沈阳职业技术学院
网络与信息安全应急预案

1.总则

1.1编制目的

为全面提升我院处置网络与信息安全突发事件能力，形成科学有效、反应迅速的应急工作机制，确保重要计算机信息系统实体安全、运行安全和数据安全，最大限度减轻网络与信息安全突发事件的危害，维护国家安全和社会稳定，保障校园网安全、可靠、稳定运行和网络信息的健康发布，制定本预案。

1.2制定依据

根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《国家网络与信息安全应急预案》、《教育部关于印发<教育系统网络安全事件应急预案>的通知》、《辽宁省网络与信息安全应急预案》、《沈阳市网络与信息安全应急预案》、《沈阳市人民政府突发公共事件总体应急预案》、《中共沈阳市委办公厅沈阳市人民政府办公厅转发市信息化工作领导小组关于加强全市信息安全保障工作实施意见的通知》等有关法律法规及文件规定，制定本预案。

1.3适用范围

本预案适用于学院主管、建设与运维的信息系统发生网络与信息安全事件的预防、检测、报告和应急处置工作，同时适用于配合各部门、二级学院网络与信息安全事件的处置工作。

1.4工作原则

坚持统一指挥、密切协同、快速反应、科学处置；坚持预防与处置相结合，以预防为主；坚持谁主管谁负责、谁运维谁负责、谁使用谁负责的原则，充分发挥各方面的力量，共同做好网络与信息安全事件的预防和处置工作。

1.4.1明确责任，分工负责

学院网络与信息安全应急工作按照“归口管理、分级响应、及时发现、及时报告、及时处理、及时控制“的要求，依法对突发事件进行防范、监测、预警、报告、响应、指挥、协调和控制。按照“谁主管谁负责，谁运维谁负责，谁使用谁负责“的原则，实行责任制和责任追究制。

1.4.2积极防御，综合防范

立足安全防护，加强预警，重点保护基础网络与信息的安全；从预防、监控、应急处理、应急保障和打击犯罪等环节，在法律、管理、技术、人才等方面采取多种措施、充分发挥各方面的作用，共同构筑网络与信息安全保障体系。

1.4.3依靠科学，平战结合

加强技术储备，规范应急处置措施与操作流程，实现网络与信息安全突发事件应急处置工作的科学化、程序化与规范化。树立常备不懈的观念，定期进行预案演练，确保应急预案切实可行。

1.4.4以人为本，快速反应

大力宣传网络与信息安全防范知识；贯彻预防为主的思想，加强对网络与信息安全隐患的日常监测，及时发现和防范重大

信息网络与信息安全突发性事件，采取有效的可控措施，及时控制事件影响范围，力争将损失降到最低程度。

1.5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、灾害性事件和其他网络安全事件等。

(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。

(7)其他安全事件是指不能归为以上分类的网络与信息安全事件。

1.6事件分级

网络与信息安全事件分为四级；I级(特别重大网络与信息安全事件)、II级(重大网络与信息安全事件)、III级(较大网络与信息安全事件)、IV级(一般网络与信息安全事件).

(1)符合下列情形之一的，为特别重大网络与信息安全事件；

①重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

③其他对国家安全、社会秩序、经济建设和公共利益构成特别严重威胁、造成特别严重影响的网络与信息安全事件。

(2)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的，为重大网络与信息安全事件；

①重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络与信息安全事件。

(3)符合下列情形之一且未达到重大网络与信息安全事件的，为较大网络与信息安全事件；

①重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络与信息安全事件。

(4)除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络与信息安全事件，为一般网络与信息安全事件。

2.组织机构及职责

2.1组织机构

根据网络与信息安全事件处置工作需要，成立沈阳职业技术学院网络安全与信息化领导小组(以下简称领导小组)，负责我院网络与信息安全突发事件应急处理工作。

领导小组成员：

组　长:王久成　肖纯凌

副组长:张学伟　夏宗光　李 静　管俊杰　梁 浩 刘钊惠

成　员:李云飞　赫　芳　邢　雨 徐国公　张广霞 杨正君

杨　海　杨昕红　董兰英　王　刚　刘瑞军　李 超

王　强　马　野　周光宇　刘　海　刘　旭　刘 洋

胡启亮　李照清　李跃中　赵　敏　王丹菲　马 力

侯宏波　陈　昊　丁　菲　于伟洋　侯伯民　齐 欣

刘　琨　王中兴 陈　伟 谭　颖

2.2组织机构职责

领导小组负责统一领导、统一谋划、统一部署全院网络安全和信息化发展,统筹制定网络安全和信息化发展战略、宏观规划 和重大政策,研究解决网络安全和信息化重要问题。

2.3日常管理机构

领导小组下设网络安全和信息化建设办公室

主　任：夏宗光　张学伟

成　员：　马 力　李云飞　邢 雨　刘瑞军　王　强

主要职能：在学院网络安全和信息化领导小组领导下,负责落实上级部门提出的网络安全和信息化方面的目标任务和各项工作,承担学院网络安全与信息化工作的总体规划部署和组织实施,对学院信息化项目进行管理；组织研究网络安全和信息化建设中涉及的关键技术,负责建立各种相关技术规范、标准和制度,开展各类相关检查工作；负责网络安全、信息安全建设,指导和推进信息系统安全等级保护和学院网站建设工作；负责调查和处置突发网络信息事件,及时上报、组织专业技术人员对所辖范围内突发网络信息事件进行应急处置,并按照相关规定作好善后工作；负责网络安全和信息化宣传普及与人员培训工作；落实学院网络安全运行、维护、管理及人员培训、配备等工作。

3.预防预警

3.1预防措施

各部门、二级学院应做好网络与信息安全事件的风险评估和隐患排查工作，避免和减少网络与信息安全事件的发生及其危害。

3.2预警响应

预警信息收到后，各部门、二级学院应依据发布的预警级别，启动相应的应急预案，组织部署所属技术力量、应急救援队伍立即响应，进入应急状态，履行承担的职责。预警发布后；

领导小组及办公室成员实行24小时值班，保持通信联络畅通，要密切关注事态发展，收集、汇总监测信息，实行每日信息报送制度，逐级上报相关信息。

应急队伍进入应急状态，确保80%应急技术人员处于待命状态；针对预警内容研究制定防范措施，指导各网络与信息系统运营使用管理单位做好安全加固和预防工作；联系社会应急力量做好应急支援准备工作。

4.应急处理预案

4.1网络应急处理预案

(1)发生通信线路中断、路由故障时，立即通知网络管理员，网络管理员应检查故障线路、进行初步故障定位并解决故障；

(2)如果通讯系统出现比较严重的问题，导致网络无法正常运转，需立即向上级主管报告，并通知相关人员，不得擅自做出决定；

(3)如果是线路故障，应立即启用备用线路；如果是设备故障，应立即启用备用设备；

(4)对有简单故障的设备，运维管理人员可以修理发生故障的设备，解决相应问题并记录；

(5)发现需要更换设备，应上报领导，经批准后马上更换相应故障设备，尽快恢复线路；

(6)如无法及时修理时，应立即通知相关厂家的维修人员，由厂家维修人员尽快解决；

(7)如发现交换机发生故障，应立即通知厂家的维修人员来修理，不能擅自修理；

(8)如发现是线路的问题，应与线路提供商联系，敦促对方尽快恢复故障线路；

(9)信息化工作处应将应急处理过程备案并报上级部门备案。

4.2信息应急处理预案

4.2.1不良信息处理预案

(1)一旦发现校园网站上出现不良信息(或者被黑客攻击修改了网页)，立刻关闭网站；

(2)备份不良信息出现的目录、备份不良信息出现时间前后一个星期内的HTTP连接日志、备份防火墙中不良信息出现时间前后一个星期内的网络连接日志；

(3)打印不良信息页面留存；

(4)完全隔离出现不良信息的目录，使其不能再被访问；

(5)删除不良信息，并清查整个网站所有内容，确保没有任何不良信息，重新开通网站服务，并测试网站运行；

(6)修改该目录名，对该目录进行安全性检测，升级安全级别，升级程序，去除不安全隐患，关闭不安全栏目，重新开放该目录的网络连接，并进行测试，正常后，重新修改该目录的上级链接；

(7)全面查对HTTP日志，防火墙网络连接日志，确定该不良信息的源IP地址；

(8)从事故发生到处理事件的整个过程，必须保持向领导小组汇报、解释此次事故的发生情况、发生原因、处理过程。

4.2.2恶意攻击应急处理预案

(1)发现有入侵迹象后，应立即通知网络管理员和安全管理员，并停止一切操作；

(2)切断受攻击计算机与网络的物理连接；

(3)由网络管理员来调查具体情况，并立即采取相应的防范措施；

(4)立即对内部网内所有的机器采取防范措施，防止入侵者用同样的手段再次入侵；

(5)由网络管理员判断损失情况，并立即上报上级主管，对损失的数据和资料立即采取相应的补救措施；

(6)受攻击的主机的一切设置都要更改，原有的用户名和口令都要更改，机器使用者的其他账户也要更改；

(7)如果受攻击的为服务器，则服务器上的所有相关信息都要立即更改；

(8)如有必要，停止使用受攻击的主机和服务器，启用备用服务器；

(9)对受攻击机器加强监控，随时注意异常情况；

(10)如果能追查到攻击者的相关信息，应对其发出警告，在警告无效的情况下，可以采取进一步的行动，包括采取法律手段。

4.2.3病毒应急处理预案

(1)发生病毒感染情况的时候，马上停止所有操作，切断网络连接，并通知系统维护人员；

(2)在感染病毒的计算机上运行杀毒软件，全面检查计算机系统，将病毒彻底清除；

(3)如果是服务器发生了病毒感染，应立即停止服务器运行的所有程序和相关服务，防止病毒进一步扩散，并通知系统维护人员；在服务器端运行杀毒软件，全面检查计算机系统，清除病毒；

(4)服务器查杀病毒的同时，所有与服务器连接的计算机都要进行病毒查杀；

(5)启动备用服务器，同时，将原有服务器与网络彻底断绝物理连接；

(6)若病毒已将系统破坏，导致系统无法恢复，应将感染病毒的计算机上的重要数据备份到其他存储介质，确保计算机内重要的数据不会丢失；

(7)备份数据也要进行病毒检测，防止病毒交叉感染；

(8)如数据无法恢复，经单位领导同意后，可与反病毒部门联系，由他们来协助恢复，需要保证数据信息不泄露，并由安全管理员做记录；如为涉密数据，按安全保密有关规定处理。

4.2.4备份应急处理预案

(1)发现数据由于某些原因丢失，首先记录故障时间和相关信息，注意保护数据现场；

(2)判断故障类型和级别；

(3)安排相关技术人员进行紧急处理；

(4)如果是硬盘错误，则需要用备用硬盘替换；如果是硬盘数据丢失，要尽力采取措施修复或复制出数据。在相关负责人员确信无法挽救数据后，才可作废弃处理；

(5)利用存储备份系统恢复离故障点最近时间的数据，尽可能降低损失；

(6)数据灾难恢复后，提交故障报告，分析并总结故障原因。

4.3消防应急处理预案

(1)当服务器机房出现火情、火灾时，现场人员应保持镇静。同时，应在最短时间内通知主管领导及网络安全和信息化建设办公室，对火情做出正确判断，及时采用一些简单可行的方法做初步处理，如到指定的位置取灭火器或采用一些应急灭火措施灭火；第一时间迅速切断总闸、关闭供电系统，将自动灭火系统转为“手动”方式；

(2)平时要注意保养和维护自动灭火系统，使之保持正常工作状态，如果夜间出现火情，机房专用的自动灭火控制器将会自动开启，实施灭火；

(3)平时机房值班人员应熟练掌握各类灭火器的使用方法，掌握灭火技能，并能做到反应迅速，操作准确，处理得当。

(4)机房发生火情90%以上是电器火灾，所以在日常巡察的基础上，主管部门应定期组织相关人员检查、维护配电系统和机房所属设备运行状态，至少一个季度进行一次全面的检修，更换有安全隐患的器件，防患于未然。

5.应急处理程序

5.1预案启动

当发生网络与信息安全事件时，由领导小组启动应急预案，负责指挥应急处理工作。

5.2现场应急处理

事件发生现场应急处理工作组尽最大可能收集事件相关信息，分辨事件类别，确定来源，保护证据，以便缩短应急响应时间。检查威胁造成的结果，评估事件带来的影响和损害。抑制事件的影响进一步扩大，限制潜在的损失与破坏。在事件被抑制之后，要进行综合分析，找出事件根源，明确相应的补救措施并彻底清除。

5.3报告和总结

认真回顾并整理发生事件的各种相关信息，尽可能地把所有情况记录到文档中，并将安全事件处理完毕后，将处理结果报领导小组。

5.4应急行动结束

根据网络与信息安全事件的处置进展情况和现场应急处理工作组意见，领导小组组织相关部门对处置情况进行综合评估，确定应急行动是否结束。

6.后期处置

6.1善后处理

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，并迅速组织实施。有关部门要提供必要的人员和技术、物资和装备以及资金等支持，并将善后处置的有关情况报领导小组。

6.2调查评估

在应急处置工作结束后，领导小组应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及损失情况，总结经验教训，写出调查评估报告，并根据有关规定，对责任人员作出处理。

7.应急保障

7.1装备保障

重要网络与信息系统在建设系统时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在网络与信息安全突发事件发生时，由应急领导小组负责统一调用。

7.2数据保障

重要信息系统均应建立异地容灾备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。各容灾备份系统应具有一定兼容性，在特殊情况下各系统间可互为备份。

7.3队伍保障

按照一专多能的要求建立网络信息安全应急保障队伍，不断加强安全应急人才培养，进一步强化安全宣传教育，努力建设一支高素质、高技术的安全核心人才和管理队伍。同时选择若干经国家有关部门资质认可的、管理规范、服务能力较强的部门作为网络与信息安全应急支援单位，提供技术支持与服务。

7.4经费保障

网络与信息安全突发事件应急处置专项经费，应列入年度预算，切实予以保障。

8.培训和演习

8.1人员培训

要充分利用各种传播媒介及有效的形式，加强网络与信息安全有关法律法规和政策的宣传，开展宣讲活动，普及信息网络安全基本知识，提高防范意识和应急处置能力。指定专人负责网络安全技术工作，并将网络与信息安全突发事件的应急管理、工作流程等列为培训内容，增强应急处置工作的组织能力。

8.2应急演习

为提高网络与信息安全突发事件应急响应水平，定期或不定期组织预案演练。通过演练，进一步明确应急响应各岗位责任，对网络与信息安全应急预案中存在的问题和不足给予及时补充和完善。

9.监督检查与奖惩

9.1预案执行监督

领导小组负责对预案实施的全过程进行监督检查，督促成员单位按本预案指定的职责采取应急措施，确保及时、到位。

发生重大网络与信息安全事件的单位应当按照规定及时如实报告事件的有关信息，不得瞒报、缓报。

应急行动结束后，领导小组对相关成员单位采取应急行动的及时性、有效性进行评估。

9.2奖惩与责任

各相关部门和单位要认真贯彻落实本预案的各项要求，领导小组将不定期组织检查，对未有效落实预案各项规定的部门、

二级学院进行通报批评；对在网络与信息安全突发事件应急处置中作出贡献的集体和个人，给予表彰奖励；对在网络与信息安全突发事件预防和应急处置中有玩忽职守、失职等行为者，依法追究责任。

10. 附则

本预案通过演习、实践检验，以及根据应急力量变更、新技术、新资源的应用和应急事件发展趋势，及时进行修订和完善。

本预案所附的网络与信息安全应急处理组织机构的组成和成员，将根据实际情况的变化随时修订。

本预案自发布之日起实施。