大连科技学院文件

大科校发〔2025〕51 号

关于印发《大连科技学院网络与信息安全应急预案（修订）》的通知

校内各单位：

《大连科技学院网络与信息安全应急预案（修订）》经学校研究通过，现印发给你们，请遵照执行。

附件：大连科技学院网络与信息安全应急预案（修订）

大连科技学院

2025 年 4 月 24 日

抄送：学校党政领导。

大连科技学院　　2025 年 4 月 24 日印发

附件

大连科技学院网络与信息安全应急预案
（修订）

一、总则

（一）编制目的

为提高我中心应对突发应急事件的处理能力，确保信息系统安全运行，维护网络和系统正常运行，降低信息安全事件对我校所造成的损失和影响，特制定本预案。

（二）编制依据及原则

1.《计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际互联网管理暂行规定》等有关法规、规定，制定本预案。

2.居安思危，预防为主。实行突发事件统一管理、统一指挥、各级负责的原则。

3.统一领导，分级负责，全面规划、及时发现、快速反应、措施果断的原则。按照事件级别迅速上报相关领导和责任人。

4.快速反应，协同应对。当突发事件发生时，各级要立即按应急预案，投入应急工作；加强各个部门配合协作。形成统一指挥、反应灵敏、功能齐全、协调有序、运转高效的应急管理机制。

5.主动报告原则：当突发事件发生后，要及时报告应急预案实施情况。

二、适用范围

本预案适用于发生与本预案定义的Ⅰ—Ⅳ级网络与信息安全突发事件和可能导致Ⅰ—Ⅳ级的网络与信息安全突发事件的应对处置工作。

三、分类分级

本预案所指的网络安全突发事件，是指网络系统突然遭受不可预知外力的破坏、毁损或故障，不良信息在我单位网络平台乃至整个互联网的传播，发生对国家、社会、公众造成或者可能造成危害的紧急网络安全事件。

事件分类根据网络安全突发事件的发生过程、性质和特征，网络安全突发事件划分为网络安全突发事件和信息安全突发事件。网络安全突发事件是指自然灾害、事故灾难和人为破坏引起的网络与信息系统的损坏；信息安全突发事件是指利用信息网络进行有目的或有组织的反动宣传、煽动和歪曲事理的不良活动或违法活动。

1.自然灾害是指地震、台风、雷电、火灾、洪水等。

2.事故灾难是指电力中断、网络损坏或者是软件、硬件设备故障等。

3.人为破坏是指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖主义活动等事件。

事件分级根据网络安全突发事件的可控性、严重程度和影响范围，将网络安全突发事件分为四级：Ⅰ级（特别重大）、Ⅱ级

（重大）、III 级（较大）、IV 级（一般）。具体级别定义如果国家有关法律法规有明确规定的，按国家有关规定执行。

1.I 级（特别重大）：造成网络环境与信息系统发生大规模瘫痪，事态的发展超出区一级相关主管部门的控制能力，对国家安全、社会秩序、公共利益造成特别严重损害的突发事件。

2.II 级（重大）：造成网络环境或其它上一级部门重要网络与信息系统瘫痪，对国家安全、社会秩序、公共利益造成严重损害，需要上级政府或公安部门协助，乃至需跨地区协同处置的突发事件。

3.III 级（较大）：造成网络环境与信息系统瘫痪，对国家安全、社会秩序、公共利益造成一定损害，但只需在本区政府或区信息中心协同处置的突发事件。

4.IV 级（一般）：造成重要网络与信息系统受到一定程度的损坏，但不危害国家安全、社会秩序和公共利益，可由我主管部门处置的突发事件。

四、组织机构及职责

（一）网络安全与信息系统领导小组

组长：蔡若松

网络安全与信息系统领导小组主要职责：

1.加强领导，健全组织，强化工作职责。

2.组织开展网络安全知识的宣传教育，不断提高广大师生的防范意识和基本技能。

3.统筹做好网络安全各项物资保障，按照预案要求积极配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资的储备工作，强化管理。

4.负责协调和督促整个应急事件的处理过程，采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。

（二）数据服务中心应急小组

组长：张剑

组员：马炜林、杨广智、姜丕武、任睿、孙凤

数据服务中心应急小组主要职责：

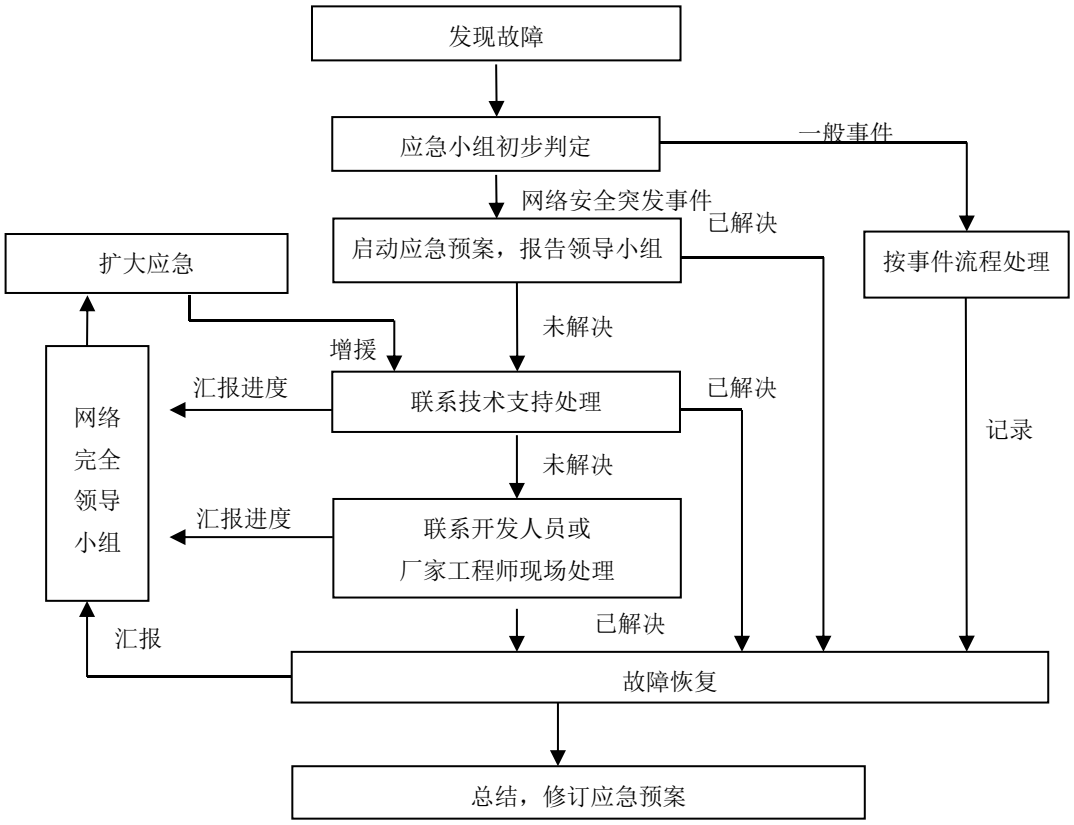
1.值班人员平时应做好应急事件的监控、预警工作，当应急事件发生后，迅速生产事件上报相关领导，并进行先期处置。

2.值班人员在发现应急事件后要进行先期处置，并迅速赶往故障现场，能联系到相关技术工程师的要第一时间要求提供技术援助。

3.对于在应急故障处理期间发生的新问题、新情况，应认真登记，及时上报。对于超出应急预案界定的应急事件，应及时汇报应急领导小组，争取尽早提出补救措施进行恢复。

五、应急响应机制

1.基本处理流程



2.值班人员平时应做好应急事件的监控工作,对于突发事件应认真分析、精准判定，负责跟踪该事件直至其结束。并做好登记工作上报领导。

3.正常情况下，要求值班人员在1小时内进行事件确认。如果属于一般事件则按照事件流程进行分派处理,如果发生重大网络安全事件,应急小组立即向网络安全与信息系统领导小组汇报同时启动《应急预案》，并严格按照《应急预案》所规定的步骤快速实施应急处置，定期汇报进度。

4.在处理过程中，如需其他部门去现场增援处理，应及时向领导汇报，协调沟通，尽快联系技术工程师或厂家技术支持赶赴现场援助处理。

六、应急方案

（一）互联网中断应急预案

1.互联网设备部署情况

应用名称	位置	设备型号	备注
出口路由器	1 排 1 柜	华为 AR6300	可通过 ssh 登录
防火墙	1 排 1 柜	齐安信 NSG7000	可通过 web 登录
核心交换机	1 排 2 柜	华为 S12700E	可通过 ssh 登录
移动互联网接入设备	2 排 1 柜	-	-
电信互联网接入设备	1 排 1 柜	-	-
教育网接入设备	2 排 1 柜	-	-

2.密切关注，准确判断链路故障位置。如故障区域属于我校范围之内，应立即启动应急预案上报相关领导，同时通知其他应急小组人员加紧监控力度。

3.检查网络硬件设备运行状态，如发现故障属硬件原因所致，尽快启用备份设备或备用端口，及时汇报领导，协调更换或维修。

4.检查链路指示灯，如果有异常，及时与对端进行确认。必要时联系接入运营商检查物理链路，如情况属实，尽快督促运营商进行抢修，并上报相关领导。

5.登录路由器、防火墙、核心交换机检查配置信息及其运行情况，如果发现配置信息有被篡改的情况，尽快启用备份数据进

行恢复。

6.坚持由简到繁，由大到小的原则逐步缩小故障范围，最后定位故障点。如果发现网络内部存在严重病毒感染或网络攻击，果断断网，报告领导，尽快通知相关责任人查杀病毒，并告知技术支持寻求补救措施。

（二）网站异常应急预案

1.网站设备部署情况

应用名称	位置	设备型号	备注
官网主页服务器	1排9柜	浪潮超融合平台	虚拟平台web登录 服务器ssh登录
官网信息服务器	1排9柜	浪潮超融合平台	虚拟平台web登录 服务器ssh登录
二级网站服务器	1排9柜	浪潮超融合平台	虚拟平台web登录 服务器ssh登录
二级网站服务器	1排9柜	DELL R730	可通过ssh登录
二级网站服务器	1排9柜	DELL R730	可通过ssh登录
二级网站服务器	1排9柜	DELL R710	可通过vnc登录
网站数据库服务器	1排6柜	H3C虚拟化平台	虚拟平台web登录 服务器ssh登录
网站服务器	1排9柜	DELL R730	可通过vnc登录

2.网站无法访问时应确定网页所属服务器，检查服务器运行

情况，并检查域名解析情况，通知网站研发人员排查具体问题。如发现故障属硬件原因所致，应尽快启用备用服务器，汇报领导，协调更换或维修。

3. 网站出现安全隐患时需要明确网站的归属部门和安全隐患等级，及时上报领导，并联系相关部门人员进行整改处理。

4. 如果发现网站被攻击、篡改、服务器系统存在严重病毒感染等重大网络安全突发情况，应立即启动应急预案同时上报领导小组，果断采取断网措施，采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。

（三）机房市电中断应急预案

机房市电中断后，应立即电话联系，询问停电原因并估计恢复时间，并上报主管部门领导。若确定停电时间超过 4 小时以上须启动应急预案，具体操作分两部分进行。

1. 市电停电后

（1）每隔一段时间观察电池剩余电量，如果发现电池电量低于 50%上报领导，关闭非核心服务器及设备。再次电话联系市电供电确认恢复时间，若恢复时间依然不确定或大于 4 小时以上；

（2）如果电池电量低于 10%并确认无需柴油发电机，需要关闭所有网络设备及服务器。

2. 市电恢复后

（1）市电恢复大约 5-10 分钟后，与电话联系确认市电供电已经稳定；

（2）检查UPS控制面板是否能正常供电，确认输入电源频率在50赫兹左右；

（3）依次复位机房空调等电器开关。

注意事项：每个开关复位时应间隔5-10秒，以免引起浪涌现象损坏配电及用电设备。

七、附则

本制度由数据服务中心负责解释，自发布之日起生效，同时废止《大连科技学院网络信息安全应急预案》（大科院发〔2016〕108）号。