常 熟 理 工 学 院 文 件

常理工信〔2020〕2 号

关于印发《常熟理工学院网络安全监控管理办法》等规定的通知

各二级学院，各部门：

《常熟理工学院网络安全监控管理办法》、《常熟理工学院网络安全事件报告与处置流程》、《常熟理工学院网络安全隐患处理规定》已经院长办公会议审议通过，现予印发，请遵照执行。

常熟理工学院

2020 年 10 月 19 日

常熟理工学院网络安全监控管理办法

第一章 总 则

第一条 目的：为保障常熟理工学院校园网络的安全稳定运行，确保各项业务正常平稳开展，合理规范网络系统运行监控操作，有效控制可能发生的各种风险，提高网络系统安全运行管理的科学化、规范化水平，特制定本管理办法。

第二条 依据：本管理办法根据《常熟理工学院网络与信息安全管理办法》制订。

第三条 范围：本管理办法适用于我校机关部门、二级学院、直属单位等机构。

第二章 遵循原则

第四条 预防性原则：遵循以预防为主、防患于未然的原则，预防案件、事故的发生。

第五条 可审计性原则：网络系统的运行监控过程必须保留痕迹，可被审计或追溯。

第六条 监督制约原则：针对网络应用与管理工作中各个环节，建立相应的监督检查机制。

第二章 人员管理

第七条 运行网络监控工作涉及的人员主要有：网络运行值班人员、网络管理员、安全管理员。

第八条 各个监控环节制定相关操作规程。各环节管理员不得混岗，应有人员备份，并建立人员管理记录。

第三章 日常运行监控

第九条 计算机中心机房运行值班人员实行 7×24 小时双人现场值班。

第十条 网络管理员正常工作时间实行现场值班，休息日与节假日为后台离线值班，接到电话及时到现场。

第十一条 现场值班要求

(一) 值班人员发现问题后，首先记录故障现象并上报主管人员，初步判断问题类型，对权限许可处理的问题及时处理，对无权处理或不能处理的问题，电话通知当班技术人员到场；

(二) 值班人员在联系负责处理问题的责任人时，正常响应时间为 5 分钟。超过正常响应时间无人响应，则逐级通知被呼人员的上级；若 10 分钟后仍未响应，则直接通知信息化办公室负责人。对重大问题（如网络瘫痪等）必须立即报告信息化办公室负责人和分管校领导。

第十二条 后台值班要求

(一)保证个人通讯渠道畅通，在现场值班人员呼叫时，必须在 5 分钟内响应；

(二)需要前往运行机房现场处理的问题，应在 1 小时之内赶到机房处理。

第十三条 运行值班人员职责

实时监控中心机房网络连接状态，对各种异常的情况，应及时报告上级主管人员。

第十四条 网络管理员职责

主要负责全行网络系统的运行情况。主要包括：

（一） 定期检查网络软、硬件设备运行情况，每天一次。

（二） 定期检查网络布线情况，确保配线的合理有序，每月一次。

（三） 定期检查各种设备接入网络的情况，每月一次。

（四） 实时监控中心机房的网络运转和网络通信流量情况。

（五） 定期检查外部网络的连接配置，监控网络通信状况，防止外部入侵。

第十五条 安全管理员职责

负责对网络日志进行监控检查，分析系统可能存在的安全隐患和漏洞，及时研究并提出补救措施，指导运行监控网络安全技术规范的制定与实施。

第四章 检查监督

第十六条 信息化办公室每季度进行一次自查，对检查中发现的问题认真分析并提出切实可行的整改意见。

第十七条 检查内容主要为运行监控记录是否完整，监控记录是否与实际情况相符等。

第五章 附 则

第十八条 本管理办法由信息化办公室负责解释和修订。

第十九条 本管理办法自发布之日起施行。

常熟理工学院网络安全事件报告与处置流程

（试行）

为加强我校网络安全工作，及时掌握和处置网络安全安全事件，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，维护正常工作秩序和营造健康的网络环境，根据《教育部进一步加强直属高校直属单位网络安全工作的通知》(教技〔2015〕1 号)、教育部《信息技术安全事件报告与处置流程》(教技厅函〔2014〕75 号)以及《常熟理工学院网络与信息安全管理办法》结合学校实际，制定本流程。

第一章 总则

第一条 网络安全事件的定义。根据《信息安全事件分类分级指南》(GB/20986-2007，以下简称《指南》，摘录部分见附件 1)，本流程中所称的网络安全事件(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。

第二条 适用范围。本流程适用于我校各单位发生的网络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按其相关规定执行。

第二章 安全事件等级划分与判定

第三条 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(IVN 级)，详见附件 1。

第四条 安全事件判定。我校各单位一旦发生安全事件，应根据《指南》，视信息系统重要程度、损失情况以及对工作和社会造成的影响迅速自主判定安全事件等级。信息化办公室在接到报告后，根据事件情况，进一步做出判定。必要时，信息化办公室组织专家组进行判定或报告学校网络安全与信息化领导小组判定。

第三章 安全事件的报告与处置

第五条 I 至III级信息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.网络与信息系统运维操作人员一旦发现上述安全事件，应根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位第一责任人和直接责任人。

2.本单位第一责任人接到报告后，应立即组织相关人员赶赴现场进行紧急处置，同时以口头通讯的方式将相关情况通报至

信息化办公室，并书面记录安全事件发现过程及口头汇报过程。涉及人为主观破坏事件应同时报告学校保卫部门。

3.信息化办公室接到报告后，应做好书面记录，并进一步判定安全事件等级，对确认属Ⅰ至Ⅲ级安全事件的，应报告网络安全与信息化领导小组相关领导。

4.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。

5.对确认属Ⅰ至Ⅲ级安全事件的，信息化办公室应立即组织相关技术力量赶赴现场进行协助处置工作。

涉及人为主观破坏事件的，学校保卫部门应组织人员赴现场协助处置，并协助公安机关做好相关取证和处置工作。

6.各单位应及时跟进事件发展情况，出现新的重大情况应及时补报。

(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6小时内以书面报告的形式进行报送，报送内容和格式见附件2。

2.事中情况报告由单位直接责任人组织编写，由本单位第一责任人审核后，签字并加盖公章报送信息化办公室。

涉及人为主观破坏事件的，事中情况报告应抄送给保卫处。

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。如果涉及人为主观破坏的安全事件应由保卫处联系、配合公安部门和学校保卫部门开展调查

(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4个工作日内以书面报告的形式进行报送，报送内容和格式见附件3。

2.事后情况报告由单位直接责任人组织编写，由本单位第一责任人人审核后，签字并加盖公章报送信息化办公室。

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。如涉及人为主观破坏的安全事件应继续配合公安部门和学校保卫部门开展调查。

第六条 一般安全事件(Ⅳ级)报告与处置。各单位发生一般安全事件，应及时、自主组织应急处置工作；需要信息化办公室协助的，联系信息化办公室予以协助。在事件处置完毕后 6天内向信息化办公室报送整改报告，报告内容和格式见附件3。

第七条 预警类信息的报告与处置。

各单位要按时、按要求完成国家、地方有关信息安全部门以及学校信息化办公室等部门通报的预警类信息的处置工作，并按要求形成书面报告，报送信息化办公室。

第四章 配套制度与问责

第八条 人事变更报告。为保障联络通畅，各单位第一责任人、直接责任人的联络方式发生变更的，应及时向信息化办公室报备。

第九条 相关配套机制。各单位应根据实际建立本单位的笪值守制度，做到安全事件早预警、早发现、早报告、早控制、早解决。各单位应建立健全本单位安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练。

第十条 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，信息化办公室将对相关单位进行约谈或通报；情况严重的，根据《常熟理工学院网络与信息安全管理办法》的责任追究条款问责处理。

第十一条 整改落实机制。发生Ⅰ至Ⅲ级安全事件后，要认真做好整改落实工作，坚持做到事故原因不查清不放过、整改措施未落实不放过、责任人员未受到教育或处理不放过，尽力杜绝类似事件再次发生。

第五章 附则

第十二条 本流程自发布之日起施行，由信息化办公室负责解释。

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于个子类;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)

特别重大事件是指能够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)

重大事件是指能够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)

较大事件是指能够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

常熟理工学院信息技术安全事件情况报告

单位名称：(公章)　　事发时间：　年　月　日　分

联系人 姓　名		移动电话	
		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	
直　接责任人意　见	签名：　　年　月　日
第　一负责人意　见	签名：　　年　月　日

附件 3

常熟理工学院信息技术安全事件整改报告

单位名称：（公章）　　事发时间：　年　月　日　分

联系人 姓　名		移动电话	
		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	
是否需要应急支援及需支援事　　项	
直　接责任人意　见	签名：　　年　　月　　日
第　一负责人意　见	签名：　　年　　月　　日

常熟理工学院网络安全隐患处理规定

一、安全隐患发现

学校从江苏省教育网络和信息安全通报平台、教育行业漏洞报告平台、公安机关、校内师生等途径获取网络安全隐患通报信息，通过信息化办公室工作人员对信息资产进行定期漏扫，通过关注的CVE信息发布获取漏洞信息。

二、安全隐患（漏洞）初步处置

对于发现安全隐患（漏洞）的网站（系统），第一时间调整策略，限制其访问范围（仅网络安全工作人员及网站管理员可访问），防止事态扩大。信息化办公室技术人员通过漏洞扫描系统和其他工具，对漏洞进行验证，以便后期进行漏洞修复情况的复核。

三、整改通知和反馈

对于经过漏洞验证的系统，信息化办公室下发整改通知书（含整改建议）、网络安全隐患处置情况反馈表等到相关二级学院（部门），要求限期整改并反馈整改情况。

四、整改情况复核

在收到二级学院（部门）提交的处置情况反馈表后，信息化办公室组织技术人员对漏洞修复情况进行复核。如果复核通过，则恢复系统的对外服务；如果复核不通过，则继续

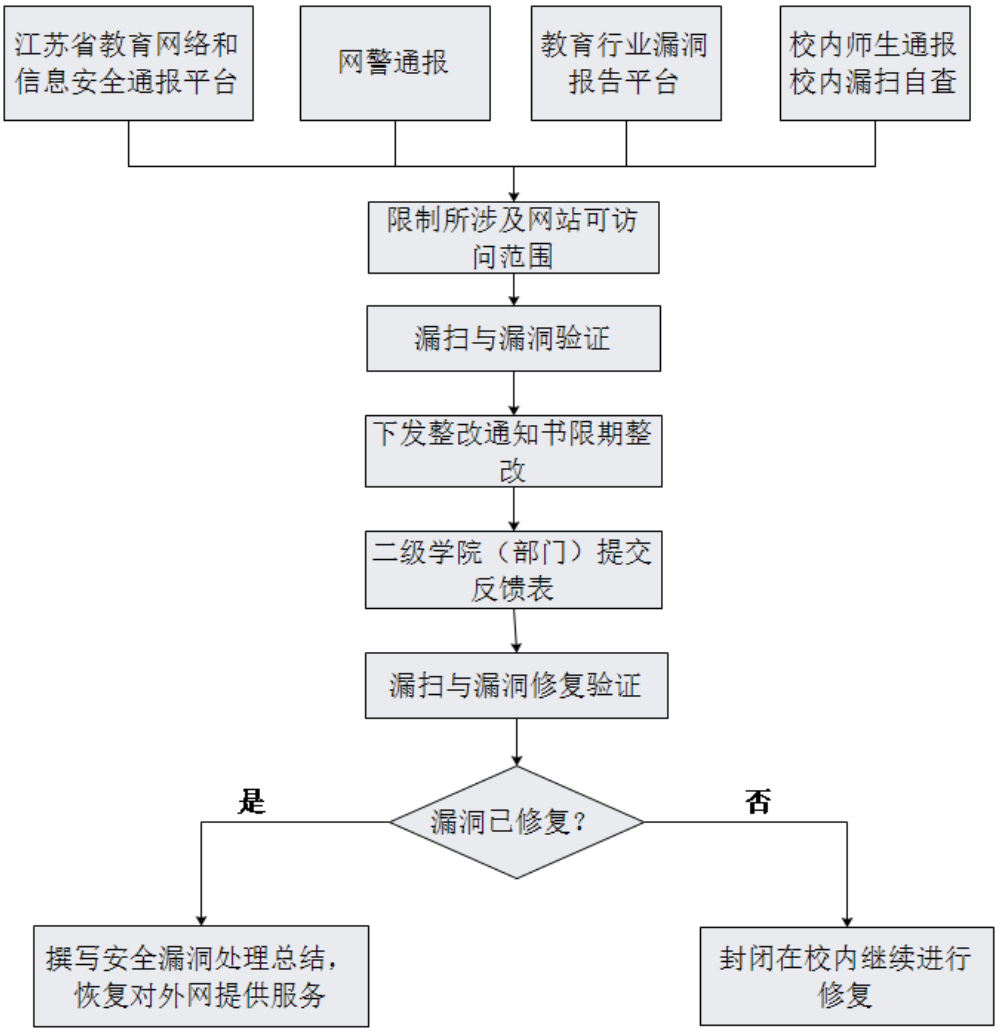
限制访问范围进行修复工作。

对于相关通报平台上的漏洞通报，及时进行流程处置。

五、总结阶段

针对本次网络安全隐患通报进行总结，包括处置过程、漏洞验证（重现）技术手段、漏洞修复方法、漏洞复核结果等。同时记录到数据库，方便后续统计分析。

网络安全隐患处理流程


江苏省教育网络和信息安全通报平台
网警通报
教育行业漏洞报告平台
校内师生通报校内漏扫自查
限制所涉及网站可访问范围
漏扫与漏洞验证
下发整改通知书限期整改
二级学院（部门）提交反馈表
漏扫与漏洞修复验证
漏洞已修复？
是
否
撰写安全漏洞处理总结，恢复对外网提供服务
封闭在校内继续进行修复

附件一

常熟理工学院校园网络整改通知书

_____:

_____发现，你单位网络存在高危隐患、请接到通知后，于____年___月___日前整改完毕，并将整改情况于_____年___月___日___时前交至信息化办公室。

查内容	你单位部署运营的　　，存在　　被控制的风险，危害严重。
改建议	
改要求	根据《网络安全法》、《计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》、《常熟理工学院网络与信息安全管理办法》等要求，请你单位立即组织技术力量进行核查整改，尽快消除安全隐患，完善内部安全管理制度和操作规程，落实网络保护责任。 签收人： 日期：
理结果	

本文书一式两份，一份交被检查单位，一份由信息化办公室存档

附件二

常熟理工学院网站安全隐患处置结果反馈表

网站名称		网站域名	
网站责任部门（盖章）		网站 IP	
部门责任人		联系电话	
服务器存放地址			
管理员		管理员电话	
系统研发单位		研发时间	
处置记录（包含问题原因、问题处置过程、问题处置结果）			
填表人		联系电话	