大连科技学院文件

大科院发〔2016〕108号

关于印发《大连科技学院网络信息安全应急预案》的通知

院内各单位:

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

特此通知。

附件：大连科技学院网络信息安全应急预案

大连科技学院

2016年7月8日

抄送：学院党政领导。

大连科技学院　　2016年7月8日印发

附件

大连科技学院网络信息安全应急预案

为确保我校网络安全，保证各项工作稳定、高效、有序地进行，最大限度地减少损失，根据《互联网网络安全管理条例》精神，结合我校校园网工作实际，特制定本预案。

一、成立安全应急工作领导小组

1.安全应急工作领导小组成员名单

组　长：郑朝方

副组长：刘笑言 滕福泉

成　员：任　睿　杨广智　马炜林　夏　琳

2.领导小组主要职责

（1）加强领导，健全组织，强化工作职责，完善各项应急预案的制定和各项措施的落实。

（2）充分利用各种渠道进行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）认真做好网络安全各项物资保障，严格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，使之保持良好工作状态，保障校园网良好运行。

（4）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。

（5）加强值班管理，网络中心做到每天有固定人员值班，出现网络事故或问题应在最短时间内快速予以解决。

二、网站不良信息事故处理预案

1.一旦发现学校网站上出现不良信息（或者被黑客攻击修改了网页），经学校书记或院长批准后可立刻关闭网站。

2.备份不良信息出现的目录、出现时间以及近期的 HTTP 连接日志。

3.将不良信息页面予以留存处理，并加强严格的保密制度。

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.全面查对不良信息的源 IP 地址，如果来自校内，则立刻全面升级此次事件为最高紧急事件，并立刻向领导小组组长汇报，视情节严重程度领导小组可决定是否向公安机关报案。

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组长汇报、解释此次事故的发生情况、发生原因、处理过程等。

三、网络恶意攻击事故处理预案

1.发现出现网络恶意攻击，立刻确定该攻击来自校内还是校外；受攻击的设备有哪些；影响范围有多大。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断校园网的服务器及公网的网络连接，以保护重要数据及信息;

2.如果攻击来自校外，立刻从防火墙中查出对方 IP 地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

3.如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台电脑，出自哪位教师或学生。接着立刻赶到现场，关闭该计算机网络连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。经学校领导批准可暂时扣留该电脑。

4. 重新启动该电脑所连接的网络设备，直至完全恢复网络通信。

5. 对该电脑进行分析，清除所有病毒、恶意程序、木马程序以及垃圾文件，测试运行该电脑 5 小时以上，并同时进行监控，无问题后归还该电脑。

6. 从事故发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因及处理过程。

7、按预案落实各项物资准备。

四、其他事项

1. 在应急行动中，学校各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。

2. 因电力以及其他自然灾害等不可控因素造成的网络瘫痪，应在恢复电力以及相关设备正常运行的情况下，在最短的时间内恢复校园网，以保证学校各项安全稳定。

3. 学校各部门应根据本预案，结合本部门实际情况，认真制定本部门的应急预案，并切实落实各项组织措施。