南京中医药大学文件

南中医大信字〔2021〕3号

关于印发《南京中医药大学网络安全监测预警与威胁处置工作流程》的通知

各学院、各部门、各单位：

为进一步加强我校网络安全工作，规范网络安全监测预警及威胁处置工作流程，根据国家相关规定，结合我校实际，特制定《南京中医药大学网络安全监测预警与威胁处置工作流程》，现印发给你们，请遵照执行。

附件：南京中医药大学网络安全监测预警与威胁处置工作流程

南京中医药大学

2021年5月11日

附件

南京中医药大学网络安全监测预警与威胁处置工作流程

为了规范我校网络安全威胁预警、通报和威胁处置工作，提高网络安全威胁的响应处置效率，根据教育系统网络安全监测预警通报工作要求和《江苏省教育系统网络安全事件应急预案》相关规定，制定本工作流程。

一、我校常见网络安全威胁分类

（一）网络安全漏洞

网络安全漏洞主要有信息系统（网站）及相关的操作系统、数据库、中间件等自身存在的安全缺陷，其中 SQL 注入、Struts 2、远程代码执行、任意文件上传、跨站请求伪造等被定为高危漏洞。以及弱口令、默认口令、信息泄露等管理类漏洞。

（二）网络安全隐患

网络安全隐患主要有僵尸网站（系统）、沉睡邮箱等。

（三）其他威胁

其他威胁主要包括计算机病毒、蠕虫、僵尸木马、网络攻击等。

二、网络安全漏洞的监测与处置

（一）网络安全漏洞监测

网络管理与信息化办公室负责综合利用各种网络安全设备，对校园网数据中心服务器和 Web 资产定期进行安全漏洞扫描和分析验证，同时跟踪江苏省教育网络和信息安全通报平台有关我校网络安全漏洞的通报，及时指导、督促涉事单位处置。

（二）网络安全漏洞处置流程

1. 通报漏洞

网络管理与信息化办公室一旦自查到漏洞或接到上级部门通报，第一时间联系涉事系统管理员，通报漏洞信息，要求 6 小时内反馈修复情况、成功完成修复。如 6 小时内未能修复成功，且开放外网访问的信息系统（网站），第一时间暂停其校外访问。

2. 修复处置

涉事系统管理员接到通知后进行紧急修复，必要情况下可联系网络管理与信息化办公室提供安全技术服务协助修复。

3. 报告修复情况

涉事单位 3 日内向网络管理与信息化办公室报告安全漏洞处置修复情况（附件 1），完成修复的，经检测确认后关闭本次任务，暂停校外访问的系统，恢复其正常访问。未完成修复的要说明原因和进展情况。

4. 发督办函

涉事单位3日内未报告修复情况的，网络管理与信息化办公室将向涉事系统建管单位发行政督办函，要求5日内完成修复。

5. 处置修复

建管单位主管领导接到督办函后，要高度重视，协调相关人员加紧修复，5日内完成漏洞修复并提交处置报告，网络管理与信息化办公室经复测确认后关闭本次任务。逾期未完成修复的，将暂停该系统（网站）所有网络服务，直至完成修复。

三、网络安全隐患处置

网络管理与信息化办公室负责运用技术手段对校园Web资产的运行状态进行实时监测，结合Web资产年检，定期组织僵尸网站（系统）、沉睡邮箱的排查和清理工作，各单位应予以积极配合。

四、其他网络安全威胁处置

网络管理与信息化办公室负责加强与国家网络安全机构、上级主管部门及相关网络安全企业的联系，主动收集常用软件漏洞信息和病毒、僵尸木马、网络攻击等威胁信息，及时通过OA或学校网络安全工作管理平台向校内发布预警通告，指导各单位和师生做好处置和防范工作。

五、工作要求

各单位要重视和加强信息系统（网站）日常运维和安全管理，及时做好系统及相关软件升级、打补丁以及数据

备份等安全加固工作，严格杜绝系统弱口令策略、管理员弱口令，做好预防工作，避免和减少网络安全事件发生。

一旦被通报安全隐患、安全漏洞，涉事单位要紧急组织相关人员快速处理，按本办法要求的时限完成修复并反馈修复情况，若因此导致我校被教育部网络安全责任制考核扣分或酿成网络安全事件，将追究该单位主要负责人、分管领导、网管员等相关人员的责任。

六、附则

本流程从发布之日起施行，由网络管理与信息化办公室管理处负责解释。

附件 1：南京中医药大学网络安全漏洞处置报告

附件 1

南京中医药大学网络安全漏洞处置报告

单位名称			
网站/系统名称			
域名			
IP 地址			
联系人姓名		联系人电话	
漏洞类型			
修复情况	□已完成　　□未完成 未完成修复的说明情况、原因以及预计完成时间。		
系统建管单位审核	单位主管负责人签字（公章）： 年 月 日		
网络管理与信息化办公室审核			