重庆青年职业技术学院文件

重青院发〔2019〕78号

重庆青年职业技术学院
关于印发《网络安全事件应急预案》的通知

各二级单位：

为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，建立了网络安全事件应急响应工作机制，经第26次党委会审议通过，现将学院《网络安全事件应急预案》印发给你们，请遵照执行。

重庆青年职业技术学院

2019年11月26日

重庆青年职业技术学院
《网络安全事件应急预案》

为建立学院网络安全事件应急响应工作机制，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》《中华人民共和国计算机信息系统安全保护条例》《信息安全事件分类分级指南》《教育系统网络安全和信息化类突发公共事件应急预案》《信息技术安全事件报告与处理流程》等国家和教育行业有关法律法规，结合学院工作实际，特制定本预案。

第一章 总 则

第一条 校园网络安全事件是指校园信息化基础设施、应用系统、网站、信息化数据等因各种因素遭到破坏，对学院工作、学习、生活秩序造成负面影响的事件。

第二条 应急处置遵循“ 统一领导，预防为本、快速反应，科学处置”的原则，最大可能的降低危害和影响。

第二章 网络安全事件分级

第三条 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：由于遭受有害程序感染、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危险，或造成信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

（二）设备故障事件：由于信息系统或外围软硬件设施

故障、人为误操作等，造成信息系统破坏、业务中断、系统宕机、网络瘫痪等导致的信息安全事件。

（三）**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。

（四）**信息内容安全事件**：利用校园网络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事件。

第四条 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：

（一）Ⅰ级（特别重大）：安全事件导致校园网全局性瘫痪、校级业务系统中断，学院主页被篡改以及网站、论坛、自媒体等非法信息引发学院大规模群体性事件，对学院正常工作造成特别严重损害，事态发展超出学院控制能力。

（二）Ⅱ级（重大）：安全事件导致校园网发生大规模瘫痪、校级业务系统中断，学院主页被篡改以及网站、论坛、自媒体等非法信息引发师生反应强烈，对学院正常工作造成严重损害。

（三）Ⅲ级（较大）：事件导致校园网某一区域网络或某一校级业务系统瘫痪，或由于网站敏感信息、谣言等，对学院正常工作造成一定损害。

（四）Ⅳ级（一般）：事件导致某一局部网络或二级学院或职能部门自建网站、信息应用系统受到一定程度损坏，但不危害学院整体工作。

第三章 组织机构及职责

第五条 学院网络安全和信息化领导小组为网络安全事件应急处理领导机构。领导小组下设办公室，挂靠教务处的信息技术中心，简称：信息技术中心。其职责包括：

（一）负责网络安全工作的组织、协调和监督，制定相关制度和应急预案；

（二）根据网络安全事件程度提出相应级别预案的启动，组织协调二级单位落实应急预案，共同做好处置工作；

（三）负责及时收集、通报和上报网络安全事件处置的有关情况；

（四）对全院各部门贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办。

第六条 各部门职责包括：

（一）信息技术中心：负责校园基础网络系统安全，保证校园网络服务不中断；负责网络攻击、设备故障类事件的处置；负责全院网络安全事件处置的技术支持工作。

（二）党政办公室：牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置；负责涉密级信息网络泄密类事件的处理。

（三）宣传统战部：负责学院舆情监测和信息内容安全类事件的处置，对于涉及师生政治思想方面的预警性、倾向性、苗头性的问题，要加强分析研判，妥善有效应对。

（四）保卫处：加强网上网下情况信息收集，协助信息技术中心开展网络信息监控，协助二级单位做好重点人员安

全管理和防控，密切联系公安机关，协助、配合公安机关对校园网络安全事件进行处置。

（五）其它二级单位：负责本单位网站和信息系统安全事件的处置工作。

第七条 各系部、职能部门负责本单位网站和业务系统的信息安全事件的处置工作，应对照本预案，建立本部门应急处置机制。

第四章 预防措施

第八条 加强网络与信息系安全管理，健全工作制度和建立预报监测与预警体系，预警等级依次分为红色、橙色、黄色、蓝色，分别对应特别重大、重大、较大和一般网络安全事件，避免和减少网络安全事件发生。

第九条 健全技术防护体系，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，发现异常情况及时防范处理并逐级报告。同时做好操作系统升级杀毒，数据备份、安全审计等日常管理工作。

第十条 建立灾害险情巡查制度。宣传统战部及各二级部门网站所属部门应随时监控网站内容，信息技术中心应做好校园网络安全和信息化的日常技术巡查，以保证最先发现灾害并及时处置突发性事件。

第五章 处置程序

第十一条 启动预案：发生网络安全事件后，涉事部门应第一时间报告学院网络安全和信息化领导小组，必要时应

采取断网等有效措施，将损害和影响降低到最小范围，保留现场，特别是保留案事件发生后设备中原始数据不被破坏。

第十二条 事件定级：学院网络安全和信息化领导小组组织各二级单位，尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认事件的类别和等级。

第十三条 应急响应：根据事件等级采取相应的响应方式

I 级：涉事部门立即上报学院网络安全和信息化领导小组，并由学院报告上级主管部门和公安部门，公安部门指挥协调校外有关单位和学院协同进行应急处置。

III 至 II 级：涉事部门应立即上报学院网络安全和信息化领导小组组长，由领导小组指挥、协调成员单位进行应急处置。涉及人为主观破坏事件时视情节严重程度由学院保卫处报告当地公安部门。

IV 级：涉事部门组织、协调相关单位及时、自主进行应急处置，做好处置记录。

第十四条 应急处理方式：根据网络安全和信息化事件分类采取不同应急处置方式。

（一）网络攻击事件：判断攻击的来源与性质，关闭影响安全的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，保留网络设备和服务器设备上的行为日志，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修

复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助进行处理。

外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（二）设备故障事件：判断故障发生点和故障原因，迅速联系 IT 运维公司尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（三）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：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

（四）信息内容安全事件：接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接

线，阻止有害信息传播，查找信息发布人并做好善后处理。对公安机关要求学院协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（五）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理，不能处理的及时咨询国家信息安全机构。

第十五条 后续处理：

（一）安全事件最初应急处置后，应及时采取措施，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。并保留服务器或其他网络设备上的数据，作为相关部门查证的原始证据。

(二) 安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

（三）安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

第十六条 总结上报

（一）系统恢复运行后，学院网络安全和信息化领导小组对事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写事件处理报告。

（二）发生网络安全事件，在报告学院网络安全和信息化领导小组的同时，应报告重庆市教委，属于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。应按照以下流程报告：

事发紧急报告：事件发生后立即以口头通讯方式向上级主管部门，涉及人为主观破坏事件应同时报当地公安机关。内容包括：时间地点、简要经过、时间类型与分级、影响范围、危害程度、初步原因分析、已采取的紧急措施等。

事中处置报告：应在事件发生后8小时内或上级主管部门规定的时间内以书面报告的形式报送。

事后整改报告：应在时间处置完毕后5个工作日内或上级主管部门规定的时间内以书面的报告的形式报送。

第六章 保障措施

第十七条 加强队伍建设，不断提高学院全体工作人员的网络安全防范意识和技术水平，确保安全事件应急处置科学得当。

第十八条 加强技术保障，不断完善网络安全整体方案，加强技术防护，确保信息系统的稳定与安全。

第十九条 加强资金保障，信息技术中心应根据校园网安全防护和应急处置工作实际需要，提出用于安全的软硬件设备及运行维护经费预算，报财务处纳入年度经费预算，以专项经费列支。

第二十条 加强安全培训和演练，学院网络安全和信息化领导小组应定期组织相关部门和网络管理员参加信息安全知识培训，增强防范意识和应急处置能力。开展应急处置演练，确保相关措施的有效落实。

第七章 附 则

第二十一条 本预案自发布之日起施行，由学院网络安全和信息化领导小组办公室负责解释。

重庆青年职业技术学院办公室　　2019年11月26日印发