

南京工业大学文件

南工校信〔2022〕6号

关于印发《南京工业大学网络安全 监测预警和信息通报实施办法》的通知

各单位、各部门：

为进一步加强网络安全监测预警和信息通报工作，有效防范网络安全事件的发生，维护学校网络安全，经研究制定《南京工业大学网络安全监测预警和信息通报实施办法》，现予以印发，请遵照执行。

特此通知。



2022年12月13日

南京工业大学网络安全 监测预警和信息通报实施办法

第一章 总 则

第一条 为切实加强网络安全保障工作，有效防范网络安全事件的发生，维护学校网络安全，依据《中华人民共和国网络安全法》和上级有关工作要求，结合学校实际，制定本办法。

第二条 网络安全监测预警和信息通报工作遵循“及时发现、科学认定、有效处置”的原则，通过建立监测预警和信息通报机制，对风险进行预警，做到“早发现、早报告、早处置”，减少和防止不良信息的传播，确保信息网络的畅通和安全。

第三条 本办法中所包含的监测预警和信息通报工作内容主要指信息技术安全事件和安全隐患，不包含信息内容安全事件及网络舆情监测预警。

第二章 监测机制

第四条 信息管理中心通过网络监测设备对全校网络环境进行实时监测，监测内容主要包含通信线路状态、网络设备运行状况、网络流量和网络基础服务等，发现异常情况，及时处理。

第五条 信息管理中心通过安全设备对全校信息系统和网站进行安全监测及防护，监测内容主要包含恶意 IP 地址、恶意电子邮件、恶意程序、应用服务器高危漏洞和弱密码等各类网络

安全隐患，对监测中发现的问题及时通报相关单位处置。

第六条 各单位按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，对本单位信息系统和网站开展日常监测，包括但不限于以下方式：

（一）定期检查信息系统和网站有无异常情况；

（二）加强账号、密码管理，杜绝弱密码，重要业务系统要定期更换管理账号密码；

（三）定期对重要数据进行备份；

（四）信息系统和网站发生变更时及时报告信息中心，对新变更的部分及时跟踪；

（五）定期对服务器操作系统、杀毒软件进行升级；

（六）确保信息先审核后发布、敏感信息不上网。

第七条 信息系统和网站的监测从系统上线开始，至系统服务下线后结束。

第三章 预警机制

第八条 网络安全预警信息来源主要包括教育部、网信机关、公安机关、省教育厅等上级部门，以及国内外计算机安全组织发布的网络安全威胁信息。

第九条 信息中心负责对各类突发网络安全事件和可能引起突发事件的有关信息进行收集、分析、判断和持续监测，出现异常情况时，及时发布最新网络安全威胁信息，推荐解决方案。

第四章 信息通报机制

第十条 信息管理中心通过校内信息网每月发布《南京工业大学网络与信息系统安全月报》。

第十一条 各单位党政主要负责人为本单位网络安全责任人。分管信息化负责人和信息化联络员负责信息通报的上传与下达。

第十二条 单位主要负责人、分管信息化负责人和信息化联络员若发生变更，应在 30 日内将变更后的人员信息报送至信息管理中心备案。

第十三条 信息通报实行 24 小时联络机制。各单位信息化联络员应保持通讯畅通，信息管理中心在发现网络信息系统存在安全隐患或发生网络安全事件后，及时通知事发单位，并协助事发单位确定事件规模和影响范围，按照《南京工业大学校园网络与信息安全应急处置预案》要求，根据事态的严重程度启动分级响应机制。

第十四条 各单位信息化联络员在收到通报后，应立即联系本单位网络信息系统责任人对事件进行处置，并及时反馈处置结果。

第十五条 收到信息通报的单位应当及时且如实地报告事件的有关信息，积极完成处置整改工作。对出现瞒报、缓报、漏报和整改不力等情况的，学校将按照《南京工业大学网络安全责任制实施细则》追究相关人员责任。

第十六条 本办法自发布之日起施行,由信息管理中心负责解释。