营口理工学院文件

营理院发〔2021〕91号

关于印发《营口理工学院网络与信息安全事件应急处置工作预案（试行）》的通知

各院、部，各部门：

《营口理工学院网络与信息安全事件应急处置工作预案（试行）》经校长办公会审议、党委会审定通过，现印发给你们，请认真贯彻执行。

营口理工学院

2021年7月7日

营口理工学院网络与信息安全事件应急处置工作预案（试行）

第一章 总则

第一条 编制目的及依据

为提高营口理工学院应对网络与信息安全突发事件的能力，建立科学、有效、反应迅速的网络信息安全监测和应急工作机制，预防和减少网络与信息安全突发事件，维护学校安全稳定和教育教学工作秩序，根据《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号）、《中华人民共和国突发事件应对法》（中华人民共和国主席令第六十九号）、《国家网络安全事件应急预案》（中网办〔2017〕4号）、《教育系统网络安全事件应急预案》（教技〔2018〕8号）、《辽宁省人民政府发布突发公共事件总体应急预案》、《辽宁省教育厅办公室关于进一步做好教育系统网络与信息安全工作的通知》（辽教办发〔2016〕124号），结合我校网络安全与信息化工作实际，特制订本应急处置工作预案。

第二条 适用范围

本预案适用于我校的网络与信息安全突发事件应急处理，指导全校网络与信息安全突发事件的应对处置工作。

第三条 工作原则

（一）统一部署，快速反应

校网络与信息安全事件应急处置领导小组（以下称应急处置

领导小组）负责统一指挥、协调学校内网络与信息安全事件的应急处置工作。建立健全网络与信息安全类突发公共事件的快速反应机制，确保预警、发现、报告、指挥、处置等环节的紧密衔接，做到快速反应，正确应对，果断处置，防止事态升级和蔓延扩大。

（二）明确责任，加强协作

按照“谁主管、谁负责”的原则，加强网络与信息安全的宣传和教育，进一步提高师生的信息安全意识。各院、部，各部门（以下统称各单位）应根据本预案的标准加强技术储备、规范应急处置措施，树立常备不懈的观念。当发生安全事件后，各单位负责人要立即深入第一线，掌握情况，开展工作，控制局面。形成各单位系统联动、密切协同的处置工作格局。

（三）规范流程，加强演练

规范网络与信息安全的应急处置措施与操作流程，定期进行预案演练，确保应急预案发挥重要作用。

第二章 事件的分类与分级

第四条 事件分类

网络与信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件等。

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与信息安全事件。

第五条 事件分级

网络与信息安全突发公共事件分为三级：Ⅰ级(特别重大事件)、Ⅱ级(重大事件)、Ⅲ级(一般事件)。

1. 特别重大事件(Ⅰ级)

符合下列情形之一的，为特别重大事件(Ⅰ级):

（1）校园网内信息系统数据丢失或被窃取、篡改、假冒，或校园网全面中断，对学校安全和稳定构成特别严重威胁。

（2）出现通过校园网传播反动信息、煽动性信息、涉密信息、谣言等情况，对学校安全和稳定构成特别严重危害，引发学校大规模突发群体性事件，对学校教学、科研和生活秩序产生严重影响，教育教学活动无法正常进行，师生反映强烈并有过激行为的事件。

（3）其他对学校安全和稳定构成特别严重威胁、造成特别

严重影响的网络与信息安全事件。

2. 重大事件(II级)

符合下列情形之一且未达到特别重大网络与信息安全事件(I级)的，为重大事件(II级)：

（1）校园网内信息系统中的数据丢失或被窃取、篡改、假冒，或校园网大面积中断，对学校安全和稳定构成重大威胁。

（2）出现通过校园网传播反动信息、煽动性信息、涉密信息、谣言等情况，对学校安全和稳定构成重大危害，引发学校突发群体性事件，对学校教学、科研和生活秩序产生较大影响，师生反映强烈的事件。

（3）其他对学校安全和稳定构成重大威胁、造成重大影响的网络与信息安全事件。

3. 一般事件(III级)

除上述情形外，校园网内出现对学校安全和稳定构成一定威胁，对学校教学、科研和生活秩序产生一定影响的网络与信息安全事件。

第三章 组织机构与职责

第六条 网络与信息安全事件应急处置领导小组

组　长：王卫兵　夏立新

副组长：彭飞　孙义　原宇　霍仕武　刘红军

成　员：各院、部，各部门党政负责人

职　责

1. 贯彻落实国家、省及上级单位有关网络与信息安全的方

针政策和法律法规，组织制定学校《网络与信息安全事件应急处置工作预案》。

2. 领导统筹网络与信息安全事件应对工作，建立健全联动处置机制，启动应急预案，负责网络与信息安全事件处置的组织指挥。

3. 审定、部署、检查网络与信息安全事件的预防预警、应急处置、调查评估、信息发布、应急保障等工作，研究解决处置工作中的问题。

第七条 应急处置领导小组办公室职责

应急处置领导小组下设办公室，办公室设在信息中心。

主　任：霍仕武

副主任：张静　单红梅　张殿涛

成　员：信息中心工作人员，宣传部（融媒体中心）工作人员，安保处工作人员，各院、部，各部门网络信息安全管理员

职　责

1. 组织起草学校《网络与信息安全事件应急处置工作预案》等相关规定。

2. 承担值守应急工作，指导各单位建立网络与信息安全突发事件的预警和防控工作；接收并处理网络与信息安全应急信息报告，配合相关部门积极开展应对处置工作。

3. 负责网络与信息安全事件的预防预警、应急处置、调查评估、信息发布、应急保障、隐患排查整改等工作；组织开展网络与信息安全培训，定期组织演练；收集信息安全事件报告统计

数据、编制统计报告、汇总工作情况、撰写工作总结；负责与上级网络与信息安全应急协调机构的沟通联络工作。

第四章 信息监测与报告

第八条 明确网络与信息安全监测责任

1. 信息中心负责学校网络与信息系统的日常管理和维护，保障网络与信息系统的正常运行；保存网络运行日志；对网络与信息安全事件调查、取证；根据校应急处置领导小组的指示，隔离部分网络或相关主机。

2. 宣传部（融媒体中心）负责互联网舆情监测，以及学校官网、官方新媒体等平台的信息监控；对网络与信息安全事件调查、取证。

3. 安保处负责配合宣传部（融媒体中心）、信息中心对网络违规行为进行调查、取证，根据相关证据、事态影响及破坏程度，对违规者按照有关规定进行处理。

4. 各单位负责本单位管理的二级网站、应用信息系统、专题网站和新媒体平台的信息审核与监测。

第九条 落实监测报告责任制

各单位网络信息安全管理员负责信息监测工作，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，落实重要时期“零报告”工作。

当发生网络与信息安全突发事件时，各单位1小时内向应急处置领导小组办公室报告，重大事件（含Ⅱ级）以上网络与信息

安全突发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。

第十条 报告流程

1. 各单位负责信息监测的人员一旦发现网络与信息安全事件，应立即采取措施控制事态，及时进行风险评估、取证并向应急处置领导小组办公室报告。

2. 对于发生一般(III级)级别的网络与信息安全事件，由应急处置领导小组办公室处理，并将处理情况向应急处置领导小组报告。

3. 对于发生重大(II级)、特别重大(I级)的网络与信息安全事件，由应急处置领导小组办公室第一时间向应急处置领导小组报告，按照本预案处置。应急处置领导小组接到报告后，应迅速召开会议，研究网络与信息安全突发事件的态势及应急处置方案。

第五章 应急处置

第十一条 应急响应

1. I级响应

出现I级事件时，由校应急处置领导小组发布并启动该级预案，统一领导和指挥全校的应急处置工作。根据事态发展，先期可由校应急处置领导小组指挥组织处置，事态有进一步扩大趋势时可寻求上级有关部门、公安机关予以支持，处置情况及时报上级有关部门。

2. II级响应

出现II级事件时，由校应急处置领导小组发布并启动该级预案，迅速开展如下处置工作并将处置情况及时报上级有关部门。

（1）启动指挥体系

①校应急处置领导小组进入应急状态，履行应急处置工作职责。工作组成员保持24小时联络畅通。

②校应急处置领导小组成员单位进入应急状态，在校应急处置领导小组的统一指挥、协调下，负责本部门的应急处置工作或支援保障工作。

③应急处置领导小组成员靠前指挥、处置人员进入现场后，立即按照职责分工，决定处置措施，向全校发出相应指令。

（2）掌握事件动态，跟踪事态发展。

事发单位和成员单位及时将事态发展变化情况和处置进展情况上报校应急处置领导小组。根据事件实际影响，请示改变应急响应等级。

（3）决策部署。

校应急处置领导小组组织成员单位及时研究对策意见，进行决策部署。

（4）检查影响范围。

各信息系统的主管单位立即全面了解主管的信息系统是否受到事件的波及或影响，并将有关情况及时上报校应急处置领导小组办公室。

（5）及时通报情况。

校应对处置领导小组办公室负责汇总上述有关情况，及时报

校应急处置领导小组。

（6）处置实施

①控制事态，防止蔓延。信息中心和事发单位采取技术措施，尽快控制事态，有针对性地加强防范，防止事件蔓延至其他信息系统。对于信息内容安全事件，宣传部（融媒体中心）和事发单位采取必要的管控措施，防止网上不良信息传播扩散。

②做好处置，消除隐患。信息中心和事发单位应根据事件发生原因，有针对性地采取措施，恢复受破坏信息系统正常运行。

③及时开展调查取证。事发单位在应急发生及恢复过程中应尽量保留相关证据，对于人为破坏活动，安保处负责组织开展侦查和调查工作，并及时向校应急处置领导小组通报调查情况。

（7）信息发布。

根据校应急处置领导小组的意见，宣传部（融媒体中心）负责做好对外信息发布工作，对受影响的学校师生和公众进行解释、疏导。

3. III级响应

出现III级事件时，由事发单位发布并研究启动预案，按照本单位网络与信息安全预案开展应对处置工作，一旦发现有升级趋势时，及时将有关情况报告校应急处置领导小组办公室；应急处置领导小组办公室根据事件实际影响，请示改变应急响应等级；校应急处置领导小组办公室可根据需要或应有关单位的请求，派出工作组赴事发单位指导处置工作。

（1）跟踪报告事态发展。事发单位及时将事态发展变化情

况和处置进展情况报告校应急处置领导小组办公室。

（2）事发单位应采取技术措施，尽快控制事态，有针对性地加强防范，防止事件蔓延至其他信息系统。对于信息内容安全事件，事发单位应采取必要的管控措施，防止有害非法信息传播扩散。

（3）事发单位在应急发生及恢复过程中应尽量保留相关证据，配合安保处开展调查取证工作。

第十二条 应急处置分类

1. 有害程序事件的应急处置

（1）信息中心、事发单位应及时公布有害程序的特征、可能造成的影响、相应的处理方法，提供查杀工具下载。

（2）各单位应加强信息系统安全防范，及时更新计算机和服务器上的防病毒软件特征库，对重要数据进行备份。及时清除有害程序，恢复系统正常运行。

（3）信息中心、事发单位在必要时应隔离遭到感染情况严重的区域或主机，避免有害程序扩散造成更大影响。

2. 网络攻击事件的应急处置

（1）信息中心、事发单位应立即断开被攻击设备的网络连接，并检查信息系统遭到损害的程度。

（2）信息中心、事发单位应果断采取技术措施，切断攻击入侵途径，并立即定位攻击的来源，分析攻击方式。

（3）信息中心、事发单位应及时修复被攻击设备的安全漏洞，查明攻击所带来的损失，恢复系统正常运行。

（4）信息中心、事发单位应及时备份日志，以备调查取证。

3. 信息内容安全事件、信息破坏事件的应急处置

（1）各单位应针对校园网内可能发生的信息内容安全事件和信息破坏事件，对主办网站的信息实施动态监控，加强防范；宣传部（融媒体中心）负责对学校重要网站和新媒体平台进行信息监控。

（2）各单位对发现的有害非法信息，应在备份留查后立即删除，阻止不良信息传播。

（3）宣传部（融媒体中心）、事发单位应密切监控事件的发展动态，及时报送舆情信息，加强与网站、论坛等信息系统管理人员的联系、沟通，防止事件蔓延，防控事件升级。做好网上思想教育工作，组织、发动网络信息员、评论员进行正面引导，争取主动。

（4）事发单位在必要时应关闭相关网站，进行全面清理。

4. 设备设施故障、灾害性事件的应急处置

（1）设备使用单位应首先保障数据安全，确保数据存储与数据备份的有效性、完整性，对被破坏、丢失的数据进行修复。

（2）设备使用单位应尽快维修故障，启用备用设备，减少服务中断所带来的损失。查明故障发生原因，采取补救措施，防范类似事件的再次发生。

（3）网络运行相关事件由信息中心负责处理，包括：线路中断、路由故障、流量异常、域名系统故障等。

（4）对火灾、盗窃、破坏等紧急事件，由安保处按照国家

有关法律法规和学校有关规定处理。

（5）遇停电等紧急事件，由后勤管理处联系市供电部门，协调处理。

第十三条 网络安全事件处置程序

1. 发现情况

各单位信息员、网络信息安全管理员、网络与信息系统的维护操作人员一旦发现安全事件或接到有关单位的安全事件通报，应立即启动应急预案程序，根据实际情况第一时间采取关停、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，并立即报告本单位网络安全责任人和主要负责人。

2. 紧急处置

事发单位网络安全责任人接到报告后，应立即组织本单位人员赶赴现场进行紧急处置，同时将相关情况报告应急处置领导小组办公室，应急处置领导小组办公室应立即报告应急处置领导小组。安保处应派员至现场参与事件的处置工作，宣传部（融媒体中心）做好相关配合工作和舆情管控工作，信息中心做好事件处置的技术支持工作。公安机关、国家安全机关到现场处置时，学校各有关单位要积极予以配合、协助。

3. 事中处置

事发单位应及时、主动组织开展事中处置。安全事件的事中处置包括：及时掌握损失情况、查找分析事件原因，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，积极配合公安机关、国家安全机关开展调查。

4. 事后整改

事件结束后，事发单位应当深入分析事件原因和存在问题，提出整改报告并积极落实整改。安全事件的事后整改包括：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，继续配合公安机关、国家安全机关开展调查。

5. 情况报告

安全事件处置过程中，事发单位应及时向应急处置领导小组办公室报告处置工作进展情况。处置结束后，事发单位应提交整改报告。

第十四条 应急响应级别降低或结束

当网络与信息系统恢复正常运行或网络与信息安全事件造成的影响减弱或消除时，则根据实际情况相应降低应急响应级别，直至应急响应结束。

第六章 后期处置

第十五条 事件总结

II级以上（含II级）的网络与信息安全事件由事发单位向校应急领导小组办公室及以上工作机构进行调查处理和总结，并根据要求向上级部门报告。

第十六条 表彰和惩处

处置网络与信息安全突发事件实行问责制，对在处置工作中作出突出贡献的集体和个人，学校将给予表彰和奖励。对迟报、谎报、瞒报和漏报突发事件重要情况，或在处置工作中有其他失

职、渎职行为的，根据其性质和造成后果的严重程度，由网络与信息安全事件应急处置领导小组根据事件的涉及范围、严重程度初步认定后移交校内纪检监察部门进行查处；涉嫌触犯国家有关法律法规的，移交司法部门进行处理。

第七章 保障措施

第十七条 技术支撑队伍

学校要加强网络与信息安全技术支撑队伍建设，做好重大网络与信息安全事件的应急技术支援工作，提高应对突发网络与信息安全事件的能力。

第十八条 基础平台

学校要加强互联网信息分析检测系统等网络与信息安全应急平台建设，做到早发现、早预警、早响应，提高应急处置能力。

第十九条 技术研发

学校要加强网络与信息安全防范技术研究，为应急响应工作提供技术支撑。

第二十条 对外合作

学校要建立合作渠道，必要时和校外相关单位合作共同应对网络与信息安全突发事件。

第二十一条 经费保障

学校利用现有政策和资金渠道，积极支持网络与信息安全应急专业队伍、基础平台建设、技术研发、预案演练、宣传培训等工作。学校为网络与信息安全突发事件的应急工作提供必要的经费保障。

第八章 宣传、培训和演练

第二十二条 宣传教育

各单位要采取有效措施，加强网络与信息安全突发事件预防和处置的有关法律、法规和政策的宣传，开展网络与信息安全基本知识和技能的宣讲活动。

第二十三条 培训

各单位要将网络与信息安全事件的应急知识等列为行政管理干部和有关人员的培训内容，加强网络与信息安全应急预案的培训，提高防范意识和技能。

第二十四条 演练

各单位要根据本预案的要求，定期组织落实重大网络与信息安全突发事件的演练，模拟处置各类网络与信息安全事件，提高实战能力，检验和完善预案。

第九章 附则

第二十五条

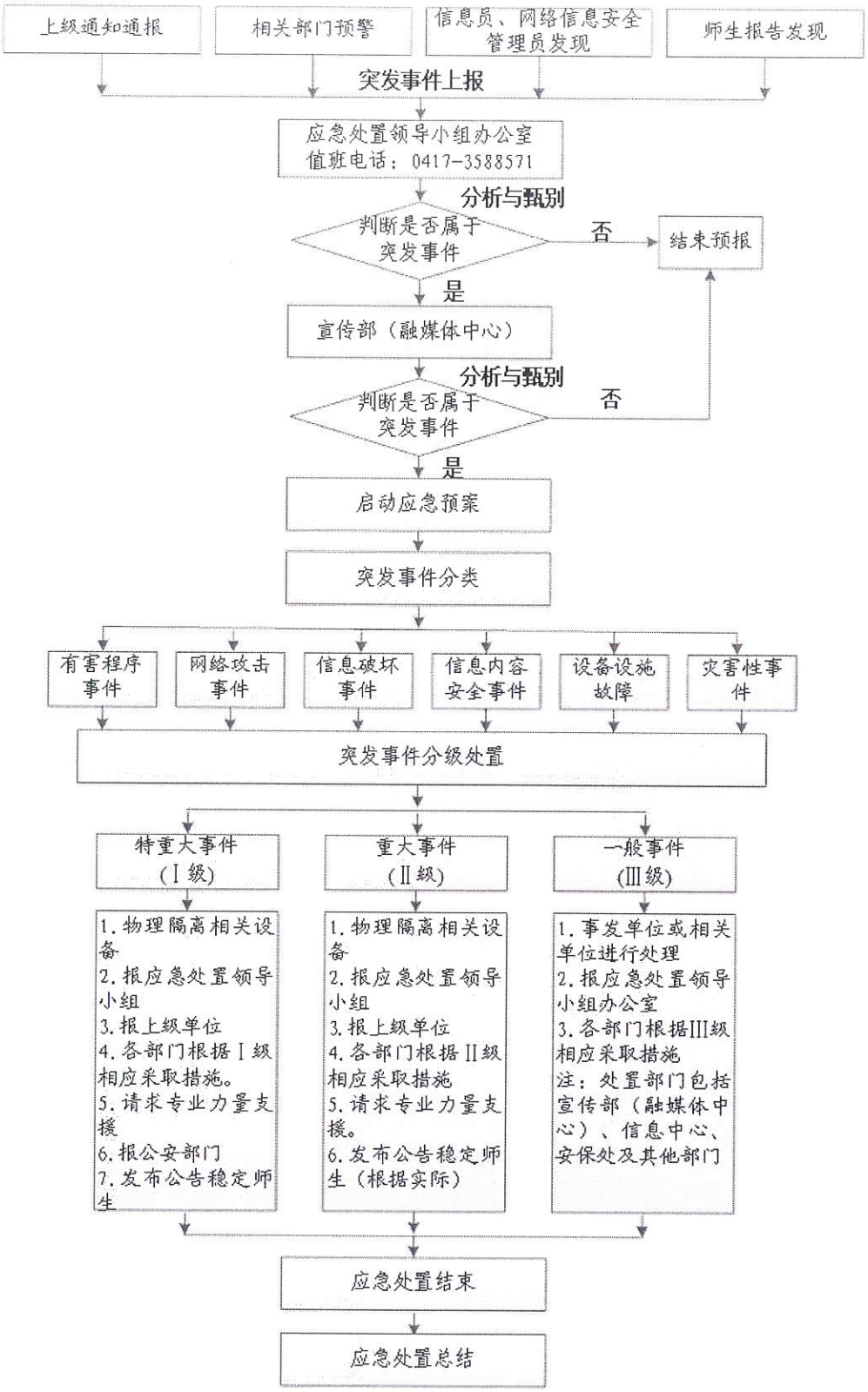
本预案由校应急处置领导小组办公室负责解释。

第二十六条

本预案自发布之日起施行。

附件：营口理工学院网络与信息安全突发事件应急处置流程图

营口理工学院网络与信息安全突发事件应急处置流程图



营口理工学院信息中心拟文

营口理工学院办公室　　2021年7月7日印发