南京中医药大学文件

南中医大信字〔2021〕2号

关于印发《南京中医药大学网络安全事件应急预案》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，规范网络安全事件应急处置工作流程，根据国家相关规定，结合我校实际，特修定《南京中医药大学网络安全事件应急预案》，现印发给你们，请遵照执行。

原《南京中医药大学校园网络突发事件应急预案》（南中大委办〔2013〕3号）从即日起废止。

附件：南京中医药大学网络安全事件应急预案

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事件应急预案

第一章 总则

第一条 根据网络信息安全管理的相关规定,切实做好学校网络与信息安全事件应急工作，网络管理与信息化办公室制定关于网络信息安全突发事件应急预案。

第二章 领导机构

第二条 网络安全和信息化领导小组负责全校网络信息安全应急预案的领导、决策和重大工作部署。由网络管理与信息化办公室负责制订具体的网络信息安全应急预案。

第三条 网络管理与信息化办公室承担信息安全专项应急的日常工作，负责信息安全突发事件日常监测与预警，网络安全和信息化领导小组组织拟订应对信息安全突发事件的工作规划和应急预案，汇总有关信息安全突发事件的各种重要信息，进行综合分析，并提出建议。定期对学校信息安全工作进行专门检查，并对出现的问题进行通报和整改。

第三章 突然事件应急响应

第四条 网络管理与信息化办公室按照网络信息安全突发事件发生的特点、规律，梳理出突发网络安全事件的类型和紧急处置方式。

第五条 网络管理人员网站、网页负责随时密切监视信息内容。发现在网上出现非法信息时，信息安全负责人立刻向上级领导通报情况；情况紧急的，应先及时采取删除等处理措施，不能立即处理的可先行关闭，或物理切断，再按程序报告。

第六条 信息安全相关负责人应在接到通知后立即赶到现场，作好必要记录，清理非法信息，妥善保存有关记录及日志或审计记录，强化安全防范措施，并将网站网页重新投入使用。

第七条 追查非法信息来源，并将有关情况向网络管理与信息化办公室汇报。情况严重的，要向公安部门报案。

第八条 当网络管理人员发现网页内容被篡改、重要数据丢失或截取，或通过入侵检测系统发现有黑客正在进行攻击时，应立即向信息安全负责人通报情况。

第九条 信息安全相关负责人应在接到通知后立即赶到现场紧急处理，并首先将被攻击的服务器等设备从网络中隔离出来，保护现场，并将有关情况向网络管理与信息化办公室汇报。

第十条 对现场进行分析，并写出分析报告存档，必要时上报主管部门。

第十一条 恢复与重建被攻击或破坏的系统。

第十二条 当发现有计算机被感染上病毒后，或接到大规模病毒爆发通知后应立即向信息安全负责人报告，信息安全相关负责人员

在接到通报后立即赶到现场紧急指挥处置。将中毒计算机从网络上隔离开来，对其他网络设备做好保护措施，并对中毒设备的硬盘做好进行数据备份。

第十三条 启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。如果现行反病毒软件无法清除该病毒，应立即向网络管理与信息化办公室报告，并迅速联系有关产品商研究解决。

第十四条 如果感染病毒的设备是主服务器，经网络管理与信息化办公室同意，应立即告知各相关单位做好相应的清查工作。

第十五条 重要的软件系统平时必须存有备份，与软件系统相对应的数据必须按本单位容灾备份规定的间隔按时进行备份，并将它们保存于安全处。

第十六条 一旦软件遭到破坏性攻击，应立即向信息安全负责人报告，并将该系统停止运行。

第十七条 检查信息系统的日志等资料，确定攻击来源，并将有关情况向网络管理与信息化办公室汇报，再恢复软件系统和数据。

第十八条 性质恶劣及情况严重的，要向公安部门报案。

第四章 应急响应机制

第十九条 在发生重大信息安全突发事件时，第一时间信息安全管理人员要及时收集、上报和通报突发事件的有关情况，向负责人汇报。

第二十条 及时分析识别网络与信息系统正常运行的主要威胁,确定应急措施的先后顺序，做出相应的决定，确保安全策略的制定与执行。同时逐级向上级相关部门汇报，相关部门共同协商，做好突发事件的处置工作。

第五章 应急预案演练

第二十一条 做好应急预案演练工作,有利于强化突发事件应急处置能力。适时进行应急预案演练，切实提高信息网络安全公共防范意识以及基础网络和重要信息系统的信息安全综合保障水平。

第二十二条 加强对信息安全隐患的日常监测,发现和防范重大信息安全突发性事件，及时采取有效的可控措施，迅速控制事件影响范围，力争将损失降到最低程度。

第六章 附则

第二十三条 本规定自发布之日起实行。