武汉纺织大学外经贸学院文件

院发〔2019〕3号

关于印发《武汉纺织大学外经贸学院信息安全应急响应管理规定》的通知

各单位:

《武汉纺织大学外经贸学院信息安全应急响应管理规定》已经学校办公会审议通过，现予以印发，请遵照执行。

特此通知。

武汉纺织大学外经贸学院

2019年9月29日

武汉纺织大学外经贸学院学校办公室　　2019年9月29日印发

共印23份

武汉纺织大学外经贸学院信息安全应急响应管理规定

为有效预防、及时控制和妥善处理网络和信息安全类突发事件，建立健全应急机制，提高快速反应和应急处理能力，保证正常的教学、科研、生活秩序，维护学校稳定，特制定本管理规定。

第一条 响应预案管理

武汉纺织大学外经贸学院网络安全与信息化工作领导小组办公室（以下简称网信办）按照信息系统安全运行情况，制定应急计划和响应预案，并按以下要求进行管理:

(一) 网信办负责制定应急计划和响应策略文档，按照要求进行评审，并填写《武汉纺织大学外经贸学院信息安全运行管理策略审批表》（见附件 1）;

(二) 网信办每年制定信息安全应急响应知识、技术和技能的培训计划，并组织实施;

(三) 网信办根据评审通过的应急计划和响应策略，每年组织一次应急响应模拟演练，对演练过程进行详细记录，填写《武汉纺织大学外经贸学院信息安全应急响应演练记录表》（见附件 2）; 每次应急响应演练结束后，网信办组织相关人员对演练效果进行评估，网信办对应急计划和响应策略进行修正和改进，适时更新应急预案。

第二条 信息安全事件分类与监测

(一) 事件分类

1. 信息安全事件

依据《中华人民共和国网络安全法》《GBT 24363-2009 信息安全技信息安全应急响应计划规范》《GB\T 20984-2007 信息安全技术 信息安全风险评估规范》《GB\Z 20985-2007 信息安全技术 信息网络攻

击事件管理指南》《GB\Z 20986-2007 信息安全技术信息网络攻击事件分类分级指南》等多部法律法规文件，根据信息安全事件发生的原因、表现形式等，结合学校的情况，将信息安全事件分为网络攻击事件、有害程序事件、信息泄密事件和信息内容安全事件四大类。

（1）网络攻击事件

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，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、干扰事件等。

（2）有害程序事件

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。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等。

（3）信息泄露事件

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，导致的信息安全事件。信息泄露事件包括专利泄露、系统主动监控及异常查单、泄露师生资料、泄露学校内部密级文件等。

（4）信息内容安全事件

利用信息网络发布、传播危害国家安全、社会稳定、公共利益和学校利益的内容的安全事件。包括违反法律、法规和学校规定的信息安全事件；针对社会事项进行讨论、评论，形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件。

2. 系统运行安全事件

按照性质又可分为物理类、系统类、网络类、病毒类、攻击类、

管理类、应用类、其它类。

(二)事件分级

信息安全事件的分级如下:

依据《GB\Z 20985-2007 信息安全技术 信息网络攻击事件管理指南》、《GB\Z 20986-2007 信息安全技术信息网络攻击事件分类分级指南》等法律法规文件，从以下因素进行考虑:

信息密级:衡量因信息安全事件中所涉及信息的重要程度的要素;

声誉影响:衡量因信息安全事件对学校品牌所造成的负面影响范围和程度的要素;

业务影响:衡量因信息安全事件对学校或事发部门正常业务开展所造成的负面影响程度的要素;

资产损失:衡量因恢复系统正常运行和消除信息安全事件负面影响所需付出资金代价的要素。

根据信息安全事件的分级考虑要素，将本校所发生的信息安全事件划分为两个级别:重大运行安全事件和一般运行安全事件;

1.重大运行安全事件包括:

(1)大面积病毒木马感染;

(2)黑客入侵;

(3)关键设备损坏;

(4)系统瘫痪;

(5)关键业务数据丢失、损坏;

(6)大面积网络连接故障;

(7)其他重大运行安全事件。

2.一般运行安全事件包括:

(1)局部病毒木马感染;

(2)网站受到攻击;

（3）一般网络设备损坏；

（4）一般业务数据丢失、损坏；

（5）局部网络瘫痪；

（6）局部网络连接故障；

（7）其他一般运行安全事件。

（三）事件监测

根据系统运行实际情况，结合系统内实施的安全审计等措施，进行系统内异常事件的检测。监测发现异常事件，相关人员须立即按照异常事件处置程序进行上报和查处，异常事件的监测有以下几种方式：

1. 电子监控；

2. 病毒检测；

3. 入侵检测；

4. 安全审计；

5. 人为发现；

6. 其他事件监测方式。

第三条 事件处置

1. 职责划分：学校网络安全与信息化领导小组是学校网络安全事件处置的指挥机构。

2. 运行安全事件的查处原则：积极主动上报、及时反馈处理、总结评估改进。

3. 事件查处程序

（1）事件分析：通过排查事件发生的现象和隐患，准确确定事件发生的原因、类型、源头和影响的范围；

（2）切断源头：在确定准确的事件发生源后，系统管理员要立即切断事件发生的源头，将事件发生源与信息系统物理断开，使事件的影响范围降到最小程度；

（3）原因清楚：事件定性后，通过安全理论分析或事件跟踪、监测等手段查清和确定事件发生的根本原因；

（4）事件重现：通过模拟攻击，仿真试验或其它测试方法重复事件发生机理，从而验证事件原因和影响分析的准确性；

（5）措施有效：在事件原因和影响分析准确的基础上，网信办制定和验证有效的补救措施，并迅速采取补救措施对事件进行处理，重大安全事件的补救措施由网信办组织评审确认；

（6）追究责任：根据实际情况提出口头警告、书面警告、停止使用网络，情节严重和后果影响较大者，提交学校及国家司法机关处理，追究部门负责人和直接责任人的行政或法律责任。

（7）预防改进：事件处理完毕，要对事件查处过程进行总结，改进相关的运行管理策略，采取预防措施、动态监控，做好工作日志，防止和杜绝同类问题的再次发生。

第四条 生效说明

本规定由武汉纺织大学外经贸学院网信办负责解释。本规定自印发之日起实施，原有规定与本规定不一致的，以本规定为准。

附件：1. 武汉纺织大学外经贸学院信息安全运行管理策略审批表

2. 武汉纺织大学外经贸学院信息安全应急响应演练记录表

附件 1

武汉纺织大学外经贸学院信息安全运行管理策略审批表

文件代号			
文件名称			
适用范围			
策略说明			
编制人		编制日期	
验证情况 说　明			
验证人员		验证日期	
评估结果			
评估人员		评估日期	
网信办意见	签名/日期：		
网络安全与信息化工作领导小组 意见	签名/日期：		

附件 2

武汉纺织大学外经贸学院安全应急响应演练记录表

演练时间		演练地点	
参加人员 及 职 责			
演练内容			
演练目的			
演练过程			
演练效果			
效果评估	签名/日期：		
记录人员		记录时间	