广东石油化工学院文件

广油〔2020〕22号

关于印发《广东石油化工学院信息技术安全事件报告与处置流程（试行）》的通知

各单位、部门:

经校长办公会议和党委常委会会议审议通过，现将《广东石油化工学院信息技术安全事件报告与处置流程（试行）》印发给你们，请遵照执行。执行中遇有问题，请及时与网络与教育信息技术中心联系。

广东石油化工学院

2020年6月29日

广东石油化工学院信息技术安全事件报告与处置流程（试行）

第一条 为进一步规范我校信息技术安全事件报告与处置工作，提高网络安全管理水平和安全事件应急处置能力，及时掌握和处置信息技术安全事件，降低安全事件带来的损失与影响，根据《中华人民共和国网络安全法》等有关法律法规，参照教育部《信息技术安全事件报告与处置流程（试行）》有关规定，制定本流程。

第二条 信息技术安全事件定义。根据《信息安全事件分类分级指南》（GB/T20986-2007，以下简称《指南》），本流程中所称的信息技术安全事件（以下简称“安全事件”）是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。（详见附件 1）

第三条 适用范围。本流程适用于我校各单位、部门信息技术安全事件的报告与处置工作，涉及信息内容安全事件的报告与处置工作仍按相关规定执行。

第四条 安全事件等级划分。根据《指南》将安全事件划分为四个等级：特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级）。（详见附件 1）

第五条 安全事件判定。一旦发生安全事件，应根据《指南》，视网络与信息系统重要程度、损失情况以及对工作和社会造成的影响，由网络与教育信息技术中心作专业判断，提出安全事件等

级建议，报网络安全与信息化工作领导小组（以下简称“领导小组”）确定事件等级。

第六条 Ⅰ至Ⅲ级安全事件的报告与处置。报告与处置分为三个步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

（一）事发紧急报告与处置

1.发现安全事件，网络与信息系统运维操作人员或个人应根据实际情况第一时间主动采取断网等有效措施进行先期处置，将损害和影响降到最小范围，保留现场，并报告本单位信息技术安全责任人、主要负责人和网络与教育信息技术中心。

2.网络与教育信息技术中心接到报告后，应立即组织技术人员进行紧急处置，并提出安全事件等级建议，及时报告领导小组。涉及人为主观破坏事件应同时报告公安机关。对确认属Ⅰ至Ⅲ级安全事件的，领导小组应上报有关部门并与公安等部门联系。

3.紧急报告内容包括：（1）时间地点；（2）简要经过；（3）事件类型与分级；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

（二）事中情况报告与处置

1.事中情况报告应在安全事件发现后 8 小时内以书面报告的形式报送领导小组。（报送内容和格式详见附件 2）

2.事中情况报告由部门安全负责人组织管理和运维人员编写，网络与教育信息技术中心配合，部门主要负责人审核后，签字并加盖公章报送领导小组办公室。领导小组办公室依据报告上

报相关部门。

3.安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。

（三）事后整改报告与处置

1.事后整改报告应在安全事件处置完毕后 3 个工作日内以书面报告的形式报送整改报告。（报送内容和格式见附件 3）

2.事后情况报告由部门安全负责人组织管理和运维人员编写，网络与教育信息技术中心配合，部门主要负责人审核后，签字并加盖公章报送领导小组办公室。领导小组办公室依据报告上报相关部门。

3.安全事件事后处置包括：进一步总结事件教训，研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。

第七条 一般安全事件报告与处置。网络与信息系统发生一般安全事件，应及时、自主组织应急处置工作，在事件处置完毕后 7 天内将整改报告报送领导小组办公室。（报告内容和格式详见附件 3）

第八条 人员变更报告。各单位的信息技术安全工作主管领导、管理员、联络方式发生变更的，应及时报送领导小组办公室。

第九条 相关配套机制

（一）网络与教育信息技术中心应每天登录上级主管部门、行业等安全平台，及时发现和处置上级主管部门、行业通报的信息技术安全事件，并根据主管部门、行业要求进行反馈。

（二）网络与教育信息技术中心定期对全校网站、信息系统进行漏洞扫描，向网站、信息系统主管部门发放扫描报告，并要求收到通报的主管部门进行整改、填写反馈表。（详见附件 4）

1. 对既不整改又不反馈的部门主管的网站、信息系统，经领导小组同意，网络与教育信息技术中心对其采取限制访问、关闭等措施。

2. 对无法整改又必须开放网站、信息系统，按照“尽职免责、失职追责”的基本原则，主管部门应妥善做好系统的管理工作，并签署责任知晓确认书（详见附件 5）。经领导小组同意，可以继续开放使用。

（三）网络与教育信息技术中心通过安全态势感知平台监测全校网络终端、服务器信息技术安全事件，向有关单位、部门或个人发放安全通报（详见附件 6），通报 1 次/2 周，要求收到通报的单位、部门或个人限期整改、填写反馈表（详见附件 4）。为防止信息技术安全事件扩散，以下情况对涉事账号采取断网措施，并向当事单位发出广东石油化工学院上网账号断网通报（详见附件 7）:

1. 未能按照上级主管部门、行业安全通报的整改限期内完成整改的;

2. 接到校内通报，未整改、未反馈且安全事件持续一周及以上的;

3. 因同一安全事件被连续通报三次及以上的。

（四）断网账号线下完成整改后，填写广东石油化工学院上

网账号复通申请表（详见附件 8），可申请账号复通。是否可以予以复通，由领导小组主要成员单位（网络与教育信息技术中心、宣传部、党办校办、保卫处）在每月安全研判会上讨论确定。特殊情况下，可经当事人所在部门及部门分管校领导审批后进行账号复通。

第十条 各单位、部门应按照学校信息技术安全事件报告与处置流程，建立值守制度，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。做到安全事件早发现、早报告、早控制、早解决。

第十一条 问责制度。各单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，将依照有关规定严肃追责问责。

第十二条 本流程由学校负责解释，具体解释工作由网络安全与信息化工作领导小组办公室承担。

第十三条 本流程自发布之日起开始施行。

附件 1

信息技术安全事件分类与等级划分

《信息安全事件分类分级指南》（GB/Z 20986-2007）根据信息技术安全事件的起因、表现、结果等，将信息技术安全事件分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件 6 个基本分类，每个基本分类分别包括若干个子类；根据信息系统重要程度、系统损失和社会影响，将信息技术安全事件划分为 4 个等级。

一、信息技术安全事件分类

1.有害程序事件

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序事件包括计算机病毒事件、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等 7 个子类。

2.网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包括拒绝服务攻击事件、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等 7 个子类。

3.信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、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等 6 个子类。

4.设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障等 4 个子类。

5.灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

6.其他事件

其他事件是指不能归为以上基本分类的信息技术安全事件。

二、信息技术安全事件等级划分

1.特别重大事件（Ⅰ级）

特别重大事件是指导致特别严重影响或破坏的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受特别严重的系统损失;

（2）产生特别重大的社会影响。

2. 重大事件（II级）

重大事件是指导致严重影响或破坏的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失;

（2）产生的重大的社会影响。

3.较大事件（III级）

较大事件是指导致较严重影响或破坏的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失;

（2）产生较大的社会影响。

4.一般事件（IV级）

一般事件是指不满足以上条件的信息安全事件，包括以下情况:

（1）会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失、一般信息系统遭受严重或严重以下级别的系统损失;

（2）产生一般的社会影响。

附件 2

广东石油化工学院
信息技术安全事件情况报告

单位名称：（加盖公章）　　事发时间：____年____月___日___时___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			
信息系统的基本情况（如涉及请填写）	系统名称：_____ 系统网址和 IP 地址：_____ 系统主管单位/部门：_____ 系统运维单位/部门：_____ 系统使用单位/部门：_____ 系统主要用途：_____ _____ 7.是否定级 ☐是 所定级别：_____，　☐否 8.是否备案 ☐是 备案号：_____，　☐否 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	
部门安全负责人意见	负责人签字：　　年　　月　　日
网络安全与信息化工作 领导小组办公室意见	负责人签字：　　年　　月　　日 （网络与教育信息技术中心 代章）

注：此表 A4 纸双面打印，交由网络与教育信息技术中心（官渡校区二教 A1106 室）代收。

附件 3

广东石油化工学院
信息技术安全事件整改报告

单位名称：（加盖公章）　　报告时间：_____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 所定级别：_____，　☐否 8.是否备案　☐是 备案号：_____，　☐否 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	
部门安全负责人意见	负责人签字：　　年　　月　　日
网络安全与信息化工作领导小组办公室意见	负责人签字：　　年　　月　　日 （网络与教育信息技术中心 代章）

注：此表 A4 纸双面打印，交由网络与教育信息技术中心（官渡校区二教 A1106 室）代收。

附件 4

广东石油化工学院信息技术安全事件处理情况反馈表

收文时间（收文单位填写）：　　年　　月　　日

<table>
<tr><td colspan="4">事件名称：网站 □ 名称_____
信息系统 □ 名称_____
单位/个人 □ 通报编号 _____</td></tr>
<tr><td colspan="4">事件涉及 IP 地址：</td></tr>
<tr><td>单位名称（盖章）</td><td></td><td>单位领导签名</td><td></td></tr>
<tr><td>接收通报时间</td><td></td><td>反馈时间</td><td></td></tr>
<tr><td>事件处理负责人</td><td></td><td>负责人电话</td><td></td></tr>
<tr><td>负责人电子邮箱</td><td colspan="3"></td></tr>
<tr><td>事件处理经过：</td><td colspan="3"></td></tr>
</table>

注：此表交由网络与教育信息技术中心（官渡校区二教 A1106 室）代收。

附件 5

广东石油化工学院
信息技术安全责任知晓确认书

收文时间（收文单位填写）：　　年　　月　　日

<table>
<tr><td>网站、信息系统名称</td><td></td><td>上线时间</td><td></td></tr>
<tr><td>网站、信息系统网址</td><td colspan="3"></td></tr>
<tr><td>开发商名称</td><td></td><td>维保期</td><td>是□ 否□</td></tr>
<tr><td>信息技术安全
隐患情况</td><td colspan="3">系统漏洞扫描报告（报告编号）：_____
本网站（信息系统）存在　高危漏洞：_____ 个
中危漏洞：_____ 个
本系统所在平台存在　高危漏洞：_____ 个
中危漏洞：_____ 个
上述情况表明系统存在严重安全隐患，亟待整改。</td></tr>
<tr><td colspan="4">我单位已知晓我单位负责的网站（信息系统）存在严重安全隐患，也积极联系厂商技术人员进行漏洞处置，但由于_____原因无法修复。该系统为重要的业务系统，必须向师生开放，不能关闭，特申请继续开放该系统。
申请开放范围：　□校园网　　□互联网
为保证学校网络信息安全，我单位将在_____年____月____日之前对该系统进行升级，完成网络信息安全隐患整改。
按照“谁主管、谁负责，谁使用、谁负责”的原则，我单位明确了解本单位应负责该网站的安全责任，将安排专人负责该系统的安全运行。

单位（盖章）　　单位领导签名：　　年　　月　　日</td></tr>
<tr><td>分管校领导意见</td><td colspan="3">签名：　　年　　月　　日</td></tr>
<tr><td>网络安全与信息化工作
领导小组意见</td><td colspan="3">签名：　　年　　月　　日</td></tr>
</table>

注：此表分管校领导签字后，交由网络与教育信息技术中心（官渡校区二教 A1106 室）代收。

附件 6

通报编号:

广东石油化工学院信息技术安全事件通报

_____（单位、部门）:

经检测发现_____（用户）办公上网账号（IP 地址）所在计算机存在网络安全隐患，详见附件: _____（附件名称），用户计算机存在资料信息被非法窃取或被非法用户远程控制等风险，给学校网络信息安全带来较大的安全隐患。

按照《广东石油化工学院信息技术安全事件报告与处置流程》，请通知用户在接到本通报后五天内，尽快备份资料，查杀木马病毒，卸载或弃用存在木马病毒的系统和应用程序，积极处置安全隐患。为了保障校园网络信息安全，未能完成安全隐患处置的用户上网账号将被关停。

请贵单位督促用户完成安全隐患处置，并填写《广东石油化工学院信息技术安全事件处理情况反馈表》，电子版发送到 xf@gdupt.edu.cn，纸质版交到网络与教育信息技术中心，地点：二教 A11 楼 1106，电话：2923790，联系人：薛锋。

检测人: _____ 审核人: _____

附件: 主机安全风险报告

网络与教育信息技术中心

年　　月　　日

附件 7

通报编号:

广东石油化工学院上网账号断网通报

_____（单位、部门）:

贵单位_____（用户）办公上网账号（IP 地址）所在计算机存在网络安全隐患，给学校网络信息安全带来较大的安全隐患。网络与教育信息技术中心已将该问题通报给贵单位，通报情况如下:

（1）_____年_____月_____日，信息技术安全事件通报编号: _____;

（2）_____年_____月_____日，信息技术安全事件通报编号: _____;

（3）_____年_____月_____日，信息技术安全事件通报编号: _____;

该用户:

□ 未能按照上级主管部门、行业安全通报的整改限期内完成整改。

□ 接到校内通报，未整改、未反馈且安全事件持续一周及以上。

□ 因同一安全事件被连续通报三次及以上。

按照《广东石油化工学院信息技术安全事件报告与处置流程》第七条的规定，对该用户的上网账号予以关闭，特此函告。

网络安全与信息化工作领导小组办公室

（网络与教育信息技术中心代章）

年　　月

附件 8

广东石油化工学院上网账号复通申请表

申请人		复通账号名称：	
处理经过	（主要针对被关停账号曾用计算机木马病毒查杀情况、操作系统更新情况、是否使用注册机破解版等情况进行说明）		
申请人所在单位意见	单位意见： 单位负责人（盖章）：　　年　月　日 提交审批： □网络安全与信息化工作领导小组 □分管校领导：　　（特殊情况报请校领导审批）		
网络安全与信息化工作领导小组成员单位负责人审批	网络与教育信息技术中心： 宣传部： 党办校办： 保卫处：		

注：此表签字后，交由网络与教育信息技术中心（官渡校区二教 A1106 室）代收。

公开方式：主动公开

校对人：陈文海

广东石油化工学院办公室　　2020年7月2日印发