南京财经大学

南财大信字〔2020〕1号

关于印发《南京财经大学网络信息安全管理办法（试行）》的通知

本校各单位：

《南京财经大学网络信息安全管理办法（试行）》已经学校研究通过，现予以印发，请认真贯彻执行。

附件：南京财经大学网络安全事件应急流程图

南京财经大学

2020年12月1日

南京财经大学
网络信息安全管理办法（试行）

第一章　总则

第一条 为保障南京财经大学校园网络和信息系统的安全稳定、促进学校信息化健康发展，根据国家相关法律法规并结合我校实际情况，制定本办法。

第二条 网络信息安全是指网络基础设施、网站、信息系统及数据内容等受到保护，保证网络、信息及内容的安全性、完整性、可用性、可控性。

第三条 网络信息安全管理的基本原则是“谁主管谁负责、谁运行谁负责、谁使用谁负责”，明确责任、突出重点、保障安全。

第四条 网络信息安全管理的总体方针是以《中华人民共和国网络安全法》和国家标准《信息系统安全等级保护基本要求》为指导，预防为主、综合防范。

第五条 网络信息安全管理的目标是建立健全网络信息安全保障体系，提高安全防护能力，确保学校网络信息安全工作规范、有序开展，保障学校信息化可持续发展。

第六条 我校网络安全事件应急预案依据《国家网络安全事件应急预案》《教育系统网络安全事件应急预案》《江苏省教育系统

网络安全事件应急预案》等文件，结合我校实际情况制定。目标是健全完善校内网络安全事件应急工作机制，提升学校应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害。

第二章　组织架构

第七条 学校网络安全和信息化领导小组（简称网信领导小组）负责制定学校网络信息安全相关政策，研究处理重大网络信息安全事件，定期召开网络信息安全工作会议，统筹指导学校网络信息安全建设。

第八条 网信领导小组办公室（简称网信办）设在信息化建设管理处，网信办主任由信息化建设管理处负责人担任，副主任分别由保卫处负责人和党委宣传部分管负责人担任。网信办负责网信领导小组的各项决策落实，负责学校网络信息安全的日常工作，负责开展各部门网络信息管理员培训。

第九条 学校各部门负责本部门网站及应用系统的建设、管理及安全运维。各部门主要负责人是本部门网络信息安全工作第一责任人，各部门的网络信息管理员负责本部门网络信息安全具体工作。

第三章　网络信息安全建设

第十条 各部门在开展网站和信息系统建设时，须将相应的网络信息安全经费编入预算,用于该网站和信息系统的安全建设、运维、测评和整改。

第十一条 各部门须明确网站和信息系统是否对校外开放，若对外开放，须满足国家标准《信息系统安全等级保护基本要求》规定的二级（或以上）安全等级要求，各部门明确其网络和信息安全需求，提供安全策略，由网信办进行防火墙设置。

第十二条 各部门网站或信息系统上线前，须开展安全自查工作，提供安全自查报告。

第十三条 网信办采用专业技术手段对网站和信息系统进行安全检测。检测未通过的须进行安全整改，直至通过检测后网站和信息系统方可上线运行。

第四章　监测预警机制

第十四条 安全监测。网信办负责实施全校范围内网络与系统（网站）安全监测；各部门负责实施本部门网络与系统（网站）安全监测。一旦发现网络安全威胁应立即报送预警信息至网信办。预警信息包括：发布单位、事件源、相关责任人、起始时间、可能影响范围、预警发布人、所需协助、已采取措施等。

第十五条 安全预警。网信办按照相关规定或上级部门要求向各部门发布网络安全监测预警信息。各部门接收到预警信息后，应及时响应，做好相应处置和防范工作。

第十六条 安全巡检。各部门应定期对本部门的网站和信息系统开展安全巡检，填写巡检记录。对校外开放的网站和信息系统，每周至少巡检一次；对校内开放的网站和信息系统，每月至

少巡检一次。各部门应加强对可能引发网络信息安全事件相关信息的收集、分析与持续监测，实现“早发现、早报告、早处置”。

第十七条 漏洞修补。各部门应及时对网站和信息系统漏洞进行修补，包括主机系统漏洞、WEB 应用漏洞、中间件漏洞、数据库漏洞等。

第十八条 复查整改。网信办定期对全校网站和信息系统开展安全复查，复查不合格的网站或信息系统，视安全漏洞级别暂停其网络访问,同时通知责任部门限期 60 小时整改并提交整改报告。安全复查合格后，方可恢复该网站或信息系统的网络访问。

第十九条 重点值守。特殊时期，各部门须加强网站及信息系统的安全监管工作，安排专人值守，加强安全巡检，做好安全整改。

第五章　网络安全事件应急预案

第二十条 网络安全事件是指由于人为破坏、软硬件缺陷或故障、自然灾害等，对校园网络和系统（网站）中的数据造成危害，对学校甚至社会造成负面影响的事件。结合学校实际情况，本预案将校内网络安全事件分为紧急事件和普通事件。分级依据如下：

1．紧急事件

（1）校外可访问的页面发生被篡改或被替换成非法信息的事件，尤其是发生在主页、新闻网站、招生信息网等访问量高的

系统或其它学校网站的事件。

（2）影响学校系统正常运转的攻击事件，如信息门户、教务系统、财务系统、学工系统、办公自动化系统等遭受攻击的事件。

（3）可能造成广大师生的个人隐私信息被窃取、被篡改、丢失的漏洞。

（4）可能对社会公共安全、对学校正常秩序造成危害和不良影响的事件和漏洞。

2．普通事件

（1）校内开放的系统或网站页面发生无害篡改或包含隐藏漏洞。

（2）影响不大的攻击事件或可能造成中低隐患的漏洞。

（3）其他不构成公共危害或社会不良影响的安全事件或漏洞。

第二十一条 网信领导小组在应急工作中负责：

1．统筹指导、指挥学校网络安全应急体系建设；

2．决定紧急网络安全事件应急启动，组织成立网络安全事件应急小组；

3．统筹指导、指挥学校网络安全事件应急工作。

第二十二条 网信办在应急工作中负责：

1．编制学校网络安全相关制度和应急预案；

2．统筹组织学校的网络安全监测工作，接收处理网络安全通报，保障校内网络与系统（网站）正常运行；

3．建立健全各部门联动机制，指导、督促各部门完成本部门网络安全事件应急机制建设，并完成检查工作；

4．组织开展校级应急演练，并在应急演练中向各部门提供技术咨询与支持；

5．在网络安全应急处置工作中选派应急技术支撑人员，提供技术支持与保障，并及时向网信领导小组报告情况；

6．每季度向网信领导小组汇报学校网络安全自查工作情况，包括网络与系统（网站）安全形势分析预测、网络与系统（网站）异常或瘫痪、应用服务中断或数据篡改、丢失等情况。

第二十三条 学校各部门在应急处置工作中负责：

1．本部门网站及应用系统的网络安全事件预防、监测、报告及应急处置工作；

2．建立健全本部门网络安全事件应急机制，制定本部门网络安全事件应急预案，定期进行网络安全事件应急演练；

3．明确本部门网络信息安全应急负责人，应急负责人负责本部门网络安全应急具体工作，并负责与网信办对接。若应急负责人员发生变动，需及时报送网信办备案；

4．积极支持配合网信领导小组及网信办进行应急处置工作。

第二十四条 各部门应在网信领导小组统筹协调下，快速反应、密切协同、科学处置，切实落实网络安全应急工作，充分发挥各部门力量，共同做好网络安全事件的预防和处置。

第二十五条 网络安全事件应急流程如下，流程图见附件：

1．网络安全事件发生后，事发部门应及时启动预案，保留相关证据，并通知网信办。网信办接到安全事件通报，立即与事发部门协调沟通，结合技术手段，开展问题定位和溯源追踪，获取网络攻击、网络入侵或网络病毒等证据。事发部门应积极配合网信办以及上级网信部门和公安机关开展调查取证工作。

2．网信办核实事件类别，发起处理流程。

3．若事件为紧急事件，网信办第一时间向分管信息化工作校领导汇报，同时通报责任部门相关情况及事件证据，并关闭相关网站或信息系统的访问权限，以降低不良影响。经分析研判，初判为较大及以上网络安全事件的，立即报告省教育网络安全应急办；对于人为破坏活动，同时报当地网信部门和公安机关。若事件为普通事件，则此环节略过。

4．网信办指导分析事件原因，并向责任部门提供整改建议。

5．责任部门对网站或信息系统进行安全修复，并提交整改报告。

6．网信办对修复后的网站或信息系统进行安全复查，复查通过后恢复其访问权限。

第六章 应急演练

第二十六条 网信办牵头各部门定期组织校级网络安全应急演练，制定详细演练方案，明确演练目标、参加演练的系统、涉及的形式、层次和范围，设定灾难情况、演练流程、操作内容、业务验证测试、应急资源、职责分工、进度安排、演练的风险及其应对措施，确保应急预案内容切实可行。

第二十七条 针对病毒传播、网络入侵、信息篡改、不良信息传播以及例外情况分别制定应急策略。

第二十八条 加强演练工作风险管理，谨慎开展应急演练。确保演练前组织、人员、资源到位。严格控制应急演练引起的系统变更风险，避免因演练导致服务中断、各项资源不可恢复。认真评估演练本身可能带来的风险和对业务的影响，制定完善的保障措施和应急回退方案。

第二十九条 记录演练开展的全过程和发现的问题，对演练的组织、过程、效果进行评估，编写应急演练总结报告。根据演练结果完善应急体系，维护更新防护设施。

第七章 附则

第三十条 涉密网络信息系统的运行安全保护工作不适用本管理办法。

第三十一条 本管理办法自颁布之日起施行,由网信办负责解释。

附件

南京财经大学网络安全事件应急流程图

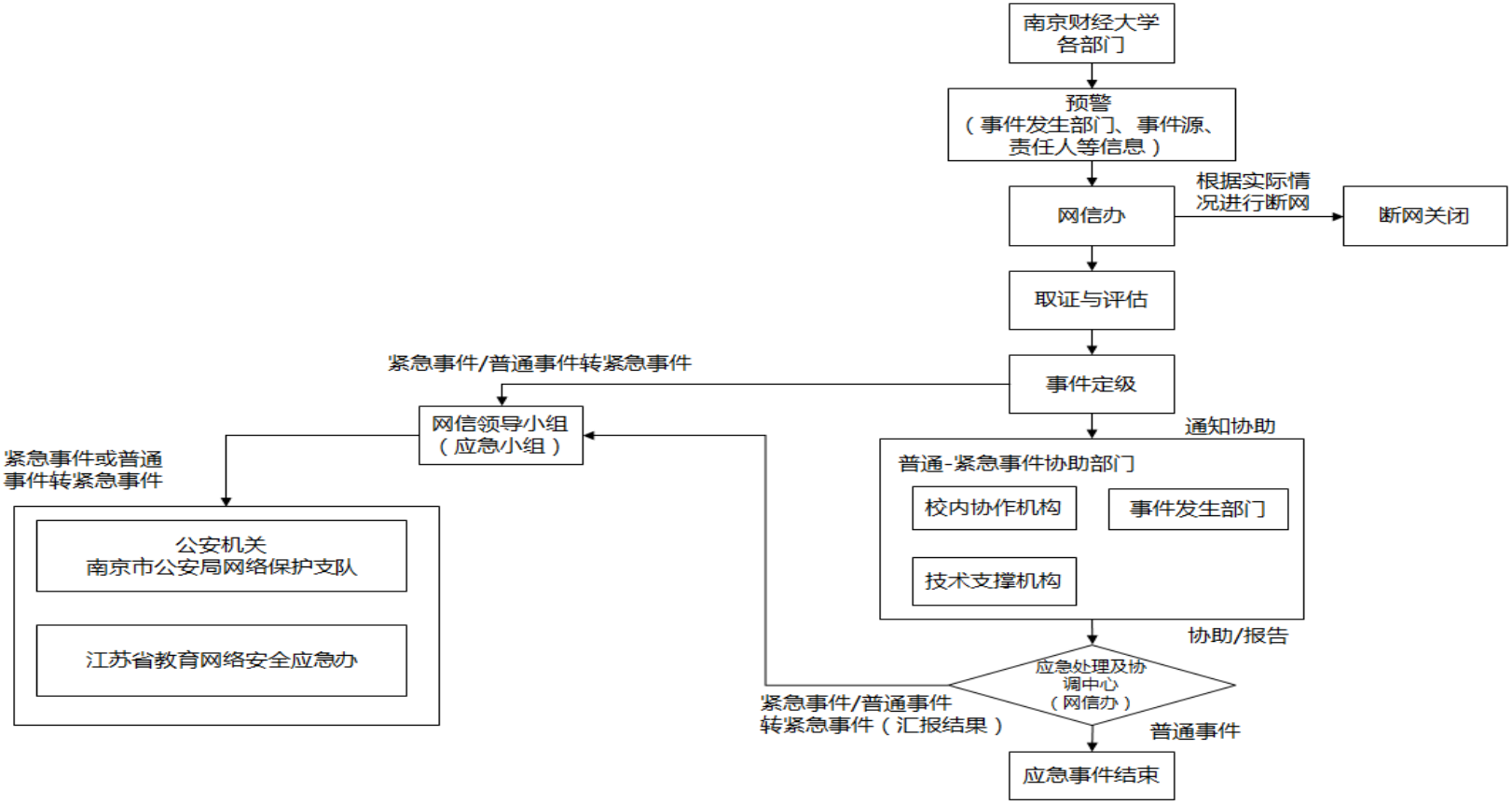

图 1南京财经大学网络安全事件应急流程图

南京财经大学校长办公室　　2020年12月7日印