广 西 工 商 职 业 技 术 学 院

文 件

广商院信息〔2021〕3 号

广西工商职业技术学院关于印发《广西工商职业技术学院网络安全事件应急预案》的通知

各部门、各单位：

现将《广西工商职业技术学院网络安全事件应急预案》印发给你们，请遵照执行。

广西工商职业技术学院

2021 年 7 月 7 日

广西工商职业技术学院网络安全事件应急预案

1 总则

1.1 编制目的。根据《广西壮族自治区教育系统网络安全事件应急预案》要求，健全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，提高我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。

1.2 编制依据。根据《中华人民共和国网络安全法》、《教育系统网络安全事件应急预案》、《广西壮族自治区教育系统网络安全事件应急预案》、广西壮族自治区教育厅的《网络安全事件报告与处置流程<试行>》及《信息安全事件分类分级指南》（GB/T20986—2007，以下简称《指南》）等文件规定。

1.3 适用范围。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，对社会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。其中信息内容安全事件，应参照有关规定和办法。

1.4 工作原则。网络与信息安全事件应急处置，依照“统一领导，快速反应，密切配合，科学处置”的组织原则和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的分级负责原则，实行预防和处置相结合，充分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

2 组织机构与职责

2.1 学校网络安全与信息化工作领导小组（以下简称网信领导小组）统筹协调全校网络安全事件应急工作，指导我校各部门、单位网络安全事件应急处置。当发生特别重大网络安全事件、重大网络安全事件时，在上级统一指挥下开展应急处置工作，具体参照《广西壮族自治区教育系统网

络安全事件应急预案》等相关规定执行。

2.2 网络安全与信息化工作领导小组办公室(以下简称网信办)负责网络安全应急管理事务性工作，对接自治区教育厅网络安全应急办公室，向学校网信领导小组报告网络安全事件情况，提出较大网络安全事件、一般网络安全事件的应对措施建议和意见，统筹组织学校网络安全监测工作，做好应急处置的技术支撑工作。

2.3 党委宣传部负责学校舆情监测；负责舆情突发事件的协调处置；负责应急处置过程中的舆论处置。

2.4 后勤管理处（保卫处）负责涉及人为破坏类安全事件的处置，配合做好网络与信息安全事件的相关处置工作，协助公安机关做好相关取证和处置等工作。

2.5 信息技术中心负责校园基础网络系统安全；负责计算机病毒疫情和大规模网络攻击事件的处置；负责学校安全事件应急处置的技术支持工作。

2.6 各部门、单位负责所建网络和信息系统（网站）的网络安全事件应急工作，切实落实相关具体工作。

3 安全事件的分类分级

3.1 网络安全事件分类。本预案中所称的网络与信息安全事件（以下简称安全事件）是指有害程序事件、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、灾害事件和其他网络安全事件。

（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、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（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。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（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。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

3.2 结合我校实际，以及网络安全事件可能造成的危害、可能发展蔓延的趋势等，网络安全事件分为四级：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。

3.2.1 特别重大网络安全事件（Ⅰ级）。事件对学校正常工作造成特别严重损害，造成严重社会影响，事态发展超出学校控制能力。

（1）因发生网络攻击、病毒感染或由于软硬件故障、灾害性事件导致学校大规模网络与信息系统（网站）瘫痪；

（2）校内重要基础设施（如：信息门户、移动端门户等）、校内核心业务系统或网站（如：学校主页、办事大厅等）遭受特别严重损失，丧失业务处理能力；

（3）校内重要基础设施、校内核心业务系统（网站）的重要敏感信息或关键数据丢失，或被窃取、篡改、假冒，对学校安全稳定和正常秩序造成特别严重影响；

（4）其他对学校安全稳定和正常秩序造成特别严重影响的网络安全事件。

3.2.2 重大网络安全事件（II级）。事件对学校正常工作造成严重损害，并造成一定社会影响，事态发展超出技术部门控制能力，需要学校各部门协同处置。

（1）因发生网络攻击、病毒感染或由于软硬件故障、灾害性事件导致学校区域性网络与信息系统（网站）瘫痪；

（2）校内重要基础设施（如：信息门户、移动端门户等）、校内核

心业务系统或网站（如：学校主页、办事大厅等）遭受严重损失，业务处理能力受到严重影响;

（3）校内重要基础设施、校内核心业务系统（网站）的重要敏感信息或关键数据丢失，或被窃取、篡改、假冒，对学校安全稳定和正常秩序造成严重影响;

（4）其他对学校安全稳定和正常秩序造成严重影响的网络安全事件。

3.2.3 较大网络安全事件（III 级）。对学校正常工作造成一定损害，但未造成社会影响，可由技术支持单位和信息技术中心协同处置的突发事件。

（1）因发生网络攻击、病毒感染或由于软硬件故障、灾害性事件导致学校小范围网络与信息系统（网站）瘫痪;

（2）重要业务系统（如校内二级单位重要系统）或网站（如校内二级单位主页）遭受较大损失，造成系统中断，明显影响系统效率，业务处理能力受到影响;

（3）重要业务系统（网站）的数据丢失，或被窃取、篡改、假冒，对学校安全稳定和正常秩序造成较大影响;

（4）其他对学校正常工作造成不利影响的网络安全事件。

3.2.4 一般网络安全事件（IV 级）：除上述情况外，其他对学校网络或信息系统（网站）造成一定影响的网络安全事件，但不危害学校整体工作，可由信息技术中心处置的突发事件。

4 处置程序

4.1 启动预案：发生安全事件后，信息技术中心和涉事单位应第一时间采有效措施，将损害和影响降低到最小范围，保留现场，并报告网信办开展相关处置工作。

4.2 事件定级：网信办组织有关单位，收集安全事件相关信息，鉴别性质，确定来源，弄清范围，评估安全事件带来的影响和损害，确认安全事件的类别和等级。如网络安全事件涉及学校相关部门，应通知相关部门负责人及时到达现场协助处理。

4.3 应急响应：根据安全事件等级采取相应的响应方式。

（1）I 级（特别重大）：网信办立即上报分管校领导和网信领导小组组长，网信领导小组上报自治区教育厅教育信息化管理处、公安部门，由上级主管部门会同学校网信领导小组统一组织、协调应急处置，网信办保持 24 小时联络通畅，技术保障人员 24 小时值班。

（2）II 级（重大）：网信办立即上报分管校领导和网信领导小组组长，网信领导小组上报自治区教育厅教育信息化管理处、公安部门，由网信领导小组统一指挥、协调应急处置。

（3）IV-III 级（较大--一般）：信息技术中心和信息系统建设、管理单位自行负责应急处置，做好处置记录，有关情况报分管校领导。

4.4 应急处理方式：根据安全事件分类采取不同应急处置方式。

（1）有害程序事件：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，及时进行杀毒处理。

（2）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，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：

外部入侵：判断入侵的来源，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。

（3）信息破坏事件：立即中止信息传输，跟踪应用程序、查看数据库安全审计记录查找信息被破坏的原因，提出修正方案和措施。

（4）信息内容安全事件：接到校内网站出现不良信息告知后，应迅速终止网站的服务、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。对公安机关要求我校协查的校外论坛或自媒体的不良信息事件，根据校园网上网相关记录查找信息发布人。

（5）设备设施故障事件：判断故障发生点和故障原因，迅速联系设备厂家尽快抢修故障设备,优先保证校园网主干网络和主要应用系统的运转。

（6）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：设备的断电与拆卸、搬迁等。

（7）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信息安全公司或顾问，以及上级信息安全机构。

4.5 后续处理

（1）安全事件经初步应急处置后，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。

（2）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。

（3）安全事件处置后，及时清理系统，恢复数据、程序和服务。

4.6 记录报告。报告内容包括：时间地点，简要经过，事件类型与分级，影响范围，危害程度，初步原因分析，已采取的紧急措施。在事件处置工作中，做好完整的过程记录，事发 8 小时内填写《网络安全事件情况报告》(附件 2) ，保存各相关系统日志，直至处置工作结束。特别重大网络安全事件、重大网络安全事件，网信领导小组第一时间报告教育厅教育信息化管理处，涉及人为主观破坏事件应同时报当地公安机关。

4.7 结束响应，整改上报。系统恢复运行后，网信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、整改报告，在处置完毕后 5 个工作日内填写《网络安全事件整改报告》(附件 3)。特别重大网络安全事件、重大网络安全事件整改报告，报送教育厅信息化管理处。

5 附则

5.1 预案管理。本预案根据实际情况适时修订。修订工作由学校网信办（信息技术中心）组织。

5.2 预案解释。本预案由学校网信办（信息技术中心）负责解释。

5.3 预案实施时间。本预案自印发之日起实施。

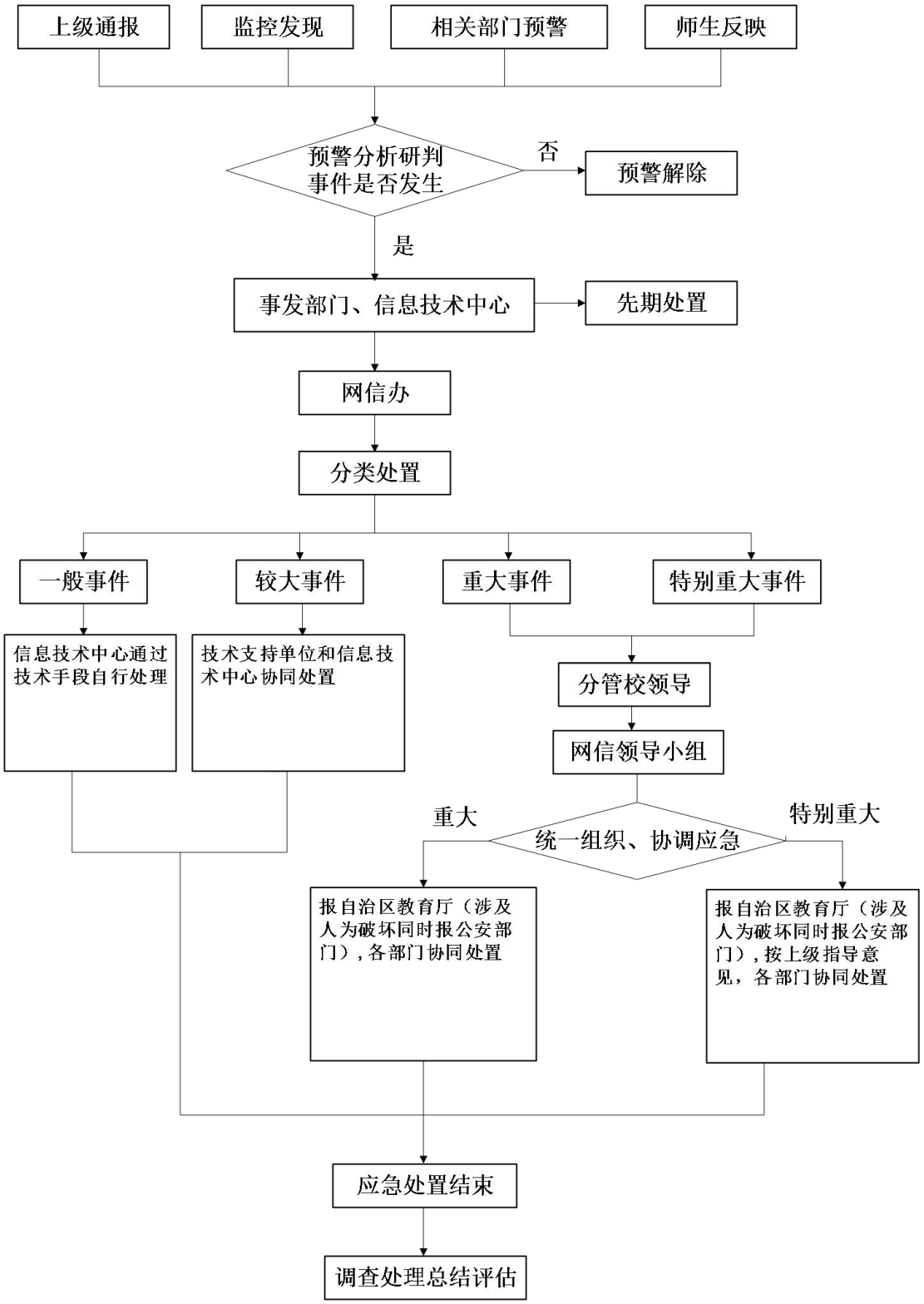
附件：1. 处置程序流程图

2. 网络安全事件情况报告

3. 教育系统网络安全事件情况报告

附件 1

处置程序流程图


上级通报
监控发现
相关部门预警
师生反映
预警分析研判
事件是否发生
否
预警解除
是
事发部门、信息技术中心
先期处置
网信办
分类处置
一般事件
较大事件
重大事件
特别重大事件
信息技术中心通过技术手段自行处理
技术支持单位和信息技术中心协同处置
分管校领导
网信领导小组
重大
统一组织、协调应急
特别重大
报自治区教育厅（涉及人为破坏同时报公安部门），各部门协同处置
报自治区教育厅（涉及人为破坏同时报公安部门），按上级指导意见，各部门协同处置
应急处置结束
调查处理总结评估

附件 2

网络安全事件情况报告

单位名称：　　（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	☐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	
网络安全分管负责人意见（签字）	
主要负责人意见（签字）	

附件 3

网络安全事件整改报告

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	
网络安全分管负责人意见（签字）	
单位主要负责人意见（签字）	