东 南 大 学 文 件

校发〔2019〕313 号

关于印发《东南大学网络安全事件应急预案（暂行）》的通知

各校区，各院、系、所，各处、室、直属单位，各学术业务单位:

根据《中华人民共和国网络安全法》等法律法规以及《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，特制定本预案，现予印发，请遵照执行。

东南大学

2019 年 12 月 9 日

（主动公开）

东南大学网络安全事件应急预案（暂行）

第一章 总 则

第一条 为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，确保学校校园网络及信息系统的安全稳定，根据《中华人民共和国网络安全法》等法律法规以及《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，特制定本预案。

第二条 参照《国家网络安全事件应急预案》相关规定，本预案所指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）或系统中的数据造成危害，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特别重大网络安全事件（Ⅰ级）、重大网络安全事件（Ⅱ级）、较大网络安全事件（Ⅲ级）、一般网络安全事件（Ⅳ级）四级。分级依据如下:

1. 特别重大网络安全事件（Ⅰ级）:

（1）因发生网络攻击、病毒感染或由于软硬件故障、灾害性事件导致学校大规模网络与系统（网站）瘫痪;

（2）校内重要基础设施（如：网站群、信息门户、移动端门户等）、校内核心业务系统或网站（如：学校主页、一卡通系统等）遭受特别严重损失，丧失业务处理能力；

（3）校内重要基础设施、校内核心业务系统（网站）的重要敏感信息或关键数据丢失，或被窃取、篡改、假冒，对学校安全稳定和正常秩序造成特别严重影响；

（4）其他对学校安全稳定和正常秩序造成特别严重影响的网络安全事件。

因上述网络安全事件发生，致使事态发展超出学校控制能力。

2. 重大网络安全事件（II级）：

（1）因发生网络攻击、病毒感染或由于软硬件故障、灾害性事件导致学校区域性网络与系统（网站）瘫痪；

（2）校内重要基础设施（如：网站群、信息门户、移动端门户等）、校内核心业务系统或网站（如：学校主页、一卡通系统等）遭受严重损失，业务处理能力受到严重影响；

（3）校内重要基础设施、校内核心业务系统（网站）的重要敏感信息或关键数据丢失，或被窃取、篡改、假冒，对学校安全稳定和正常秩序造成严重影响；

（4）上级主管或监管部门要求立即整改的网络安全事件；

（5）其他对学校安全稳定和正常秩序造成严重影响的网络安全事件。

因上述网络安全事件发生，致使事态发展超出网络与信息中心处置能力，需协同相关部门进行处置。

3. 较大网络安全事件（III级）:

（1）因发生网络攻击、病毒感染或由于软硬件故障、灾害性事件导致学校小范围网络与系统（网站）瘫痪;

（2）重要业务系统（如校内二级单位重要系统）或网站（如校内二级单位主页）遭受较大损失，造成系统中断，明显影响系统效率，业务处理能力受到影响;

（3）重要业务系统（网站）的数据丢失，或被窃取、篡改、假冒，对学校安全稳定和正常秩序造成较严重影响;

（4）其他对学校正常工作造成不利影响的网络安全事件。

4. 一般网络安全事件（Ⅳ级）:

除上述情况外，其他对学校网络或系统（网站）造成一定影响的网络安全事件，包括但不限于校内个人计算机感染病毒、三级单位信息系统（网站）发生软硬件故障等，定义为一般网络安全事件。

第三条 根据“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，坚持网络安全和信息化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，充分发挥各单位力量共同做好网络安全事件的预防和处置。

第四条 本预案是东南大学网络安全事件的专项预案，适用于东南大学发生、或可能发生网络安全事件情况下的应急处置工作。

第二章 组织架构

第五条 网络安全和信息化领导小组（以下简称领导小组）是学校网络安全和信息化工作的领导机构，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Ⅰ、Ⅱ级网络安全事件应急响应启动，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响应工作。

第六条 网络与信息中心为领导小组办公室所在单位，在应急工作中负责:

1. 制定学校网络安全相关制度和应急响应预案;

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. 建立健全各单位联动机制，指导、督促各单位完成本单位网络安全事件应急机制建设，并完成检查工作;

4. 在应急演练与响应中提供技术咨询与支持、保障和培训工作;

5. 在网络安全应急处置工作中组织应急技术支撑队伍，提供技术支持与保障，并及时向领导小组报告情况;

6. 每季度向领导小组报告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。

第七条 学校各单位在应急工作中负责:

1. 本单位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. 建立健全本单位网络安全应急响应机制，制定单位内网络安全应急响应预案，定期进行网络安全事件应急演练;

3. 明确本单位应急响应负责人，应急响应负责人负责本单位网络安全应急具体工作，并负责与网络与信息中心对接。应急响应负责人员发生变动时，需及时报送网络与信息中心备案;

4. 积极支持配合领导小组及网络与信息中心进行应急响应处置工作。

第三章 监测预警

第八条 建立健全校内网络与系统（网站）监测预警机制，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”。

第九条 网络与信息中心负责进行全校范围内网络与系统（网站）实施安全监测；各单位负责实施本单位网络与系统（网站）的安全监测，一旦发现网络安全威胁应立即报送预警信息至网络与信息中心。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。

第十条 收到网络安全威胁预警后，由网络与信息中心进行取证以及风险评估，若存在紧急风险，网络与信息中心根据监测与评估结果情况发布预警信息并向领导小组进行汇报，根据威胁情况启动相应预案，必要时执行断网、关闭服务器等措施防止事态扩大。

第十一条 发布预警信息后，网络与信息中心与相关技术支撑队伍对预警现场情况进行跟踪和态势分析与分级预判。根据预判，若可能发生III级及以下网络安全事件，由网络与信息中心组织技术支撑队伍做好应急准备或处置；若可能发生II级及以上网络安全事件，网络与信息中心应及时上报领导小组，研究制订应对方案，积极做好应急处置准备或保障，在处置期间实行24小时值守，若事态发展可能超过学校控制能力，应及时上报教育部。

第四章 应急响应

第十二条 各单位落实网络安全应急工作。在国家重大活动、会议期间，各单位实行24小时值班制，确保网络安全事件发生时能及时联系、及时处置。

第十三条 网络安全事件发生后，事发单位应及时启动预案，保留相关证据，并通知网络与信息中心。网络与信息中心组织现场搜集相关信息，分析安全事件态势，若初判为II级以上网络安全事件，及时报告领导小组，由领导小组启动I级、II级应急响

应，成立应急小组，组织研究处置方案并进行指挥协调工作。网络与信息中心及相关技术支撑队伍进行具体工作推进实施，提供现场安全保障，控制事态蔓延。应急小组在领导小组指挥下，根据具体情况调动相关物资、设备，必要情况下请求校外应急支援，相关成员保持 24 小时通讯畅通。

第十四条 若初判为Ⅰ级网络安全事件，应急小组应及时上报教育部；对于人为破坏活动，同时报公安机关。

第十五条 应急处置过程中，网络与信息中心及相关技术支撑队伍持续跟踪事态发展、检查影响范围，若为Ⅱ级事件，或Ⅲ级及以下事件有转化为Ⅱ级事件的趋势，网络与信息中心应及时将事件危害程度、损失情况及现场处置情况上报领导小组；若为Ⅰ级事件，或Ⅱ级事件有转化为Ⅰ级事件的趋势，领导小组应及时将事件危害程度、损失情况及现场处置情况上报上级部门。

第十六条 在Ⅰ级、Ⅱ级网络安全事件经应急处置后，应急小组将监测数据及其他处置情况报告领导小组，由领导小组确定结束应急处置，发布应急结束信号。

第十七条 应急响应工作结束后，相关单位迅速执行整改计划，采取措施修整受损设施、数据，减少损失，消除隐患，恢复网络或系统（网站）至突发事件前状态，同时对事件损失进行统计、记录、分析。

第十八条 整改工作结束后，网络与信息中心组织技术人员与专家对事件发生及处置进行全面调查，实施取证工作，定位溯

源，总结经验教训，完成《安全事件总结报告》，修订完善应急响应体系。

第五章 应急演练

第十九条 各单位应建立健全网络安全事件应急演练机制，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。

第二十一条 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。

第二十二条 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响应体系，维护更新防护设施。

第六章 预防工作

第二十三条 做好网络安全日常预防与监测工作，根据学校工作实际开展情况，逐渐更新、完善应急管理体制。做好网络安

全检查与监测、风险评估和容灾备份，加强校内网络及系统（网站）的安全保障能力与监测预警能力。

第二十四条 将网络安全教育作为国家安全教育的重要内容，充分利用网络安全宣传周等各种活动形式及多种传播媒介，加强对突发网络安全事件预防与应急处置相关法律、法规和政策的宣传，积极开展网络安全基本知识和技能的宣传活动，提升学校师生网络安全防范意识。

第二十五条 定期对学校各单位网络安全相关负责人进行网络安全事件应急知识集中培训，使相关人员熟悉应急方案流程、应急设备的操作方法等，增强各单位防范意识和应急处置能力。

第七章 工作保障

第二十六条 加强我校网络安全应急保障队伍与专家队伍建设，与机关团体、企事业单位等力量形成良好合作与互动。通过推动等级保护等工作提升学校对于网络安全事件的监测预警、安全防护、应急处置能力。

第二十七条 建立监督检查机制。按预案的规定不定期进行检查，对未有效落实预案各项规定的部门进行通报批评，责令限期改正。

第二十八条 加强我校网络安全应急基础平台与管理平台建设及应急资源准备，为重要系统建立容灾环境，预留应急网络硬件、软件、车辆等应急物资，由领导小组负责统一调度。

第二十九条 学校每年提供专项经费，用于网络安全应急技术支撑队伍建设、专家队伍建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。

第八章 附　则

第三十条 本预案原则上每年评估一次，根据实际情况适时修订。修订工作由学校网络安全和信息化领导小组办公室组织。

第三十一条 本预案由学校网络安全和信息化领导小组办公室负责解释。

第三十二条 本预案自印发之日起实施。

抄送：各党工委，各基层党委、党总支、直属党支部，党委各部、委、办，工会、团委。

东南大学校长办公室　　2019年12月9日印发