束后 5 个自然日内完成，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，并填报《网络安全事件总结调查报告》(附件 3)。

第七章　预防工作

第十九条　各单位应做好网络安全事件日常预防工作，不断完善本单位网络安全事件工作机制，细化应急操作流程。按照网络安全等级保护等相关要求，落实各项防护措施，做好网络安全检查、风险评估和系统备份，加强信息系统的安全保障能力。

第二十条　各单位应加强网络安全监测预警，及时发现并处置安全威胁。网信领导小组办公室应全面掌握全校信息系统（网站）情况，建立全校网络安全监测预警和通报机制，指导、监督各单位及时修复安全威胁，排查安全隐患，提高发现和应对网络安全事件的能力。

第二十一条　网信领导小组办公室每年组织一次针对网络安全事件的应急演练;充分利用网络安全宣传周等各种活动形式，

加强网络安全事件预防和处置的有关法律、法规和政策的宣传教育，提高在校师生的网络安全意识。

第二十二条 各单位应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。网信领导小组办公室定期组织面向全校相关技术人员的网络安全知识培训。

第八章 工作保障

第二十三条 按照“谁主管谁负责”的原则，各单位应落实网络安全应急工作责任制，明确具体岗位和人员，建立健全应急工作机制。

第二十四条 学校配齐配足信息与网络安全技术队伍，信息化建设办公室作为全校网络安全应急技术支撑单位，应加强网络安全技术队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支撑等工作。

第二十五条 建立学校网络安全专家组，为全校网络安全事件的预防和处置提供技术咨询和决策建议。

第二十六条 加强与周边高校、网络安全专业机构、行业学会（协会）等单位的合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制。

第二十七条 学校每年提供专项经费，用于网络安全应急技术支撑队伍建设、专家队伍建设、监测通报、宣传教育培训、预案演练、物资保障、设备修购和安全测评及服务等工作开展。

第二十八条 学校对网络安全事件应急管理工作中表现突出的单位给与正面融合考核评价；对不配合组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照有关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

第九章 附 则

第二十九条 处置过程中，对重大或特别重大网络安全事件，可能威胁全市教育网络安全，经网信领导小组同意，及时向重庆市教育网络安全应急部门报告。积极配合网信部门和当地公安机关开展调查取证工作。

第三十条 本预案原则上每年评估一次，根据实际情况适时修订。修订工作由学校网信领导小组办公室组织。各单位要根据本预案适时调整本单位的网络安全事件应急工作机制。

第三十一条 本预案由学校网信领导小组办公室负责解释，自印发之日起实施。

附件：1.网络安全事件分类

2.西南大学网络安全事件情况报告

3.西南大学网络安全事件总结调查报告

附件 1

网络安全事件分类

网络安全事件可分为有害程序事件、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、灾害性事件和其他网络安全事件等。

1.有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件。如系统感染勒索病毒、网站被上传webshell、系统被渗透或控制等。

2.网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。如系统遭 DDOS 攻击、SQL 注入攻击、尝试爆破密码等。

3.信息破坏事件分为信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件。如发现网络上存在与系统数据高度雷同的数据，或发现业务数据被篡改。

4.信息内容安全事件是指通过网络发布、传播法律法规禁止信息，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、社会稳定和公共利益的事件。如网站被悬挂反动标识，或

有人在网站互动区发布非法内容等。

5.设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障。如服务器硬件故障，机房供电中断等。

6.灾害性事件是指由于自然灾害等其他突发事件导致的网络安全事件。如机房遭遇地震、火灾等。

7.其他事件是指不能归为以上分类的网络安全事件。

附件 2

西南大学网络安全事件情况报告

单位名称:（盖公章）　　事发时间:　　年　　月　　日　　时　　分

联系人姓名		电子邮箱	
手机		QQ	
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			
信息系统的基本情况 (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		

事发网络和信息系统功能描述	
事件发生时间、事态发展与处置的简要经过	
事件初步估计的危害和影响（影响程度、人数、紧急损失等）	
事件原因的初步分析	
已采取的应急措施和效果	
是否需要应急支援	
安全负责人意见（签字）	
主要负责人意见（签字）	

备注：学校网信领导小组办公室联系电话：023-68254080

附件 3

西南大学网络安全事件总结调查报告

单位名称：（需加盖公章）　　报告时间：　　年　　月　　日

联系人姓名		手机	
		电子邮件	
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			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.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）	

西南大学党政办公室　　2020年12月17日印发