南京邮电大学文件

校信发〔2020〕3 号

南京邮电大学网络安全突发事件应急预案

第一章 总则

第一条 为积极应对、妥善处理学校各类校园网络突发事件，维护学校正常的教学秩序，营造健康向上的网络环境，根据《教育系统网络安全事件应急预案》（教技〔2018〕8 号）、《江苏省网络安全事件应急预案》（苏教信〔2018〕4 号）、《信息安全事件分类分级指南》（GB/T 20986-2007）、《南京邮电大学网络与信息系统安全管理办法》以及其他相关法律法规，结合学校实际情况，特制定本应急预案。

第二条 本预案所指网络突发事件是指包括但不限由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统及相关数据安全造成危害，或对社会造成负面影响的事件。

第三条 本办法适用于南京邮电大学IP公网地址段及域名包含（njupt.edu.cn后缀）的所有网络资源，或互联网络域名解析到南京邮电大学校内IP地址段的信息化资源；只要满足上述任意一条均属于本办法管辖的范围。

第二章 组织机构及工作原则

第四条 我校网络与信息安全的相关工作均由校网络安全和信息化领导小组（以下简称“网信领导小组”）负责，校信息化建设与管理办公室（以下简称“信息办”）作为下设办事单位，协调校内各相关单位（部门）负责具体实施。

第五条 信息办负责全校所有网络突发事件的应急响应及通报工作，主要包括：

1.负责监督、检查与指导各单位（部门）的应急响应和信息通报工作；

2.负责整理汇总各单位（部门）上报的网络信息安全突发事件并备案；

3.负责拟定及发布各类网络信息安全通知及公告；

4.每年组织一次全校规模的网络安全应急演练。

第六条 各单位（部门）主要职责：

1.负责建立本单位（部门）的应急响应与信息通报工作机制；

2.负责及时上报本单位（部门）的各类网络安全突发事件，并按要求上报信息办进行登记备案；

3.负责接收、转发上级单位发布的网络安全事件、安全预警等信息，并及时采取防范措施，争取早发现、早报告、早控制、早解决，严控网络安全突发事件的风险和影响范围；

4.明确本单位（部门）的信息化分管领导及信息系统安全管理员（以下简称“信息管理员”），并报信息办备案，如有任何人员变动，需及时更新备案；

5.各单位（部门）应做好网络安全的日常预防工作，完善本单位（部门）应急处理机制，落实各项防护措施，责任到人，做好网络安全检查、风险评估和容灾备份，加强信息系统的安全保障能力；

6.各单位（部门）作为信息系统的直接负责单位，应对网络安全突发事件预防和处置的相关法律法规和政策加强宣传教育；

7.各单位（部门）应定期组织本单位教职工参加网络安全培训教育，提高本单位师生的网络安全意识，并按要求将每次培训记录提交信息办备案。

第七条 按照《信息安全事件分类分级指南》（GB/T 20986-2007）的明确要求，根据信息安全事件的分级考虑要素，结合学校实际，信息安全事件主要类型包括：

1.网站、网页出现非法信息事件；

2.黑客攻击事件；

3.病毒感染事件；

4.软件系统遭破坏性攻击事件；

5.数据库安全事件；

6.广域网外部线路中断事件。

第三章 应急响应原则及处置

第八条 信息办通过多种途径实时监测，搜集各类安全漏洞、病毒、网络攻击等安全事件信息，并根据影响范围分级通知各单位（部门）及全校师生。各单位（部门）信息管理员应负责督促本单位（部门）安全漏洞的修复情况，并协同信息办进行全面排查安全隐患，提高发现和应对网络安全突发事件的能力。

第九条 网络安全突发事件发生后，各单位（部门）应立即启动应急预案，同时告知信息办协同处理，根据不同的事件类型和事件原因，采取科学有效的应急处置措施，将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。信息办将根据事件紧急情况和影响范围上报校网信领导小组，情节严重的应立即上报公安部门。

第十条 当发生网络安全突发事件时，信息管理员应立即切断发生突发事件系统或设备的网络连接，确保其断网停止服务，立即通知信息办及本单位信息化工作分管领导，同时填写相关表格报送信息办。信息办接报后应立即采取必要措施，尽可能缩小事件的影响范围；随后组织该系统或设备的维保厂商及安全服务厂商，在保护现场的同时积极进行修复解决。网络安全突发事件处理完毕并经相关机构进行检测复核无误后，信息办将与相关事

件的直接负责单位沟通，恢复原有的网络服务。最后，由校网信领导小组和信息办共同判定该突发事件的等级范围，并按要求及时上报。

第四章 通报制度和方法

第十一条 通报制度

1.各部门（部门）应建立网络与信息安全突发事件的信息通报制度：当发生网络与信息安全突发事件时，填写《网络安全突发事件报告单》（见附件 1）。

2.信息办在收到突发事件报告单后，应立即上报校网信领导小组并通知各相关单位（部门），各单位（部门）在收到信息办的通报后，应立即检查本单位的网络信息安全情况，如有任何异常，应立即上报《网络安全事件反馈单》（见附件 2）。

3.网络与信息安全突发事件应急处置结束后，涉事单位（部门）应填写《网络安全突发事件应急处置总结》（见附件 3），并在 3 个工作日内提交信息办备案存档。

第十二条 通报办法

1.各单位（部门）信息管理员负责信息通报的接收与反馈；

2.对于网络安全突发事件，应先通过电话紧急通知，随后按要求填写相关表单并发送邮件给信息办备案；

3.各单位（部门）应及时、全面、准确报送信息，不得瞒报、缓报、谎报。因瞒报、缓报、谎报而造成重大安全事故的后果，

依据国家、学校有关法律及规定追究其部门及领导的责任。

第十三条 各单位（部门）应按照国家、教育部门保密规定，做好本单位（部门）网络与信息安全信息通报的保密工作。

第七章 附则

第十四条 本办法由信息办负责解释。

第十五条 本办法自发布之日起执行，原《南京邮电大学网络突发事件应急预案》（校信发〔2014〕7号）同时废止。

附件：1、网络安全突发事件报告单

2、网络安全事件反馈单

3、网络安全突发事件应急处置总结

2020年10月29日

附件 1：

网络安全突发事件报告单

报告单位		报告时间	年_月_日_时
事发单位		事件起始时间	__年_月_日_时
填报人		审核人	
事件分类	☐有害程序类事件 ☐网络攻击类事件 ☐信息破坏类事件 ☐信息内容安全类事件 ☐故障类事件 ☐灾害类事件 ☐其它类事件		
危害表象	☐网络中断 ☐系统瘫痪 ☐数据毁坏 ☐数据泄密 ☐其它危害		
事件描述：（包括突发事件发生原因、性质，初步原因和危害程度判断）			
处置措施：（突发事件发生单位已采取的控制措施及其他应对措施）			
事件后果的初步估计：			
有关意见和建议：			

附件 2：

网络安全事件反馈单

反馈单位		反馈时间	年 月 日
填报人		审核人	
检查情况	□有同类隐患　　□无同类隐患		
处置措施			
其他说明			

附件 3：

网络安全突发事件应急处置总结

<table>
<tr><td>上报单位</td><td colspan="2"></td><td>填报时间</td><td>年 月 日 时</td></tr>
<tr><td>事件名称</td><td colspan="4"></td></tr>
<tr><td>填报人</td><td colspan="2"></td><td>审核人</td><td></td></tr>
<tr><td colspan="5">事件最新概况：（包括当前事态、已造成的影响情况及发展趋势等）</td></tr>
<tr><td colspan="5">应急处置进展情况：（包括开展的应急处置行动、已经取得的进展、当前主要工作及政府部门开展的工作情况）</td></tr>
<tr><td colspan="5">应急资源调配情况：（包括人员调动、物资调配及资源需求等情况）</td></tr>
<tr><td colspan="5">下一步应急工作部署：（包括应急进展预估和应急处置计划等）</td></tr>
</table>

（此页无正文）

南京邮电大学校长办公室　　2020 年 10 月 29 日印发