中共衡阳师范学院委员会文件

校党字[2018]50 号

关于印发《衡阳师范学院网络安全事件应急预案》的通知

各党总支、直属党支部，校属各部门：

经党委会研究同意，现将《衡阳师范学院网络安全事件应急预案》印发给你们，请结合实际，认真贯彻执行。

中共衡阳师范学院委员会

2018 年 11 月 5 日

衡阳师范学院网络安全事件应急预案

为健全完善教育系统网络安全事件应急工作机制，提高网络安全应急处置能力，根据《中华人民共和国网络安全法》《教育部教育系统网络安全事件应急预案》《湖南省教育系统网络安全事件应急预案》等有关法律法规及文件要求，结合我校工作实际，特制定本预案。

一、总则

（一）编制依据

本预案是依据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规,《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》《教育部教育系统网络安全事件应急预案》《湖南省教育系统网络安全事件应急预案》《湖南省教育厅<关于加强教育行业网络与信息安全工作的指导意见>》《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007)等文件编制而成。

（二）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、数据（信息）破坏事件、设备设施故障、灾害性事件和其他事件。信息内容安全事件的应对，参照有关规定和办法。

（三）事件分类与分级

本预案所指网络安全事件分为以下七类：

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、社会稳定和公众利益的事件。

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。

本预案参照《湖南省教育系统网络安全事件应急预案》事件分级规定，根据网络安全事件对我校影响范围、严重程度和可控性，分为以下四级：

I 级（特别重大）：网络与信息系统发生全校性大规模瘫痪或发生特别严重信息内容安全事件和信息破坏事件；对学校正常工作造成特别严重损害,且事态发展超出学校控制能力的安全事件。

II 级（重大）：学校网络与信息系统造成大面积瘫痪或发生严重信息内容安全事件和信息破坏事件，对学校正常工作造成严重损害，事态发展超出信息与网络中心控制能力，需学校各部门协同处置的安全事件。

III 级（较大）：学校某一区域的网络与信息系统瘫痪或发生较严重信息内容安全事件和信息破坏事件，对学校正常工作造成较严重损害，但可以在一定时间内通过相应技术手段进行重建和恢复，需信息与网络中心和网络安全事件影响区域所属各部门协同处理完成的安全事件。

IV 级（一般）：学校某一局部网络与信息系统受到一定程度损坏，或发生一定程度信息内容安全事件和信息破坏事件，对学校某些工作有一定影响，可以在短时间内通过相应技术手段进行重建和恢复，不危及学校整体工作的，可由信息与网络中心处理完成的安全事件。

（四）工作原则

1. 统一领导，快速反应。

学校网络安全和信息化领导小组统一领导、协调全校网络安全事件应急处置工作。

2.分级管理，各负其责。

学校各部门要按照“谁主管、谁主办、谁负责”的原则，加强对本部门所属的网络与信息的安全管理。强化部门主要领导对网络安全事件的处置职责。

3.预防为先，强化保障。

在处置网络与信息安全突发事件中，要根据实际，合情合理，依法办事，维护师生合法权益，防止事态扩大激化。要坚持提前防范，及时排查，争取早发现早报告早解决，化解风险，减少不良影响。

二、组织机构与职责

（一）在学校网络安全和信息化领导小组（以下简称“领导小组”）的领导下，网络安全和信息化领导小组办公室（以下简称“网信办”）统筹协调组织学校网络安全事件应对工作，建立健全跨部门联动处置机制，党政办公室、宣传统战部、保卫处、学生工作处、信息与网络中心、后勤处等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立学校网络安全事件应急指挥部（以下简称“指挥部”），负责特别重大网络安全事件处置的组织指挥和协调。

办事机构与职责：

网信办负责网络安全应急跨部门协调工作和指挥部的事务性工作，组织指导学校网络安全应急技术支撑队伍做好应急处置的技术支撑工作。有关部门派负责相关工作的同志为联络员，联络网信办工作。

各部门职责：

党政办公室：负责网络与信息安全事件应急处置的总体协调工作。

宣传统战部：负责网络信息内容安全事件应急处置、互联网舆情监控及网络与信息安全事件处置宣传等工作。

保卫处：负责网络与信息安全事件应急处置的安全保卫相关工作。

学生工作处：负责与学生相关的网络与信息安全事件应急处置的协调工作。

信息与网络中心：负责网络与信息安全事件应急处置的技术支持工作。

后勤处：负责网络与信息安全事件应急处置的后勤基建保障工作。

学校其他各部门按照职责和权限，负责本部门网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

三、监测与报告

（一）明确网络与信息安全监测责任

宣传统战部负责互联网舆情监测，以及学校官网、官方新媒

体平台的信息监控。

信息与网络中心负责监测网络和信息系统的通信和资源使用异常，网络和信息系统瘫痪，应用服务中断或数据篡改、丢失等情况。

保卫处负责外围设施的安保、网络从业人员审查工作，以及事件发生后协助信息与网络中心与公安机关相关部门的联系协调工作。

各部门负责本部门管理的二级网站、应用信息系统、动态性专题网站和新媒体平台的信息审核与监测。

（二）落实监测报告责任制

各部门要指定专人负责信息监测工作，要落实责任制，按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发事件和可能引发突发事件的有关信息的收集、分析判断和持续监测。

当发生网络安全事件时，按规定及时向网络安全与信息化领导小组报告，重大的网络安全事件要有日报告和态势进程报告。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。重要敏感时期要实行日报告制度，各部门按照网信办要求的报告频度及时上报监测情况。

（三）报告流程

各部门负责信息监测的人员一旦发现网络安全事件，应立即采取措施控制事态，及时进行风险评估，并向网信办报告。

对于发生一般(Ⅳ级)级别的网络安全事件，由信息与网络中心进行处理,并向网信办报告。

对于发生较大(Ⅲ级)级别的网络安全事件，由信息与网络中心和网络安全事件影响区域所属各部门协同处理,并向网信办报告。

对于发生重大(Ⅱ级)、特大(Ⅰ级)级别的网络安全事件，由网信办第一时间向学校网络安全和信息化领导小组报告，并迅速召开会议，研究确定网络安全事件的态势及应急处置方案。

四、应急处置

（一）网络安全事件处置

相关部门对有权限直接处理的校园内发生的网络安全事件，要按以下流程应急处置。

1.校园网络异常和网络恶意攻击事故处置

（1）信息与网络中心组织相关人员研判确定该攻击来源和影响范围。根据需要可以紧急切断中心网络的服务器及公网的网络连接，以保护重要数据及信息。如果攻击来自学校外，通过网络安全防护设备对此类攻击进行阻拦和过滤，组织技术人员并联系专家进行分析研究应对措施，并视情况严重程度决定是否关闭外网访问；如果攻击来自学校内，查找确定攻击源，切断攻击源相关设备网络连接。查到攻击源计算机 IP 地址后，关闭该计算机校园网络连接，通知使用者及所属部门进行处理。

（2）如果攻击源来自学校内办公电脑，电脑使用者需清除病

毒、恶意程序、木马程序或重装操作系统，运行5小时以上没有问题后提出联网申请，信息与网络中心测试无问题后再接入校园网。

（3）如果查明是学校内人员主观恶意网络攻击，网络安全应急处理领导小组视情节轻重，提交学校相关部门按学校规定进行处理，涉嫌触犯法律的移送公安机关依法处理。

2.网络系统漏洞应急处置

（1）信息与网络中心接到系统漏洞通报或定期扫描检查发现高危系统漏洞后，组织相关技术人员进行研究分析，制定解决方案。

（2）需要在核心网络设备和服务器进行封闭协议及端口、停止服务的操作，由信息与网络中心在24小时内完成处理。

（3）需要通过更新操作系统补丁的操作由信息与网络中心协助使用部门尽快完成。

（4）需要应用软件进行升级更新处理的，信息与网络中心通知使用部门联系软件厂商及时完成处理，在没有处理完成前关闭服务器外网访问。

（5）需要在办公电脑进行升级补丁的，由信息与网络中心在校园网及时发布漏洞情况和处理步骤的通知，各部门组织进行升级维护工作。

3.计算机病毒应急处置

（1）各部门信息管理员发现计算机感染病毒后，应立即将感

染病毒的办公电脑断网，在病毒彻底清除干净前禁止连接到网络，并对该设备的硬盘进行数据备份。启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。

（2）如果感染病毒的设备是服务器，并且反病毒软件无法清除该病毒，信息管理员应立即联系有关产品厂商研究解决并上报本部门负责人和信息与网络中心具体负责人。信息与网络中心负责人组织相关技术人员研究采取恢复备份等措施，并立即告知各相关部门做好相应的清查工作。

（二）分级措施

1．Ⅰ级响应措施

经网信办确认属于特别重大网络安全事件的，启动Ⅰ级响应措施。

（1）网信办成员立即到位，迅速向网络安全和信息化领导小组汇报情况，研究对策，协调部署应对工作，同时向上级部门报送信息。

（2）领导小组各成员单位进入紧急状态，成立学校网络安全事件应急指挥部，各部门按指挥部要求开展工作，采用各种手段迅速处置，控制事态防止扩大。各部门主要负责人保持通讯24小时畅通，办公室安排人员值班。网信办及时监控事态进展，从技术手段保证尽快消除影响，系统恢复正常。

（3）必要时，领导小组在第一时间向校内外公开通报处理过程及结果，引导正确舆论，平息师生情绪。

（4）各有关部门在应急处置过程中，要做好工作记录，尽可能保留有关证据。对于人为破坏的违法行为，将配合公安司法机关依法处理。

2. Ⅱ级响应措施

（1）网信办向网络安全和信息化领导小组汇报情况。领导小组迅速研究制定对策，指导各部门开展应急处置工作，必要时向上级部门报送信息。

（2）各部门按领导小组要求开展工作，采用各种手段进行处置，防止事态扩大。各部门主要负责人保持通讯畅通。网信办及时监控事态进展，从技术手段保证尽快消除影响，系统恢复正常。

（3）必要时，网信办及时通过学校新闻中心，公开通报处理过程及结果，引导正确舆论。

（4）各有关部门在应急处置过程中，要做好工作记录，尽可能保留有关证据。对于人为破坏的违法行为，将配合公安司法机关依法处理。

3. Ⅲ级响应措施

（1）网信办迅速研究制定对策，通报和协调有关各部门开展应急处置工作，及时监控事态进展，并向网络安全和信息化领导小组汇报处置情况。

（2）有关部门及时进行处置，防止事态扩大。信息与网络中心从技术上进行指导，保证尽快消除影响，系统恢复正常。

（3）必要时，网信办及时通过学校新闻中心，公开通报处理过程及结果，引导正确舆论。

（4）各有关部门在应急处置过程中，要做好工作记录，尽可能保留有关证据，并按规定追究相应责任。

4.Ⅳ级响应措施

（1）信息与网络中心及时进行处置，防止事态扩大，尽快消除影响，恢复系统正常。

（2）在应急处置过程中，要做好工作记录，尽可能保留有关证据，并按规定追究相应责任。

五、调查与评估

Ⅰ级网络安全事件由学校在上级部门的指导下，组织事件的调查处理和总结评估,部署学校各有关部门负责系统的恢复重建。Ⅱ级以下网络安全事件由网络安全和信息化领导小组领导网信办协同有关部门进行事件调查总结和系统重建。

应急处置工作结束后,网信办组织有关人员对事件发生原因、影响、责任及应急处置能力、恢复重建等问题进行全面调查评估，并出具总结报告。报告要素：事件发生时间、地点、原因、信息来源，事件类型、性质、危害及损失程度，事件发展趋势、采取处置措施等。

根据应急处置过程中暴露出的管理、协调和技术问题，改进和完善应急预案，定期实施演练，总结经验教训，整改存在隐患，进一步提升安全防护能力。

六、预防工作

（一）信息与网络中心及各部门应对校园内外所属网络硬件软件设备及接入网络的计算机设备定期进行全面检查，封堵网络漏洞，升级、更换有安全隐患的设备。各部门要建立网络安全检查台账，及时记录检查情况。

（二）加强对校园网内计算机设备的管理，加强对学校网络的使用者的网络安全教育。加强对重要网络设备的软件防护以及硬件防护，确保正常的运行软件硬件环境。

（三）加强网络值班值勤，值班人员在值班期间必须保持通讯畅通，及时掌握学校情况，全力维护正常教学、工作和生活秩序。

七、保障措施

（一）技术支持队伍

加强信息与网络中心的技术队伍建设，确保校园网公共服务符合技术标准和管理规范。通过技术培训、研讨、承担科研任务等方式不断提高技术人员的业务水平，为校园网络和信息的安全保障提供强大技术支撑。

其他部门相关人员作为网络安全事件应急预备队，可根据工作需要，安排应急工作。

信息与网络中心通过定期培训、讲座、报告等方式加强对其他部门相关信息管理人员的业务指导。

（二）信息报送机制

建立健全并落实网络安全事件信息收集、传递、报送、处理等各环节运行机制，完善信息传输渠道，确保信息报送渠道的安全畅通。

（三）经费保障

信息与网络中心应根据校园网络信息安全防护和应急处置工作的实际需要，申报网络安全设备及软件的运维、应急安全培训等专项资金，纳入年度预算，由学校给予资金保障。

（四）宣传、培训与演练

学校宣传统战部、信息与网络中心要利用适当时机，加强网络与信息安全的法律法规、新闻动态和知识技能的宣传教育，提高师生的网络与信息安全意识和应对水平。

学校各部门要将网络安全事件的应急知识列为管理干部和有关人员的培训内容，加强网络与信息安全特别是网络安全事件应急预案的培训，提高防范意识和技能。学校宣传统战部、信息与网络中心每年组织至少一次安全培训和针对不同级别安全事件的预案演练，并将演练情况报告学校网络安全和信息化领导小组。

（五）物资保障

应储备充足物资和备用设备,保障应对网络安全事件的需求。

八、附则

（一）二级预案建设

本预案由网信办制定和组织修订。学校相关职能部门须参照本预案制定本部门的网络与信息安全事件应急预案，并报网信办备案。

（二）预案解释

本预案由网络安全和信息化领导小组办公室负责解释。

（三）预案实施

本预案自下文之日开始实施。原《衡阳师范学院网络安全应急处理预案》（校党字〔2017〕28 号）同时废止。

附：衡阳师范学院网络安全事件应急处置流程图