重庆文化艺术职业学院文件

重艺院发〔2021〕65号

重庆文化艺术职业学院
关于印发《重庆文化艺术职业学院网络安全突发事件应急处置工作预案》的通知

各系、处（室、部、中心）：

为了有效预防、及时控制和妥善处理学校网络和信息突发事件，建立健全应急机制，根据国家有关法律法规和学校有关规定，制定《重庆文化艺术职业学院网络安全突发事件应急处置工作预案》，现印发你们，请认真抓好贯彻落实。

重庆文化艺术职业学院

2021年3月29日

重庆文化艺术职业学院网络安全突发事件应急处置工作预案

第一章　总 则

第一条 本预案所称突发性事件，是指自然因素或者人为活动引发的危害学校网络设施及信息安全等有关的突发事件。

第二条 本预案适用范围是学校网络和信息系统发生的信息破坏等可能会引发影响学校和社会稳定的事件。

第三条 本预案的指导思想是确保计算机网络及信息安全，将事件危害和影响降到最低。

第四条 应急处置工作原则：预防为主、及时控制；统一领导、统一指挥；各司其职、整体作战；发挥优势、保障安全。快速反应，及时做好记录上报等工作并删除或隔离有害信息；积极引导，弱化有害信息引发的焦点、热点问题；迅速查明有害信息来源，根据事件的危害程度，按照国家法律法规和学校有关规定进行早报告、早控制、早解决。

第二章　组织指挥和职责任务

第五条 网络与信息安全应急处置工作由学校网络安全与信息化工作领导小组统一负责，学校主要领导为学校网络安全第一责任人，学校各职能部门、系部负责人为本部门网络安全的第一责任人。图书信息中心负责学校网络信息的管理、监控工作，加强对有害信息的跟踪、过滤、封堵和删除，并随时向学校网络安

全与信息化工作领导小组报告网上有害信息的情况和处理结果。

第三章　处置措施和处置程序

第六条 处置措施

处置的基本措施分突发事件发生前与突发事件发生后两种情况。

（一）突发事件发生前

1. 预警预报体系建设。学校网络安全与信息化领导小组要预先对突发事件预警预报体系进行建设，开展突发事件调查，编制突发事件防治规划，建设专业监测网络，并规划建设突发事件信息管理系统，及时处理突发事件讯情信息。

2. 突发事件险情巡查。图书信息中心要充分发挥专业监测的作用，进行定期和不定期的检查，加强对突发事件重点部位的监测和防范，发现有不良险情时，要及时处理并向主管部门报告。

3. 建立健全灾情速报制度。保障突发性突发事件紧急信息报送渠道畅通。属于大型突发事件的，在向市文旅委、市教委报备同时，还应向巴南区公安局计算机信息安全监察科报告。

（二）突发事件发生后

立即启动应急预案，采取应急处置程序，判定突发事件级别，并立即将灾情向市文旅委、市教委报告，在处置过程中，应及时报告处置工作进展情况，直至处置工作结束。

第七条 处置程序

（一）发现情况

信息主管部门要严格执行值班制度，做好学校网信息系统安全的日常巡查及其日志保存工作，以保障最先发现突发事件并及时处置此突发性事件。

（二）预案启动

一旦突发事件发生，立即启动应急预案，进入应急预案的处置程序。

（三）应急处置方法

在突发事件发生时，首先应区分突发事件发生是否为自然突发事件与人为破坏两种情况，根据这两种情况把应急处置方法分为两个流程。

流程一：当发生的突发事件为自然突发事件时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：设备的断电与拆卸、搬迁等。

流程二：当人为或病毒破坏的突发事件发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的IP或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照突发事件发生的性质分别采用以下方案：

1．病毒传播：针对这种现象，要及时断开传播源，判断病毒的性质、采用的端口，然后关闭相应的端口，在公布病毒攻击信息以及防御方法。

2．入侵：对于网络入侵，首先要判断入侵的来源，区分外网

与内网。入侵来自外网的，定位入侵的IP地址，及时关闭入侵的端口，限制入侵地IP地址的访问，在无法制止的情况下可以采用断开网络连接的方法。入侵来自内网的，查清入侵来源，如IP地址等信息，同时断开对应的交换机端口。

3. 信息被篡改：这种情况，要求一经发现马上断开相应的信息上网链接，并尽快恢复。

4. 网络故障：一旦发现，可根据相应工作流程尽快排除。

5. 其它没有列出的不确定因素造成的突发事件，可根据总的安全原则，结合具体的情况，做出相应的处理。不能处理的可以请示相关的专业人员。

（四）情况报告

1. 突发事件级别判定。突发事件发生时，按照应急处置方法进行处置，同时需要判定突发事件的级别，首先向图书信息中心汇报。大型突发事件发生或上级领导通知的特殊时间内发生的突发事件，同时向巴南区公安局计算机信息系统安全监察科汇报。中、小型级别的突发事件，向学校的分管和主管领导汇报，并及时报告处置工作进展情况，直至处置工作结束。

2. 情况报告内容。突发事件发生的时间、地点，突发事件的级别，突发事件造成的后果，应急处置的过程、结果，突发事件结束的时间，以后如何防范类似突发事件发生的建议与方案等。

（五）发布预警

突发事件发生时，可根据突发事件的危害程度适当地发布预

警，特别是一些在其它地方已经出现，或在安全相关网站发布了预警而学校网还没有出现相应的突发事件，除了在技术上进行防范以外，还应当向全体用户发布预警，直至突发事件警报解除。

（六）预案终止

经专家鉴定，突发事件险情或灾情已消除，或者得到有效控制后，由学校的主管部门宣布险情或灾情应急期结束，并予以公告，同时预案终止。

第四章　保障措施

突发事件应急防治是一项长期的、持续的、跟踪式的、深层次的和各阶段相互联系的工作，是有组织的科学与社会行为，而不是随每次突发事件的发生而开始和结束的活动。因此，必须做好应急保障工作。

第八条　人员保障

重视人员的建设与保障，确保在突发事件发生前的人员值班，突发事件处置过程和灾后重建中的人员在岗与战斗力。

第九条　技术保障

重视网络信息技术的建设和升级换代，在突发事件发生前确保网络信息系统的正常、安全，突发事件处置过程中和灾后重建中的相关技术支撑。

第十条　物资保障

根据近几年全国甚至全世界网络信息系统安全防治工作所需经费情况，及时购买相应的应急设施。建立应急物资储备制度，

保证应急抢险救灾队伍技术装备的及时更新，以确保突发事件应急工作的顺利进行。

第十一条 训练和演练

加强网络用户的防灾、减灾知识的宣传普及，增强网络用户的防灾意识和自救互救能力。有针对性地开展应急抢险救灾演练，确保发灾后应急救助手段及时到位和有效。

第五章 附 则

第十二条 本预案由重庆文化艺术职业学院网络安全与信息化工作领导小组负责解释。

第十三条 本预案自印发之日起施行。

重庆文化艺术职业学院党政办公室　　2021年3月29日印发