沈阳职业技术学院网络信息安全应急措施方案

为贯彻国家互联网信息安全管理的精神，落实在关键时期加强学院网络与信息资源的安全管理和网上信息监测的精神，提高信息化工作处对校园网和网络信息安全突发事件的应急能力，保障校园网安全、可靠、稳定运行和网络信息的健康发布，制定此网络与信息安全保障应急措施方案。

一、关键定义

(一)**关键时期**是指由学院党委办公室或院长办公室直接通过会议或文件通知信息化工作处。明确规定中心安全防范任务和具体执行时段的非常时期。

(二)**突发事件**是指由市委市政府、学院及相关部门定性的涉及网络安全和网络信息安全，影响到校园网安全、可靠、稳定运行和网络媒体健康发布的事件。

(三)**网络与信息安全保障应急措施**分为校园网络安全应急措施和网络信息安全应急措施两部分。

二、应急措施的启动程序和总体要求

(一)应急措施的启动

在关键时期应该启动网络与信息安全保障应急措施。

在网络与信息安全保障工作责任期，可以由信息化工作处主任决定启动网络与信息安全保障应急措施。

网络与信息安全保障应急措施的启动程序为：

1.经信息化工作处主任向主管领导或必要时向学院主要领导请示同

意后，确定启动应急措施。

2.由信息化工作处主任向以工作会议形式向信息化工作处内部通知启动网络与信息安全保障应急措施，明确保障工作期限、相关工作要求和人员职责。

3.由信息化工作处制定《网络与信息安全保障工作值班表》报信息化工作处办公室备案，同时上报院办公室。

4.由信息化工作处分管副主任会同网络运维人员组织对校园网设施、关键网站与设备运行和安保环境进行全面安全巡检,，对存在的安全隐患制定解决方案，并将解决方案和巡检结果上报信息化工作处办公室备案，批准后立即执行解决方案。

5.网络与信息安全保障应急措施启动日为保障工作期的起始之日，相关工作即按应急措施实施总体要求贯彻落实。信息化工作处主任和副主任即日起负起监管落实工作和人员考核责任。

(二)应急措施实施总体要求

1.实时监控要求：值班人员负有监控之责，值班期间应保证对监控对象实行一定频度（一般时期每2小时不少于1次，紧急关键时期每小时不少于1次）的设备运行状态监控或网站信息内容监控。

2.及时报告要求：值班人员负有及时报告之责，发生紧急事故或发现非正常情况应在第一时间按网络与信息安全紧急突发事件处理程序中规定的流程及时报告情况，并配合做好相应的保护现场、记录日志等工作。

3.紧急恢复要求：信息化工作处网络运维人员负有及时恢复系统正常运行和服务之责，发生紧急事故或发现非正常情况应及时配合学院调查，

组织技术人员做好事故（故障）定性、取证和系统恢复工作，原则上要求在2小时之内恢复校园网和关键网站的正常运行和服务。

4.安全备份要求：信息化工作处网络运维人员负有做好关键数据信息安全备份之责。

网络运维人员应做到：

（1）校园网主干设备和网络安全设备应做好每次更改变动后的配置备份。

（2）电子邮件服务器和关键网络应用服务器每天应做好近线数据完全备份和每隔6小时进行增量备份，备份内容保留1周。

（3）校主页服务器、门户网站主服务器每天应做好静态页面文档和动态新闻数据库的在线数据完全备份。

（4）学院主页服务器、OA 服务器和各监督保护级网站服务器每天应做好近线数据完全和每隔6小时进行增量备份，备份内容保留1周。

5.日志记录要求：值班人员负有及时做好值班日志和系统运行日志记录之责。日志记录应认真、完整、清晰。系统运行日志至少保持60天；值班日志至少保持一年。到期应及时做归档处理。

三、校园网网络安全应急措施

校园网网络安全应急措施指对校园网网络设备和服务器出现故障时采取的处理方案。

(一)在**关键时期**，信息化工作处采取24小时不间断留守值班制度，值班分成两班：

第一班时间：从上午8：00至下午5：00止。

第二班时间：从下午5：00至次日上午8：00止。

(二)留守值班人员应以高度的责任心做好以下几点工作：

1.密切监视校园网主干拓扑以及校园网主干、关键网络设备和重要服务器的工作状态，保证校园网重要设备和关键服务器的正常运行。

2.遇到下列事件发生，应根据实际情况关闭存储备份服务器、业务服务器、非主干网络设备、关键业务服务器、网络服务器和校园网重要设备。并在第一时间按照《突发事件汇报程序》及时上报情况。

（1）遇到突发性的主机房断电，并且网络主机房 UPS 电源的可持续供电时间已少于15分钟。

（2）网络主机房遇到灾难性事件（火灾、损害性雷击、破坏性不强的地震、不可抗拒的入侵和破坏等)。

（3）网络主干设备严重故障和损坏，已不能提供相关应用服务。

（4）发现严重的涉及网络信息安全的DDOS攻击和服务器入侵攻击行为。

（5）交接班时严格执行移交手续：确认网络中心所有空调和日常用电器开关处于安全状态；主机房和中心门窗安全完好；视频监控和火警装置工作正常。

（6）做好值班记录。应确保60天内的网络运行日志的完整，保证发生突发事件后能迅速有效地提供相关日志信息。

四、校园网信息安全应急措施

校园网信息安全应急措施分为校园网应用信息安全保障和学院门户网站信息安全保障两个方面。

（一）校园网应用信息安全保障

1.在**关键时期**信息化工作处采取24小时不间断留守值班制度，值班分成两班：

第一班时间：从上午8：00至下午5：00止。

第二班时间：从下午5：00至次日上午8：00止。

留守值班人员应以高度的责任心做好以下几点工作：

（1）密切监视学院主页服务器、OA 服务器、电子邮件服务器、各监督保护级服务器的运行状态，保证校园网信息发布功能和内容的正常。

（2）遇到下列事件发生，应首先关闭服务器的服务进程，然后及时解决故障（如封堵漏洞、内容恢复等），恢复正常服务，并在第一时间按照《突发事件汇报程序》及时上报情况。

a.在服务器上发现违反国家安定团结的反动信息

b.在服务器上发现有伤风化或影响社会治安的信息

c.在服务器上发现有被黑客攻击后篡改的主页内容

d.在服务器上发现有严重的网络信息安全隐患（已受到僵尸病毒或黑客的攻击；存在恶性计算机病毒、木马或蠕虫的感染等现象）

（3）遇到下列事件发生，应首先断开电子邮件服务器与校园网的连通，然后技术人员及时解决。并在第一时间按照《突发事件汇报程序》及时上报情况。

a.发现违反国家安定团结的反动的群发邮件

b.发现有伤风化或影响社会治安的群发邮件

c.在电子邮件服务器上发现有严重的网络信息安全隐患（已受到僵尸

病毒或黑客的攻击；存在恶性计算机病毒、木马或蠕虫的感染等现象）

（二）学院门户网站信息安全保障

1.在**关键时期**信息化工作处采取24小时不间断监控值守制度，监控值守分成两班：

第一班时间：从上午7：30至下午5：00止。

第二班时间：从下午5：00至晚上22：30止。

监控值守人员应以高度的责任心做好以下几点工作：

（1）每天上午8：00起开启网站所有交互栏目的对外服务；晚上22：00至次日上午8：00关闭网站所有交互栏目的对外服务。

（2）校门户网站采取各栏目负责人责任制度。由值班人员同意负责监控和联络，密切注意网上学习交流板块所发布的各类信息的安全性，每天上午8：00至晚上22：00进行实时随机观察，一旦发现有以下信息，及时删除，并在第一时间按照《突发事件汇报程序》及时上报情况。

a.发现违反国家安定团结的反动信息

b.发现有伤风化或影响社会治安的信息

c.发现有被黑客攻击后篡改的内容

（3）做好值班记录。应确保60天内的监控日志的完整，保证发生突发事件后能迅速有效地提供相关日志信息。

五、网络与信息安全紧急突发事件处理程序

(一)关键时期如遇突发事件应立刻向主管领导汇报，必要时向学院主要领导汇报。

(二)关键时期内每日16：00时前，各相关部门应将本日网络运行与信

息安全情况上报信息化工作处办公室，汇总后由信息化工作处办公室上报院党委办公室和院长办公室。

(三)值班人员或栏目负责人一旦发现网上出现反动言论或有伤风化及影响社会治安的信息，应立即采取信息屏蔽防扩散措施，保留现场取证后予以删除。对难以鉴别性质的可疑信息，应立即上报宣传部协助鉴定。

(四)若遇门户网站遭到大面积非法攻击，值班人员在第一时间按处理流程汇报的同时，可直接通知相关技术人员，进行紧急技术处置，原则上任何技术问题应在2个小时内予以解决。

六、信息化工作处联系方式

主　任：马　力　　13019370909

技术员：肖　鑫　　13704015692

孙　骑　　13252857329

王冠军　　15640160125

罗　鹏　　13478284396

信息化工作处

2021 年 5 月 18 日