# 南京邮电大学文件

校发〔2020〕63 号

## 南京邮电大学网络与信息系统安全管理办法

为加强南京邮电大学校园网络与信息系统的安全保护和管理，形成与教育信息化发展相适应的网络与信息安全保障体系，保障和促进南京邮电大学信息化建设与运行维护工作的合理发展，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、公安部《信息安全等级保护管理办法》等有关法律文件的规定，结合学校实际情况，特制定本办法。

### 第一章 总则

**第一条** 本办法所称的网络与信息系统，是指包括但不限于基础信息网络、信息系统（含采用移动互联技术的系统）、云计算平台（系统）、大数据应用（平台、资源）、物联网等。校园网

络与信息系统安全管理包含服务于南京邮电大学计算机及其相关的配套设备设施的安全、网络运行环境的安全、网络信息的安全、监测预警和应急处置等方面。

**第二条** 南京邮电大学网络安全和信息化领导小组是学校网络与信息系统安全管理的领导机构。信息化建设与管理办公室（以下简称“信息办”）负责学校网络与信息系统的安全管理与监督工作，负责全校校园网络和公共信息系统安全保护的技术支持和应急处置以及安全教育和培训。宣传部、信息中心负责对学校宣传内容审核，并对各二级网站进行指导和督查。

**第三条** 我校校园网络与信息系统安全保护工作实行分级管理模式。学校各二级单位、职能部门是本单位（部门）网络和信息系统安全工作的责任主体，其主要领导是本单位（部门）的网络和信息系统安全工作第一责任人，负责依据本办法贯彻具体落实工作。

**第四条** 我校校园网络与信息系统安全管理实行工作责任制，按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的基本规则，全校各单位（部门）及全体师生员工应依照本办法及其相关标准规范履行网络与信息系统安全的义务和责任。

## 第二章 网络与信息系统安全管理

**第五条** 南京邮电大学网络与信息系统安全管理实行等级保护制度。各信息系统建设管理单位（部门）应依照国家要求及相关标准规范，履行安全等级保护的义务和职责。

**第六条** 南京邮电大学网络与信息系统实行备案制度。各信息系统建设管理单位（部门）应将本单位（部门）内部信息系统向信息办备案，具体备案方式请参照《南京邮电大学网络与信息系统安全管理实施细则》（见附件）相关条例执行。

**第七条** 南京邮电大学网络与信息系统安全管理实行安全监测和通报制度。信息办根据内部安全监测实时跟踪涉及我校的网络与信息系统安全问题，通知用户单位进行处理。

**第八条** 各单位（部门）应遵照《南京邮电大学网络与信息系统安全管理实施细则》（见附件）进行网络与信息系统安全日常管理。

## 第三章 网络与信息系统应急管理

**第九条** 网络与信息系统安全事件的应急处置，依照“统一领导，快速反应，密切配合，科学处置”的组织原则，充分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

**第十条** 学校各二级单位、职能部门发生网络与信息安全事件后，应立即向信息办和相关部门报告，应按照《南京邮电大学网络突发事件应急预案》采取相应处置措施，将不良影响与损失降到最低。

## 第四章 附则

**第十一条** 本办法由信息办负责解释。

**第十二条** 本办法自发布之日起施行，原《南京邮电大学网络与信息系统安全管理办法（试行）》（校发〔2014〕47号）、《南

京邮电大学信息系统安全等级保护工作管理办法》（校信发〔2014〕2号）、《南京邮电大学校园网安全管理条例》（校信发〔2014〕5号）、《南京邮电大学校园无线网络管理办法（暂行）》（校信发〔2015〕1号）、《南京邮电大学校园网络信息安全管理办法》（校信发〔2019〕5号）同时废止。

附件：南京邮电大学网络与信息系统安全管理实施细则

2020年10月29日

附件：

# 南京邮电大学
# 网络与信息系统安全管理实施细则

为加强南京邮电大学网络与信息系统安全管理工作，根据国家相关法律法规和《南京邮电大学网络与信息系统安全管理办法》的具体内容，特制定本实施细则。

## 第一章 专职人员管理

**第一条** 各二级单位、职能部门主要领导是本单位（部门）的网络与信息系统安全工作第一责任人，负责贯彻具体落实工作，并指定专人担任网络与信息系统安全管理员（以下简称“信息管理员”），负责本单位（部门）网络与信息系统安全管理工作。

**第二条** 各二级单位、职能部门应设定至少一名信息管理员，信息管理员主要负责本单位（部门）网络与信息系统的安全管理、本单位（部门）师生网络信息安全培训学习等工作。

**第三条** 各二级单位、职能部门主要领导应每年签订《南京邮电大学网络与信息系统安全责任书》，并报送信息化建设与管理办公室（以下简称“信息办”）。

## 第二章 安全等级保护管理

**第四条** 学校各网络信息系统的建设管理单位（部门）作为安全等级保护的责任主体，应当按照国家等级保护相关管理规范、技术标准确定网络信息系统的安全等级。涉密信息系统应当

根据国家涉密信息保护的基本要求，按照学校保密工作部门有关涉密信息系统分级保护管理规定和技术标准进行保护。

**第五条** 对新建、改建、扩建的网络信息系统，建设管理单位（部门）应当在规划、设计阶段按照《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）确定信息系统的安全等级，同步建设符合该安全等级要求的信息安全设施，按照《南京邮电大学系统上线安全管理规定（试行）》要求提交申请，经信息办核准后，方可上线正常运行。

## 第三章 备案管理

**第六条** 在履行信息系统备案手续时，申请单位（部门）应当向信息办提供以下材料：

1.设立该信息系统的目的、用途、服务范围、功能说明等基本信息；

2.信息管理员的基本情况。其中，第一责任人应为本校在职教职工；

3.办理备案手续，该信息系统所属单位（部门）的信息化分管领导需在申请材料上签署审核意见并加盖部门公章；

信息系统在备案有效期内需要变更信息或终止服务的，应当在相关变更发生之日起30日内向信息办履行备案变更或终止服务的手续。

**第七条** 信息办对学校所有信息系统的备案实行年度审核。在年度审核时，信息管理员应在规定时间提交年度审核信息。未

通过年度审核的，信息办将直接关闭该网站系统并注销备案。

## 第四章 监测与处置管理

**第八条** 信息系统建设管理单位（部门）应当建立信息系统安全状况日常监测工作制度，按照国家有关管理规范和技术标准，定期对信息系统安全状况、安全制度及措施的落实情况进行自查。

**第九条** 信息办负责对学校所有公网IP和网络资源进行实时安全监测，一旦发现安全漏洞或安全问题，第一时间封闭网站的外网访问及出校访问权限，并通知相关负责单位（部门）进行紧急处理。按照要求，校内安全漏洞的处理时限为60小时，修复完成后反馈信息办。如超过60小时没有修复完成，信息办将收回网站（系统）的公网IP地址及域名，并断网停止服务器的运作。

## 第五章 运维管理

**第十条** 各二级单位、职能部门应积极推进以下工作：

1.严格执行学校网络安全责任制和网络安全培训；

2.仔细核实、登记并及时更新网络与信息系统资产信息；

3.做好信息发布的审核、登记、保存、清除和备份；

4.按照要求做好网络信息安全处置及备案；

5.及时上报网络安全事件，对突发事件及时做好应急处理。

**第十一条** 各二级单位、职能部门应落实以下安全保护技术措施：

1.针对操作系统的补丁、安全漏洞、更新等内容的定期维护；

2.针对应用系统重要数据的管理、备份、容灾恢复；

3.针对计算机病毒等破坏性程序的防治；

4.针对网络入侵、攻击破坏等危害网络安全行为的防范；

5.做好系统运行和用户使用日志的备份，备份信息至少保存6个月；

6.针对密钥、密码安全进行重点管控和及时更新。

**第十二条** 外包管理

采取信息技术外包的单位（部门），应重视外包服务的安全管理工作，选择具有国家专业资质认证的外包服务提供商，与其签订网络与信息系统安全保密协议，并在外包服务合同中明确安全与保密责任。

外包技术人员远程服务时应采取书面审批、访问控制、在线监测、日志审计等安全防护措施。现场服务过程中应安排专人管理，并记录服务过程。外包开发的系统、软件上线前，必须通过信息办的安全测评。

## 第六章 网络使用行为规范

**第十三条** 任何单位（部门）或者个人不得从事下列危害网络与信息系统安全的行为：

1.擅自进入、使用他人的计算机信息网络；

2.擅自增加、修改、删除、复制、利用他人的信息网络数据；

3.擅自增加、修改、删除、干扰、利用他人的信息网络功能；

4.破坏计算机信息网络运行环境、设备设施；

5.窃取、盗用、篡改、破坏他人网络资源；

6.故意制作、传播、使用计算机病毒、恶意软件等破坏性程序，或制作、发布、复制、传播含破坏性程序或其机理、源程序的信息；

7.故意阻塞、阻碍、中断计算机信息网络的信息传输，恶意占用网络资源；

8.利用电子邮件、电话、即时通信软件或社交平台，大量或多次发送垃圾邮件、短信、微博、微信信息等，干扰他人正常生活或网络秩序；

9.利用网络违背他人意愿、冒用他人名义发布信息；

10.明知本单位或本人的网络地址、主机空间等资源已被他人利用，存在可能危害网络信息安全的活动而不予报告或制止；

11.擅自利用网络收集、使用、提供、买卖学校公共数据或他人专有信息；

12.其他危害网络与信息系统安全的行为。

**第十四条** 任何单位（部门）或者个人不得利用网络制作、发布、传播含有下列内容的信息：

1.反对宪法基本原则的；

2.危害国家安全，泄露国家秘密，颠覆国家政权，或任何涉及破坏国家统一的；

3.损害国家荣誉和利益的；

4.煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族

风俗习惯的；

5.破坏国家宗教政策，宣扬邪教、封建迷信的；

6.散布谣言，扰乱社会秩序，破坏社会稳定的；

7.鼓动公众恶意评论他人、公开发布他人隐私或者通过暗示、影射等方式对他人进行人身攻击的；

8.公然侮辱他人或者捏造事实诽谤他人的；

9.以非法社团名义活动的；

10.买卖法律、法规禁止流通的物品的；

11.非法买卖法律、法规限制流通的物品，对公共安全构成威胁的；

12.含有淫秽、色情、赌博、暴力、欺诈等内容，或者教唆犯罪、传授犯罪方法的；

13.含有法律、法规禁止的其他内容的。

## 第七章 其他管理

**第十五条** 教育培训

各单位（部门）应加强网络与信息系统安全教育，信息系统管理人员应主动参加信息办组织的安全类专业培训。

信息办每年组织一次网络与信息系统安全管理人员和技术人员专业培训，不定期邀请校内外专家开展网络与信息系统安全讲座。

**第十六条** 应急演练

各二级单位、职能部门应按照《南京邮电大学网络突发事件

应急预案》的具体要求，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。

各单位（部门）应根据本单位（部门）实际情况，补充完善本单位（部门）的安全事件应急处置机制，制定安全事件应急处理方法或预案，并定期组织应急演练。信息办每年将对所有网络与信息系统安全工作的落实情况进行统一检查，并根据具体情况进行调查处理。

**第十七条** 处理意见

信息办对不遵守上述条例的行为可作以下处理，并根据具体情况及时上报网络安全和信息化领导小组。处理建议包括但不限于：

1.提出警告，并勒令限期整改安全漏洞及相关错误信息；

2.中断网络服务 3 至 60 天;

3.关闭服务器、停止信息系统的一切服务。

（此页无正文）

南京邮电大学校长办公室　　2020 年 10 月 29 日印发