南通师范高等专科学校文件

通师高专校〔2020〕17 号

关于印发南通师范高等专科学校网络与信息安全管理相关规章制度的通知

各部门、各单位：

为加强学校网络与信息安全管理，提高学校网络与信息安全防护能力和水平，保障学校信息化可持续发展，经学校研究，制定《南通师范高等专科学校网络与信息安全管理组织体系与岗位职责》《南通师范高等专科学校网络与信息安全人员管理办法》《南通师范高等专科学校网络机房安全管理办法》《南通师范高等专科学校校园网基础设施管理办法》《南通师范高等专科学校校园网安全管理办法》《南通师范高等专科学校信息系统建设管理办法》《南通师范高等专科学校信息系统运行安全管理办法》《南通师范高等专科学校信息系统终止管理办法》《南通师范高等专科学校信息安全事件报告和处置管理办法》《南通师范高等专科学校校园信息化文档管理办法》《南通师范高等专科学校计

算机信息系统密码安全管理办法》《南通师范高等专科学校计算机病毒防治管理办法》《南通师范高等专科学校网站建设与管理办法》《南通师范高等专科学校教育移动应用管理制度》等管理办法。现予以印发，请遵照执行。

附件：1.南通师范高等专科学校网络与信息安全管理组织体系与岗位职责

2.南通师范高等专科学校网络与信息安全人员管理办法

3.南通师范高等专科学校网络机房安全管理办法

4.南通师范高等专科学校校园网基础设施管理办法

5.南通师范高等专科学校校园网安全管理办法

6.南通师范高等专科学校信息系统建设管理办法

7.南通师范高等专科学校信息系统运行安全管理办法

8.南通师范高等专科学校信息系统终止管理办法

9.南通师范高等专科学校信息安全事件报告和处置管理办法

10.南通师范高等专科学校校园信息化文档管理办法

11.南通师范高等专科学校计算机信息系统密码安全管理办法

12.南通师范高等专科学校计算机病毒防治管理办法

13.南通师范高等专科学校网站建设与管理办法

14.南通师范高等专科学校教育移动应用管理制度

南通师范高等专科学校

2020年6月8日

附件 1

南通师范高等专科学校
网络与信息安全管理组织体系与岗位职责

第一章 总　则

第一条 为加强南通师范高等专科学校网络与信息安全管理，按照教育部网络与信息安全工作“分级管理、逐级负责”的指导原则，建立南通师范高等专科学校网络与信息安全管理组织体系，明确岗位职责。

第二章 学校网络与信息安全管理组织体系

第二条 南通师范高等专科学校网络与信息安全管理组织体系由学校网络安全与信息化领导小组（以下简称领导小组）、网络与信息安全工作处室、各部门与各学院二级部门网络安全与信息化工作小组组成。

第三条 领导小组全面负责和统一管理校园网络安全与信息化的规划、建设和管理工作，是学校网络安全管理的最高决策机构，学校网络安全总体方针政策的制定者，学校网络安全管理工作的领导和总负责者。领导小组组长由校党委书记和校长担任、副组长由其他校级领导担任；小组成员由学校各部门、各学院主要负责人组成。

第四条 网络与信息安全工作处室是学校网络与信息安全工

作的责任单位，根据领导小组的部署组织开展学校网络与信息安全工作。

第五条 各学院、部门、单位（以下简称各单位）是学校网络与信息安全管理的基层组织。各单位应成立网络安全与信息化工作小组，其主要负责人为第一责任人，并指定专人担任网络与信息安全员，负责本单位及下属单位的网络与信息安全工作。

第三章 网络与信息安全管理岗位职责

第六条 领导小组主要职责：领导学校网络与信息安全总体工作。根据网络与信息安全相关政策和法律法规审议批准学校网络与信息安全总体策略规划和网络与信息安全建设规划；建立健全学校网络与信息安全管理组织体系和管理机制；对重大网络与信息安全事件的处理进行决策；指导和检查网络与信息安全职能部门的各项工作等。

第七条 网络安全工作处室主要职责：信息化工作办公室负责学校网络安全与信息化的总体规划、建设、运行，制定学校网络与信息安全管理制度，为网络与信息安全提供技术保障；党政办公室负责学校网络安全和信息化工作的组织协调工作，通报校园网络与信息安全事件；组织宣传部负责网络信息内容的安全监管，负责校园网络舆情信息的监控和管理；安全保卫处负责对网络违规行为进行调查、取证、处理，根据相关证据及事态影响或破坏程度，对违规者按照有关规定进行处理。

第八条 各单位网络安全与信息化工作小组主要职责：负责

本单位网络与信息安全和保密管理工作；制定适合本单位业务工作需要的安全管理制度与工作规程；加强对本单位业务服务器、信息系统和网站的安全监管，明确网络管理员、系统管理员、业务操作人员以及技术维护人员的职责；随时做好本单位的网络信息发布内容的监控；根据学校部署开展单位网络安全检查并按时完成安全整改工作；配合学校网络安全事件应急响应与处置小组处理网络安全事件，积极协助有关部门开展调查取证工作等。

第四章　附　则

第九条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第十条 本办法自公布之日起实施。

附件 2

南通师范高等专科学校
网络与信息安全人员管理办法

第一章　总　则

第一条 为加强对学校网络与信息安全人员的管理，根据国家和教育行业相关政策规定，制定本管理办法。

第二条 网络与信息安全人员包括校内各单位网络与信息安全责任人、网络与信息安全员及各类信息系统关键岗位人员。

各单位网络与信息安全责任人由主要负责人担任，各单位需指定专人担任网络与信息安全员，信息系统关键岗位人员包括系统管理员、网络管理员、数据库管理员、系统应用开发人员、系统维护人员、系统业务操作人员等岗位人员。

第三条 网络与信息安全人员由学校信息化工作办公室统筹管理，各类网络与信息安全人员的任职、调动、离岗等应履行相关手续，承诺其调离后的保密义务。

第二章 网络与信息安全人员任职要求

第四条 网络与信息安全人员必须政治可靠、业务素质高、遵纪守法、恪尽职守、技术过硬。

第五条 网络与信息安全人员应严格遵守国家有关法律、法规和学校有关规章制度，严守单位秘密。违反国家法律、法规和行业规章以及受过处罚的人员，不得从事网络安全管理与相关技

术工作。信息系统关键岗位人员有责任保守信息系统的秘密，必要时应以签署保密协议的方式作出安全承诺。

第三章 安全责任人和网络安全员安全责任

第六条各单位网络与信息安全责任人全面负责本单位的网络与信息安全管理工作，承担网络与信息安全事故管理责任。

第七条 网络与信息安全员应履行以下职责：负责本单位网络与信息安全管理的日常工作；规范本单位信息发布流程，确保单位网站或信息系统信息发布合规合法，防止有害信息传播和涉密信息泄露；配合学校网络与信息安全工作处室和公安机关开展网络安全检查工作，对重要信息系统安全管理进行指导和监督；负责维护和审查有关安全审计记录，及时发现存在问题，提出安全风险防范对策；定期对单位信息基础设施进行巡检；开展网络安全知识的培训和宣传工作；监控本单位网络与信息安全总体状况，保管网络设备资产台账，制定网络与信息安全工作方案和应急预案；及时向学校网络与信息安全工作处室报告网络信息安全事件，协助调查取证和落实整改措施。

第八条 网络与信息安全员在行使安全防控职责时，如确因工作需要，经批准，可了解涉及单位运作与管理有关的信息系统的重要信息。

第九条 网络与信息安全员如发现本单位重大网络与信息安全隐患，有责任向学校网络与信息安全工作处室报告。

第十条 网络与信息安全员如发现信息系统关键岗位人员使用不当，应及时建议单位进行调整。

第四章 信息系统关键岗位人员安全责任

第十一条 信息系统关键岗位人员按“分权和授权”原则，明确岗位权责，允许兼任，但避免权责过于集中。其中系统管理人员、网络管理人员、数据库管理员、系统开发人员、系统维护人员行使各自职权，相互监督，但不宜兼任系统业务操作员。

第十二条 对信息系统关键岗位人员应实行人员备份管理，保证至少有两个合适的人员可处理系统问题。关键岗位人员应定期接受安全相关业务培训与学习，加强自身安全意识和风险防范意识。

第十三条 关键岗位人员调离岗位，必须严格办理调离手续，承诺其调离后的保密义务。

第十四条 关键岗位人员离岗后，必须即刻更换其操作密码或注销用户。

第十五条 系统管理员负责系统的运行管理，实施系统安全运行细则；严格用户权限管理，维护系统安全正常运行；认真记录系统安全事件，及时向网络与信息安全员报告安全事件；对系统操作的其他人员予以安全监督。

第十六条 网络管理员负责网络的运行管理，实施网络安全策略和安全运行细则；安全配置网络参数，严格控制网络用户访问权限，维护网络安全正常运行；监控网络关键设备、网络端口、网络物理线路，防范网络入侵与破坏，及时向网络与信息安全员报告安全事件；对操作网络管理功能的其他人员进行安全监督。

第十七条 数据库管理员负责系统数据库的运行维护，确保安全运行，数据有备份、可恢复。严格控制数据库用户访问权限。

第十八条 系统开发人员在系统开发建设中，应严格执行系统安全策略，保证系统功能的安全准确实现。

第十九条 系统维护人员负责系统维护，及时排除系统故障，做好维护记录，确保系统正常运行；不得擅自改变系统功能；不得安装与系统无关的其他计算机程序；维护过程中，发现安全漏洞应及时报告信息安全员。

第二十条 系统业务操作员应严格执行系统操作规程和运行安全管理制度；不得向他人提供自己的操作密码；及时向系统管理员报告系统各种异常事件。

第二十一条 关键岗位人员必须严格遵守保密法规和有关信息安全管理规定。

第五章　附　则

第二十二条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第二十三条 本办法自公布之日起实施。

附件 3

南通师范高等专科学校网络机房安全管理办法

为保证校园信息化应用高效、稳定运行，加强配套的信息基础设施安全管理，特制定网络机房安全管理办法。

第一章　总　则

第一条 网络机房即电子信息系统机房，主要为电子信息设备提供运行环境的场所，可以是一幢建筑物或者建筑物的一部分。

第二条 电子信息系统由计算机、通信设备、处理设备、控制设备及其相关的配套设施构成，按照一定的应用目的和规则，对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 网络机房根据用途及特点分为数据中心机房、公共机房、专用机房。根据《数据中心机房设计规范》（GB 50174-2017），我校数据中心机房属于 B 级机房，公共机房属于 C 级机房。

第四条 网络机房安全包含环境安全、设备安全、信息安全、人员安全。

第二章 环境安全

第五条 网络机房基础设施应根据机房所属等级并严格按照《数据中心机房设计规范》（GB 50174-2017）进行设计施工。

第六条 网络机房需根据机房等级采用相应的环境监控及管理机制，保持监控设施良好运行。

第七条 网络机房需对供电线路的负载能力、负载情况进行监控，及时调节，避免局部线路负载过高。

第八条 网络机房需根据机房等级保证充足的制冷量，并为重要区域备份制冷设备。

第九条 网络机房的环境保障设备，如不间断电源（UPS）、空调、消防设备、机柜电源插座（PDU）等，需定期巡检、维保，及时发现并消除各种隐患。

第十条 网络机房需制定和完善应急预案，尤其是停电、消防预案，有计划地进行演练。

第三章 设备安全

第十一条 应明确网络机房设备进场、维护、使用、标识、报废、撤离等各个环节的具体流程及备案内容。

第十二条 应定期清点网络机房设备及配件，并更新设备相关信息。

第十三条 应定期对网络机房设备设施进行巡检，及时发现并处理隐患。

第十四条 非工作期间，网络机房应关好门窗，关闭不用的设备设施，防火防盗。

第十五条 网络机房内严禁私接电源、私拉线路，严禁越权操作设备。

第十六条 网络机房内禁止使用与工作无关的电器，尤其是

功率大、发热量高、发出强磁辐射、易产生火花的电器。

第四章　信息安全

第十七条 网络机房通过校园网出口接入互联网，不得以任何形式私设其它出口。

第十八条 网络机房接入校园网需在信息化工作办公室备案，并由主管单位签署《网络信息安全责任书》。

第十九条 网络机房设备责任方应及时更新升级设备配置及操作系统版本，做好病毒木马防护工作。

第二十条 任何单位或个人如需通过信息机房内设备提供网络信息服务，应提出申请，经校组织宣传部审批备案后，转交信息化工作办公室办理。网络信息服务提供者作为服务安全责任方须保证服务内容合法合规，禁止提供备案范围外的信息服务内容。

第二十一条 如果责任方提供的信息服务范围发生变化，需提出变更申请，由校组织宣传部审批备案后，转交信息化工作办公室办理。

第二十二条 如果责任方停止提供信息服务，需提出服务终止申请，经由校组织宣传部审批备案后，转交信息化工作办公室办理。

第二十三条 当网络机房出现网络信息安全问题、存在网络安全隐患及校园网进行必要维护等特殊情况时，信息化工作办公室有权对机房实行紧急断网隔离处置。

第二十四条 设备管理人员、维护人员在工作结束后，应及

时清理现场所用资料，以免信息泄露。

第五章 人员安全

第二十五条 网络机房管理人员须具备相应的业务能力，并实现岗位备份。

第二十六条 网络机房管理人员须按时值岗，不得擅离职守。

第二十七条 网络机房管理人员有权、有义务拒绝未经授权许可的人员进入机房。

第二十八条 网络机房设备操作人员均需做实名制认证，设备操作需要做好日志备案。使用公共机房计算机终端设备应服从管理安排。

第二十九条 进入网络机房的人员严禁携带易燃、易爆、腐蚀性、强电磁、流体物质等对设备构成威胁的物品。

第六章 附 则

第三十条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第三十一条 本办法自公布之日起实施。

附件 4

南通师范高等专科学校
校园网基础设施管理办法

为加强校园网络基础设施管理，确保用户合理有序利用网络资源，保障校园网安全畅通，为教学、科研、管理、生产、生活提供正常服务，根据国家有关法律、法规，并结合学校实际情况，特制定本办法。

第一部分 弱电管网的管理

第一章 总 则

第一条 学校弱电管网是指按照国家有关技术规范统一设计和施工、埋入地下建设并延伸至建筑物内部的共同弱电管网，包括校内户外地下弱电管道、人（手）井、网络通讯线路、楼宇内弱电间综合布线等。

第二条 弱电管网是学校重要的公共基础设施，是学校的公共财产，学校所有单位或个人都有保护、爱护学校弱电管网的权利和义务，对任何损害弱电管网的行为，有权进行监督和举报。

第三条 学校弱电管网建设、管理的职能部门包括国有资产管理处、后勤基建处和信息化工作办公室。国有资产管理处主管管网资产，后勤基建处主管管道建设，信息化工作办公室主管弱电管网的使用管理及维护工作。弱电管网的使用管理实行事项审批备案制度，由信息化工作办公室审核批准后，报国有资产管理

处备案，重大事项须经学校主管领导审核批准。

第二章 弱电管网建设管理

第四条 除后勤基建处外，任何单位、部门或个人不得擅自在校内建设弱电管道。确需建设的，应及时向后勤基建处申报，审批同意后，报信息化工作办公室备案，方可按照规定进行建设。

第五条 凡经批准开工建设前，应在施工现场设置明显标志和安全护围设施，竣工后应当及时清理现场，恢复道路，并需经主管部门检查验收，现场恢复质量须合格。

第六条 校外单位经学校许可自建的弱电管网，需纳入学校弱电管网统一管理和使用。

第三章 弱电管网使用管理

第七条 信息化工作办公室参与学校弱电管网资源的使用规划和监管，促进校园网、一卡通、校园监控、电话、有线电视等业务等应用正常运转。

第八条 任何单位、部门或个人使用学校弱电管网须向信息化工作办公室提出申请，经批准后方可按照规定使用相应的管网及光纤资源。对未经许可强行进行弱电管网施工的行为，信息化工作办公室将与学校安保处联合行动及时制止。

第九条 学校的弱电管网及光纤线缆属学校自有资源，校外单位如有需求应有偿使用。校外单位有涉及到使用学校弱电管网的业务时，须向学校党政办公室提出申请，批准后与代表学校的信息化工作办公室签订相关使用协议，并服从信息化工作办公室的管理，并报国有资产管理处备案。

第十条 弱电管网使用的审批流程：

校内需使用学校弱电管网单位、部门或个人，应事先填写并提交《南通师范高等专科学校弱电管网使用申请表》、《南通师范高等专科学校校园弱电光纤使用申请表》（见附件）、设计方案、施工方案，由信息化工作办公室审核批准后，报国有资产管理处备案。

第十一条 弱电管网周边的施工管理：

（一）凡涉及到学校弱电管网的施工，须遵循施工规范，接受后勤基建处的指导和监督，不得影响学校已有的通信系统，不得私自开挖管道毁坏校园环境。后勤基建处应对施工过程进行监督。

（二）经许可的单位、部门或个人在线路施工时，须遵照审核的施工方案，科学施工和管理，不得擅自占用未经许可的管网及光纤资源。

（三）工程竣工后，由牵头建设单位提交竣工材料（包括设计文件、管线路由管孔图、竣工验收报告、工程竣工文件、竣工图纸等及电子版），经后勤基建处、信息化工作办公室共同验收，验收合格后方可完工。

第十二条 需要临时占用学校弱电管网部署线路的单位、部门或个人，除按规定进行审批和施工外，在工程结束时，应拆除临时设施并恢复原状，经相关部门验收合格后方可完工。

第十三条 未经许可擅自使用学校弱电管网的单位、部门或个人，信息化工作办公室有权会同安全保卫处、国有资产管理处、后勤基建处责令其将铺设的线路及安装的相关设施拆除，并追究其造成的相应损失。

第十四条 对不符合技术规范且已使用学校弱电管网的情况，应落实整改，达到要求后再投入正常使用。

第四章 弱电管网日常管理

第十五条 对学校弱电管网（线）禁止有以下行为：

（一）擅自拆除、破坏、损坏、改变学校弱电管网（线），或改变其性质、用途。

（二）擅自在学校弱电管网（线）安全保护范围内开挖沟渠、挖坑取土、打桩、顶进作业。

（三）擅自在学校弱电管网内安置无关线路。

（四）擅自破坏、损坏、去除管网（线）标识和标志。

（五）未经许可利用学校弱电管网（线）进行宣传、商业等活动。

（六）其他损害、侵占学校弱电管网（线）及其附属设施的行为。

第十六条 信息化工作办公室安排专人对弱电管网设施进行日常检查和维护，确保其使用状态良好。对于造成弱电管网毁坏的任何单位或个人，要追究其责任。

第十七条 对弱电管网中废弃的线路，业务主管单位应及时清理拆除，同时形成技术文档备案，否则将收回其学校弱电管网使用权。

第十八条 凡有可能涉及到弱电管网的校园建设（如修路、绿化、管道开挖、市政建设等）工程，施工前应向信息化工作办公室申报并做好相应的防范措施，以免破坏学校弱电管网。

第十九条 校内强电线路不应使用弱电管网。

第二十条 弱电管网维护费用应纳入学校年度经费预算。

第五章 档案管理

第二十一条 为便于维护管理，信息化工作办公室应建立完备的学校弱电管网使用档案，并及时更新。形成的档案资料，按学校档案管理规定进行管理。

第二十二条 凡涉及管网线路施工的工程资料，相关学院、单位须到信息化工作办公室建档备案。

第六章 处　罚

第二十三条 凡违反本办法规定的，学校将视其情节轻重予以相应处罚：

（一）赔偿损失：违反本规定对学校弱电管网基础设施造成危害、损害、破坏的，涉事人应将设施恢复原状，自行承担相关费用，并赔偿学校直接乃至间接经济损失。

（二）强行拆除违章设施：对违反本规定在涉及学校弱电管网安全范围内设置的其他设施，尚未对学校弱电管网造成损害的，予以强行拆除，拆除费用由涉事人承担。

（三）责令限期改正：对违反本规定，尚未损害学校弱电管网基础设施的，责令限期整改，整改费用由涉事人承担。

（四）处分：本校人员或部门违反本规定，尚未对学校弱电管网基础设施造成损害的，视其情节轻重处以通报批评、警告、严重警告处分。

第二部分 楼宇综合布线的管理

第一章 总　则

第一条 楼宇网络布线系统是新建、扩建和改建楼宇必备的公共基础设施之一，国有资产管理处、后勤基建处和信息化工作办公室三个部门相互协作共同完成建设或改扩建。

第二条 信息化工作办公室是我校楼宇综合布线系统建设规划的主管部门，担负布线系统规划、方案审核、使用验收和管理维护等职责。

第二章 综合布线建设管理

第三条 楼宇布线系统建设实行严格有序的全过程管理并实行项目管理责任制及分工负责制。

（一）新建、扩建楼宇布线系统的建设立项由后勤基建处负责、信息化工作办公室负责，招投标由国有资产管理处负责。

（二）大修楼宇布线系统的建设立项由信息化工作办公室负责和招投标由国有资产管理处负责。

（三）楼宇布线系统的布线质量管理、网络接入及日常维护、维修由信息化工作办公室负责。

（四）各单位自筹资金建设的内部局域网布线系统由各单位自行管理。

第四条 改建楼宇布线系统时，应注意对原布线系统的保护。如需废除及扩建新的布线系统，应向信息化工作办公室提交申请，并按要求施工。

第五条 楼宇布线系统建设过程应实行项目监理。工程质量监理由工程主管单位委托专业监理单位担当，工程完工时应由监

理单位出具监理报告。楼宇布线系统施工过程中如遇实际情况的变化需修改设计或施工方案，应事先以书面形式征得信息化工作办公室的同意。

第六条 楼宇布线系统建设应符合国家的有关标准规定，保证工程质量。楼宇布线系统建设完成后，由工程主管单位会同信息化工作办公室、国有资产管理处、后勤基建处组织验收，并出具经各方（招标、设计、施工、监理、使用等）代表会同签字认可合格的验收报告。未经验收合格的楼宇布线系统不得交付使用。

第三章 综合布线使用管理

第七条 楼宇布线系统经验收合格开通投入使用前，须向信息化工作办公室完成移交，网络的开通使用须满足环境、安全和管理等必要的条件。移交须包含的文档资料和网络开通使用的条件由信息化工作办公室另行规定。

第八条 楼宇布线系统的施工单位应承诺不少于一年的免费服务期及适当的质保期。其提供的质保范围、内容、响应时间、服务形式等应事先在签约时以合同或其附件形式予以明确。

第九条 校园内每幢楼宇都应配置独立的网络布线及设备间，新建楼宇在基建设计中落实，已建楼宇由国有资产管理处负责调整落实。网络布线及设备间由信息化工作办公室负责使用管理，为保证设备运行环境的安全和整洁，网络布线及设备间不得堆放杂物、不得挪作它用。

第十条 各单位需要对楼宇进行内部装修、改扩建、重建等工程时，应保护好楼宇现有网络布线系统。对楼宇已有布线系统

有影响的工程，须向信息化工作办公室提出书面报告及对网络布线系统改动或重建的设计和施工方案，经审核同意后方能投入施工。对未经信息化工作办公室审核同意的装修、改扩建、重建等工程申请，主管部门不予批准。

第十一条 经批准改建或重建的楼宇布线系统，完工后应向信息化工作办公室移交布线系统竣工图纸等文档资料，经信息化工作办公室验收合格后方可投入使用。

第十二条 各单位自行安排建设的内部局域网布线系统，均由各单位自己负责内部网络的开通、用户管理、维护等工作。信息化工作办公室负责校园网与该局域网一个端口的连通，并提供相应的技术支持。

第四章 综合布线日常管理

第十三条 校园网楼宇布线系统（包括光纤、交换机、设备箱、网线、模块等）属学校财产，作为学校重要的通讯基础设施受国家相关法律和学校有关规定的保护。任何单位和个人未经允许不得擅自改造、迁移和对设备进行操作。如因违反有关规定造成破坏的除责令其恢复原状、赔偿损失外，还将进一步追究有关人员的责任。

第十四条 因学校楼宇、房间重新调配，使用方发生变化时，原使用方应将包含完好网络设施的楼宇或房间（原无此类设施的除外）交还给国有资产管理处，对有在运行设备的房间在移交前应确保其安全。任何单位和个人在进行装修前均应得到资产管理部门的批准同意，凡涉及到网络设施变更均应得到信息化工作办公室同意和在其指导下实施。

第十五条 各单位要加强对搬迁中有关人员的安全指导，主动保护好校园网设施，对由于工作不到位，造成校园网设施损毁的，应追究责任，对有关直接责任者，信息化工作办公室将停止对其提供网络和信息服务。

第十六条 对涉及校内各校区、建筑物的重大变动，有关部门应及时和信息化工作办公室沟通，以提前做好校园网线络和设施的调整，保证校园网用户的正常使用。

第十七条 对恶意破坏校园网设施的行为，将交由校安保处依法进行处理。

第十八条 为进一步加强校园网楼宇布线系统的维护和管理，学校要求各楼宇网络布线系统的主要使用单位应承担起保护网络布线设施的责任，应指定一名兼职网络协管员，负责与信息化工作办公室的沟通，协助信息化工作办公室保证校园网楼宇布线系统的正常运行及其相关数据的一致性和准确性。

第三部分 楼宇弱电间的管理

第一条 弱电间是楼宇中各楼层弱电系统的布线集中汇聚场所，安装有配线设备、网络设备，校园内弱电间由信息化工作办公室统一管理。

第二条 弱电间钥匙由专人保管，严禁随意转借，遗失应及时声明。

第三条 弱电间管理人员应定期检查设备运转是否正常，供电情况和线缆连接是否松脱等；离开时察看灯、锁是否关好。

第四条 弱电间中的交换机等硬件设备，任何人未经授权不得自行拆装或更换，更不能挪作它用；弱电间机柜禁止随意拖动，

非管理人员不可擅自操作弱电间内任何设备。

第五条 弱电间禁止放置杂物、垃圾及易燃、易爆、腐蚀、强磁性物品。

第六条 弱电间管理须做到防静电、防火、防潮、防尘、防热。

第七条 禁止将弱电间内的电源引出挪做它用，确保设备用电安全。

第八条 如有需要进入弱电间工作的人员，需经信息化工作办公室登记允许后方可进入。

第四部分 校园无线网络的管理

第一条 校园无线网络为学校资源，南通师范高等专科学校校园内的无线网络覆盖工作由学校统一规划部署、科学利用。

第二条 信息化工作办公室是在学校授权下开展无线网络建设规划和管理工作的职能部门，其他任何单位或个人无权代表学校就无线网络覆盖相关事宜开展与校外无线网络服务供应商（如：各通信运营商及其代理商）的谈判与合作。

第三条 未经信息化工作办公室审核许可，任何单位和个人不得擅自进行校内（含楼宇内）无线网络（单个房间覆盖的除外）的建设和服务，也不得擅自同意校外无线网络服务提供商在校园内（包含对外经营场所）从事无线网络安装、经营业务。

第四条 校内单位及个人架设的自用小型无线网络，应采用经过入网认证合格的无线路由设备（含有线路由设备）连接校园网，不得干扰校园网络的正常运行，一旦发现与学校无线网络发生冲突或干扰，信息化工作办公室有权采取断网整改措施。

第五条 无线网络是有线网络的补充和延伸，所有用户必须严格遵守国家相关法律、法规及学校有关规定，自觉遵守网络礼仪和道德规范，自觉抵制不良信息，不得利用校园无线网络进行各类非法和违规活动，一旦发现，将依据相关规定严肃处理。

第六条 按照“谁安装谁负责”的原则，架设无线路由设备的单位及个人，需要加强对所设无线网络的接入安全管理，落实安全管理责任人。未设置无线热点登录密码的要增设密码，并妥善保管和定期更改。

第五部分 附　则

第一条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第二条 本办法自公布之日起实施。

附表１．南通师范高等专科学校弱电管网使用申请表

２．南通师范高等专科学校弱电光纤使用申请表

附表 1

南通师范高等专科学校校园弱电管网使用申请表

申请单位		用途	
联系人		电话	
申请事由			
申请单位意见	主管领导签字： 单位（公章） 年　月　日		
相关部门会签意见	主管领导签字： 单位（公章） 年　月　日		
校领导意见			
备注			

附表 2

南通师范高等专科学校校园弱电光纤使用申请表

申请单位		用途	
联系人		电话	
申请事由			
申请光纤芯数	起点	终点	备注说明
申请单位意见			
相关部门会签意见			
校领导意见			
备注			

附件 5

南通师范高等专科学校
校园网安全管理办法

为保障校园网系统的安全、促进学校计算机网络的应用和发展，维护校园网的正常运行和网络用户的使用权益，更好地为学校教学科研服务，依照国家和教育行业的相关政策法规，结合学校实际，特制定如下管理办法。

第一章 总　则

第一条 南通师范高等专科学校校园网是为学校教学及管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网络应用资源。本管理办法所称的校园网络安全管理，是指由校园网络运维管理、网络资源与服务管理、非涉密网络保密管理等所构成的安全管理。

第二条 信息化工作办公室负责校园网规划建设和安全管理工作，保障计算机网络设备、配套设施、机房环境、网络系统和信息系统等的安全。

第三条 校园网出口由信息化工作办公室统一建设和进行安全管理，任何单位或个人不得私自另建互联网出口。

第二章 网络运维安全管理

第四条 校园网由信息化工作办公室统一管理及维护，对校园网用户进行安全审查和监督。接入校园网的各单位，以及教室、实验室、机房、宿舍和个人使用者必须严格使用由信息化工作办公室分配的 IP 地址。任何人不得随意变更 IP 地址及网络设置，不得盗用 IP 地址及相关用户帐号。

第五条 设备安全管理。接入校园网的计算机、服务器、交换机等网络设备应当符合国家有关技术标准和使用规定。各种网络接入设备要切实做好防病毒技术措施，主机操作系统及时更新系统补丁。禁止私拉乱接网络布线及私自安装、更换和拆除网络设备。如有特殊需要，须经过信息化工作办公室审批后方可实施。所有服务器、主干交换机及其他系统主要设备配置更新变化时及时进行备份。网络设备、安全设备、应用系统、操作系统、数据库均应设置登录密码安全管理，密码应符合规定的长度及复杂度，并定期进行更新。设备安全运行日志至少保存 60 天。

第六条 校园网账号安全管理。在校园网开设的用户账户和口令，信息化工作办公室将严格信息管理，不向任何单位和个人提供相关信息，记录账号使用情况、账号对应 IP 地址情况。

第七条 用户安全管理。所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度和实名上网制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网服务器、工作站、终端设备甚至校外服务设施的活动。

第八条 域名安全管理。南通师范高等专科学校注册域名为：ntnc.edu.cn，信息化工作办公室负责管理，校内用户可按相关规定申请使用二级以下各级域名，暂不提供其他域名解析服务。

各学院、各单位域名须有专人管理，定期进行安全和使用情况检查，防止出现违法或无效链接。

第三章 网络资源与服务管理

第九条 应确保校园网及网络资源服务系统的信息数据安全、完整、可用。校园网提供WWW、DNS、DHCP、VPN、FTP、电子邮件、视频组播等信息服务。校园网电子邮件系统为校园用户提供电子邮件收发服务，严禁利用电子邮件散发垃圾邮件、传播计算机病毒等。任何用户不得利用校园网制作、复制、查阅和传播违反法律法规、破坏学校和社会和谐稳定的信息。

第十条 为保障网络正常运行，信息化工作办公室须严格执行网络值班、设备巡检、故障排查、网络监控等制度和技术措施。用户按指定方式报修网络故障，信息化工作办公室安排技术人员排除解决，包括远程指导和现场处理。接入校园网的全体师生员工，须配合国家有关部门及学校依法依规进行的监督检查，接受信息化工作办公室进行的网络资源及服务系统的安全检查。

第四章 非涉密网络保密管理

第十一条 定期按非涉密网络保密要求开展检查，严控涉密信息流转。校园各接入单位应定期依据相关规定对网络设备及信息内容进行检查，严禁通过校园网传播涉密信息，及时发现、上报、解决存在的问题。

第十二条 各级网络与信息安全管理员负责本单位网络与信息的安全工作，根据相关规定上报网络与信息安全事件，及时解

决突发事件和问题。在出现人员调离或离职的情况时，应及时收回操作密码、门禁卡、钥匙等使用权限。

第十三条 校园网主、辅节点设备及服务器等发生信息安全事件，信息化工作办公室将根据相关规定及时处置、备案或向公安机关报告。

第十四条 如发现违反上述任何规定者，信息化工作办公室将视情节轻重和所造成的影响和损失程度，采取警告、关闭帐号、追究法律责任等措施。

第五章　附　则

第十五条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第十六条 本办法自公布之日起实施。

附件 6

南通师范高等专科学校信息系统建设管理办法

为加强校园信息系统的安全管理，保障学校数字化校园整体安全运行，避免信息系统重复建设，根据《信息安全技术、信息系统安全管理要求》和《教育部关于加强教育行业网络与信息安全工作的指导意见》要求，结合学校信息化建设相关规定，制定本办法。

第一章 总　则

第一条 本办法所指“信息系统”，是指学校各部门建设管理、面向学校师生和公众提供业务管理和信息服务，基于校园网运行的应用系统。

第二条 信息化工作办公室是学校信息系统建设的统一协调单位。各单位新建信息系统，须报信息化工作办公室备案，并参与立项讨论和项目验收。

第二章 规划与立项

第三条 各单位建设的信息系统，除满足自身的业务需求外，还需符合学校的信息化建设整体规划，确保在学校规划的总体框架内实现业务协同。

第四条 信息系统开发立项需经各单位主管领导审批，或学校网络安全与信息化领导小组讨论批准，方可正式立项。对于规模较大或业务重要的项目，原则上需进行可行性论证。

第五条 对于新建信息系统须根据《教育行业信息系统安全

等级保护定级工作指南（试行）》（教技〔2014〕4号）进行系统定级，按照教育部政策要求系统建设与系统安全同步规划、同步建设，确保信息系统建设完成时具备相应的安全防护能力。对于重要项目，其信息安全规划须组织相关安全技术专家进行项目安全性论证并报学校网络安全与信息化领导小组讨论批准，方可正式立项。

第六条 信息系统建设项目招标需严格按照国家及学校招投标相关规定执行。参与招标的系统研发商，须具有相应的计算机软件研发资质。

第三章 建　设

第七条 信息系统项目的建设或改造，委托建设单位及承建单位均须指定项目负责人，项目负责人应监督和管理项目的全过程，并制定项目实施计划，作为项目管理过程的依据。

第八条 信息系统项目建设如需外包，应选择具有服务资质、信誉较好的承包商，要求其已获得国家主管部门的资质认证并取得许可证书、能有效实施安全工程过程、有成功的实施案例。对重要的信息系统工程项目外包，应在主管部门指定或特定范围内选择具有服务资质的信誉较好的厂商，并应经实践证明是安全可靠的厂商。外包方应签署信息安全保密协议。

第九条 信息系统建设、实施过程中应严格遵守国家及学校信息化建设管理相关规定，遵循学校的信息标准与规范，并提供标准化的数据交换接口，共享数据应同步至学校主数据库。

第四章　验　收

第十条 信息系统建设验收由委托建设单位提交申请，符合

条件的,信息化工作办公室组织专家评审验收。信息系统验收条件:

1.系统经过试运行,达到了预期建设目标,各项功能符合用户需求(以需求说明书为准);

2.试运行中提出的各类问题(程序类、配置类、常识类)整改完成;

3.试运行中提出各类非功能性需求解决;

4.人员培训完成;

5.进行了系统安全评估,达到相应安全等级保护规定要求,二级以上信息系统应由第三方专业测评机构开展安全测评;

6.集成系统达到集成方案预定要求;

7.系统间数据交换及时、准确。

第十一条 信息系统项目承建方提供项目验收文档资料,并对所提供报告、资料、数据及结论的真实性和可靠性负责。验收文档资料包括但不限于以下内容:

1. 验收申请书;

2. 系统需求说明确认书(原件);

3. 系统功能预览确认单(原件);

4. 系统交付测试申请单(原件);

5. 系统功能列表确认单(原件,用户确认);

6. 系统变更申请单(原件);

7. 系统部署及技术实施方案确认书;

8. 系统试运行申请单(原件);

9. 系统试运行情况说明书(包括试运行方案、试运行报告、用户使用意见等);

10. 系统集成方案(原件);

11. 集成测试报告单；

12. 系统集成功能列表确认单(建设方和图书与信息中心确认)；

13. 运维保障承诺书；

14. 安全评估报告或等级保护测评报告；

15. 数据库表结构及代码；

16. 附件：管理员使用手册、用户手册、系统集成技术文档、系统光盘等。

第十二条 信息系统验收程序。验收程序按项目的合同金额分为三类，A 类：合同金额 20 万以上；B 类：合同金额 5-20 万元；C 类：合同金额 5 万以下。

１．A 类：信息系统项目承建方提交验收申请，建设方检查验收材料，根据信息系统等级保护要求开展系统安全检测，符合该系统安全等级所需安全防护要求后组织专家组进行评审验收。信息系统项目承建方提供的验收文档至少包括材料准备中的1-5项、7-9 项和 13-16 项。

２．B 类：信息系统项目承建方提交验收申请，建设方检查验收材料，根据信息系统等级保护要求开展系统安全检测，符合该系统安全等级所需安全防护要求后组织专家组进行评审验收。项目承建方提供的验收文档至少包括材料准备中的 1-5 项、7-9 项和 13-16 项或 1、10-16 项。

３．C 类：信息系统项目承建方提交验收申请，建设方检查验收材料，根据信息系统等级保护要求开展系统安全检测，符合该系统安全等级所需安全防护要求后建设方、信息化工作办公室根据建设方案进行验收测试，形成验收报告。项目承建方提供的验收文档至少包括材料准备中的 1、10-13 和 16 项。

第十三条 验收结果处理

1．验收合格

（1）通过验收检查和专家评审；

（2）系统安全评估达到相应等级保护标准；

（3）基本满足运行条件；

（4）根据建设内容，完成应用系统所涉及的用户培训。

2．验收不合格

具有下列情况之一的，视为验收不合格：

（1）未通过验收检查小组检查；

（2）未通过验收专家组评审；

（3）系统安全评估未达到相应等级保护标准；

（4）所提供验收材料不真实。

验收不合格的，信息化工作办公室以将书面形式通知承建方限期整改，整改后由项目承建方重新申请验收。

第十四条 信息系统投入运行后，使用单位要按照学校有关网络与信息安全规定，及时配合学校开展信息系统安全等级保护工作，明确专人管理，并落实信息系统运行安全管理制度。

第十五条 信息系统的调整、升级和运行维护方案，须由建设单位负责人会同信息化工作办公室与系统供应商共同协商制定。

第五章 附　则

第十六条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第十七条 本办法自公布之日起实施。

附件 7

南通师范高等专科学校
信息系统运行安全管理办法

第一章　总 则

第一条 为进一步加强南通师范高等专科学校信息系统安全运行管理，确保各类信息应用系统稳定、安全、高效运行，根据国家、教育部及地方教育主管部门发布的政策文件和技术标准，结合南通师范高等专科学校信息系统运维管理的实际情况，制定本办法。

第二条 信息化工作办公室作为学校信息化规划建设的管理部门，负责学校信息系统运维体系的总体规划、建设和管理。各级系统管理员是相关系统安全运行管理的第一责任人。

第三条 各类信息系统运行期间须依据学校安排做好信息系统安全等级保护工作，包括安全等级变更备案与安全测评，不符合要求的须在指定期间内完成整改建设工作，使之持续具备与其安全等级相适应的信息安全防范能力。

第四条 信息系统日常运行维护须从物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复及安全管理措施等方面加强安全管理。

第二章　物理安全

第五条 信息系统主要运行设施应集中存放于指定的信息机房，严格按《南通师范高等专科学校网络机房安全管理办法》要

求加强机房管理，保障信息系统运行环境物理安全。

第六条 编制并保存与信息系统相关的设施清单,根据设施特点制定相应的日常巡查管理办法,通过巡查及时发现相关设施安全隐患并及时排除，保障信息系统相关设施安全运行。

第七条 对信息系统相关存储介质进行控制和保护，对介质存放环境、使用、维护和销毁等制定具体安全管理要求,并对介质的归档和查询等进行登记记录。

第三章 网络安全

第八条 保障系统运行的网络结构安全合理。保证关键网络设备的业务处理能力满足系统运行需要,保证接入网络和核心网络的带宽满足系统运行需要。

第九条 确保系统具有合理的访问控制措施。在网络边界部署访问控制设备，启用访问控制功能。通过访问控制列表对系统资源实现允许或拒绝用户访问。

第十条 保证系统所用网络设备得到有效防护。对登录网络设备的用户进行身份鉴别,登录密码符合安全要求的长度和复杂程度。当需要对网络设备进行远程管理时，应采取必要措施防止信息在网络传输过程中被截取。

第四章 主机安全

第十一条 应对登录主机操作系统和数据库系统的用户进行身份标识和鉴别。

第十二条 主机访问控制。应启用访问控制功能，依据安全

策略控制用户对资源的访问。应限制默认账户的访问权限，重命名系统默认账户，修改默认口令。应及时删除多余的、过期的账户，避免共享账户的存在。

第十三条 入侵和计算机病毒防范。操作系统应遵循最小安装的原则，按需安装组件和应用程序，并保持系统补丁及时得到更新。主机应安装防计算机病毒软件，并及时更新软件版本和病毒特征库。

第十四条 根据安全要求设置登录终端的操作超时锁定策略，限制单个用户对系统资源的最大或最小使用限度。

第五章 应用安全

第十五条 系统身份鉴别机制。信息系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别；提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；启用身份鉴别和登录失败处理功能，并根据安全策略配置相关参数。

第十六条 访问控制机制。信息系统应提供访问控制功能，控制用户组、用户对系统功能和用户数据的访问；应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

第十七条 软件容错机制。信息系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式符合系统设定要求。在系统发生故障时，应确保部分基本功能可用。

第六章 数据安全及备份恢复

第十八条 采用密码技术确保信息系统重要数据在传输过程中的完整性、在系统中的可用性以及符合特定要求的保密性。

第十九条 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据传输方法。

第二十条 信息系统应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

第二十一条 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。

第二十二条 根据信息系统的备份技术要求，制定相应的应急预案与灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新。

第七章 安全管理措施

第二十三条 信息系统运行期间应根据《南通师范高等专科学校网络与信息安全人员管理办法》配备信息系统安全运维所需的管理人员并加强人员管理。

第二十四条 信息系统投入运行、网络系统接入和重要资源的访问等关键活动应进行审批、记录。

第二十五条 应对网络设备、主机系统和信息系统进行定期安全漏洞检测评估，及时修补漏洞，整改加固安全防护措施。

第二十六条 应定期对信息系统运行日志和审计数据进行分

析，以便及时发现异常情况，采取措施调整纠正。

第二十七条 信息系统应使用符合国家密码管理规定的密码技术和产品。

第二十八条 信息系统重大变更，应制定相应的变更方案，报主管部门审批后方可实施变更，并在实施后向相关业务人员通告。

第二十九条 信息系统运行期间如发生信息安全事件，应按照《南通师范高等专科学校网络安全管理暂行办法》《南通师范高等专科学校网络安全事件报告和处置管理办法》规定进行报告处置。

第八章　附　则

第三十条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第三十一条 本办法自公布之日起实施。

附件 8

南通师范高等专科学校信息系统终止管理办法

第一章 总　则

第一条 信息系统随着其生存环境的变化，具有产生、发展、成熟、终止的生存循环周期。

第二条 对信息系统的安全保障管理贯穿于其整个生存周期的各个阶段。

第二章 终止运行申报与审批

第三条 任何现有信息系统或子系统、信息系统设备需要终止运行时，应由使用者或管理者提出申请，说明原因及采取的保护措施，经过主管部门领导审批才能正式终止运行，具体程序按照有关主管部门的规定执行。（申报表见附件）

第四条 按照信息系统等级保护要求已定为三级及以上的信息系统的终止，由学校网络安全与信息化领导小组负责审批，二级信息系统终止由信息化工作办公室审批，其它系统由使用部门自行审批。校外相关部门部署信息系统的子系统的终止，具体程序按照信息系统主管部门的规定执行。

第三章　终止运行的信息保护

第五条 信息系统终止运行前，使用者或管理者应根据信息系统资产清单、硬件设备清单、存储介质清单处理信息转移、暂

存和清除，设备迁移或废弃，存储介质的清除或销毁等活动，记录处理过程与结果。信息系统设备若改变用途，应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。存储介质包括磁盘、磁带和纸质文档。

第六条 二级及以上信息系统终止运行时，应对其设备进行不可恢复的数据清除，如果存储设备损坏则必须采取销毁措施。

第七条 对信息系统数据和设备进行以上必要的处理后，经系统技术负责人认可才能正式终止运行，并形成文档备案。

第四章　附　则

第八条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第九条 本办法自公布之日起实施。

附表：南通师范高等专科学校信息系统终止申报审核表

附表

南通师范高等专科学校信息系统终止申报审核表

系统名称：_____ 申请日期：　　年　月　日

信息系统保护级别	_____级
信息系统主要构成	
信息系统主要功能	
信息系统终止原因	
使用单位审核意见	负责人签字：
信息化工作办公室 审核意见	负责人签字：
网络安全与信息化 领导小组审核意见	负责人签字：

附件 9

南通师范高等专科学校
信息安全事件报告和处置管理办法

第一章　总　则

第一条 信息安全事件定义。信息安全事件是指由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害或对社会造成负面影响的事件。

第二条 信息安全事件的分类。根据信息安全事件性质分为信息内容安全事件和信息技术安全事件两大类。信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件。除信息内容安全事件外的其它信息安全事件为信息技术安全事件。

第二章　信息安全事件分级

第三条 根据信息安全事件所危害信息系统的重要程度不同、损失程度不同以及社会影响程度不同，对信息安全事件进行分级管理。

第四条 信息系统的重要程度划分。信息系统安全等级保护定级为三级的信息系统为特别重要信息系统，定级为二级信息系统为重要信息系统，其它为一般信息系统。

第五条 信息系统的损失程度划分。根据信息安全事件对信息系统业务信息和系统服务能力的破坏程度划分信息系统损失

程度。造成信息系统大面积瘫痪业务全面中断、系统关键数据遭到严重破坏、恢复系统运行和消除负面影响的代价非学校能够承受的为特别重大系统损失；造成系统长时间中断或局部瘫痪、业务处理能力受到极大影响、系统关键数据遭到破坏、恢复系统运行和消除负面影响的代价较大的为重大系统损失；造成系统暂时中断，业务处理能力受到影响、系统重要数据遭到破坏，恢复系统运行和消除负面影响的代价不大的为一般系统损失。

第六条 信息系统的社会影响程度划分。极大威胁国家安全、引起社会动荡、对经济建设有极其恶劣的负面影响、或者严重损害公众利益的为特别重大社会影响；威胁到国家安全、引起社会恐慌或对经济建设有重大负面影响、或损害到公众利益的为重大社会影响；可能影响到国家安全、社会秩序、经济建设或公众利益，或对学校及师生利益造成损害或影响学校工作秩序的为一般社会影响。

第七条 信息安全事件等级分为四级：特别重大事件（I级）、重大事件（II级）、较大事件（III级）、一般事件（IV级）。

（一）特别重大事件（I级）：对特别重要信息系统造成特别重大损失，或造成特别重大社会影响。

（二）重大事件（II级）：对特别重要信息系统造成重大损失、或对重要信息系统造成特别重大损失、或造成重大社会影响。

（三）较大事件（III级）：对重要信息系统造成一般损失、或对一般信息系统重大损失、或造成一般社会影响的。

（四）一般事件（IV级）：对一般信息系统产生一般系统损失且不造成社会影响的。

第三章 信息安全事件报告与处置

第八条 任何人发现发生信息安全事件时应立即报告学校信息化工作办公室，并根据实际情况及时取证。信息化工作办公室接到举报并初步核实后立即报告领导小组，领导小组根据事件危害程度初步判定安全事件等级并启动应急响应预案，并第一时间向上级主管领导汇报。

第九条 初判为 I 级、II 级安全事件的最终等级由学校网络安全与信息化领导小组核定。I 至 III 级安全事件的报告与处置分为三个步骤：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。

（一）事发紧急报告与处置

除信息化工作办公室按应急响应预案进行事件处置外，领导小组了解信息安全事件基本情况后以口头通讯的方式将相关情况通报至市网信办，如出现新的重大情况应及时补报。涉及人为主观破坏事件应同时报告当地公安机关。情况通报内容包括：（1）时间地点；（2）简要经过；（3）事件类型与分级；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

（二）事中情况报告与处置

1. 事中情况报告应在安全事件发现后 8 小时内以书面报告的形式进行报送，信息技术安全事件报送内容和格式见附件 1，信息内容安全事件报送内容和格式见附件 3。

2. 事中情况报告由学校领导小组组织相关部门共同编写，由领导导小组负责人审核后签字并加盖公章，信息技术安全事件报告报送市网信办。

3. 安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为主观破坏的安全事件应积极配合公安部门开展调查。

（三）事后整改报告与处置。

1. 事后整改报告应在安全事件处置完毕后5个工作日内以书面报告的形式进行报送，信息技术安全事件报送内容和格式见附件2，信息内容安全事件报送内容和格式见附件4。

2. 事后整改报告由学校领导小组组织相关部门共同编写，由领导小组负责人审核后签字并加盖公章后报市网信办。

3. 信息安全事件事后处置包括：进一步总结事件教训，研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合公安部门开展调查。根据事件的影响程度开展责任追究。

第十条 IV级安全事件在根据应急响应预案处置完毕后7天内将整改报告报送市网信办。

第十一条 预警类信息的报告与处置。预警类信息包括校内网络病毒、木马集中爆发，校内主机遭受入侵或发生向外攻击等事件。学校要按时、按要求完成有关信息安全部门或教育部通报的预警类信息的处置工作，并按要求形成书面报告，按预警信息类型报送市网信办或相关部门。

第十二条 人事变更报告。学校信息化工作主管领导、主管部门、联络员、联络方式发生变更的，应及时报送市网信办。

第十三条 相关配套机制。学校信息化工作办公室制定安全

值守制度，设立24小时值班电话，做到安全事件早发现、早报告、早控制、早解决。学校信息化工作办公室应建立健全学校安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练。

第十四条 问责制度。学校网络与信息安全相关工作处室及成员应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，将追究相关人员责任。

第四章 附　则

第十五条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第十六条 本办法自公布之日起实施。

附件：1．信息技术安全事件情况报告

2．信息技术安全事件整改报告

3．信息内容安全事件情况报告

4．信息内容安全事件整改报告

附件 1

信息技术安全事件情况报告

单位名称：（需加盖公章）　　事发时间：_____年___月___日___分

联系人姓名		手机	
		电子邮箱	
事件分类	□ 有害程序事件　□ 网络攻击事件 □ 信息破坏事件　□ 设备设施故障 □ 灾害事件　　□其他_____		
事件分级	□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1. 系统名称：_____ 2. 系统网址和 IP 地址：_____ 3. 系统主管单位/部门：_____ 4. 系统运维单位/部门：_____ 5. 系统使用单位/部门：_____ 6. 系统主要用途：_____ _____ 7. 是否定级 □是　□否，所定级别：_____ 8. 是否备案 □是　□否，备案号：_____ 9. 是否测评 □是　□否 10. 是否整改 □是　□否		
事件发现与处置的简要经过			
事件初步估计的危害和影响			
事件原因的初步分析			
已采取的应急措施			
是否需要应急支援及需支援事项			
安全负责人意见（签字）			
主要负责人意见（签字）			

附件 2

信息技术安全事件整改报告

单位名称：（需加盖公章）　　报告时间：_____年___月__日

联系人姓名		手机	
		电子邮件	
事件分类	☐ 有害程序事件　☐ 网络攻击事件 ☐ 信息破坏事件　☐ 设备设施故障 ☐ 灾害事件　　☐其他_____		
事件分级	☐Ⅰ级　☐Ⅱ级　☐Ⅲ级　☐Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统网址和 IP 地址：_____ 3.系统主管单位/部门：_____ 4.系统运维单位/部门：_____ 5.系统使用单位/部门：_____ 6.系统主要用途：_____ _____ 7.是否定级 ☐是　☐否，所定级别：_____ 8.是否备案 ☐是　☐否，备案号：_____ 9.是否测评 ☐是　☐否 10.是否整改 ☐是　☐否		
事件发生的最终判定原因（可加页附文字、图片以及其他文件）			
事件的影响与恢复情况			
事件的安全整改措施			
存在问题及建议			
安全负责人意见（签字）			
主要负责人意见（签字）			

附件 3

信息内容安全事件情况报告

单位名称：（需加盖公章）　事发时间：_____年___月__日__分

联系人姓名		手机	
		电子邮箱	
事件分级	□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1. 系统名称：_____ 2. 系统网址和 IP 地址：_____ 3. 系统主管单位/部门：_____ 4. 系统运维单位/部门：_____ 5. 系统使用单位/部门：_____ 6. 系统主要用途：_____ a) _____ 7. 是否定级 □是　□否，所定级别：_____ 8. 是否备案 □是　□否，备案号：_____ 9. 是否测评 □是　□否 10. 是否整改 □是　□否		
事件发现与处置的简要经过			
事件初步估计的危害和影响			
事件原因的初步分析			
已采取的应急措施			
是否需要应急支援及需支援事项			
安全负责人意见（签字）			
主要负责人意见（签字）			

附件 4

信息内容安全事件整改报告

单位名称：（需加盖公章）　　报告时间：_____年___月__日

联系人姓名		手机	
		电子邮件	
事件分级	□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级		
事件概况			
信息系统的基本情况（如涉及请填写）	1.系统名称：_____ 2.系统网址和 IP 地址：_____ 3.系统主管单位/部门：_____ 4.系统运维单位/部门：_____ 5.系统使用单位/部门：_____ 6.系统主要用途：_____ _____ 7.是否定级 □是　□否，所定级别：_____ 8.是否备案 □是　□否，备案号：_____ 9.是否测评 □是　□否 10.是否整改 □是　□否		
事件发生的最终判定原因（可加页附文字、图片以及其他文件）			
事件的影响与恢复情况			
事件的安全整改措施			
存在问题及建议			
安全负责人意见（签字）			
主要负责人意见（签字）			

附件 10

南通师范高等专科学校
校园信息化文档管理办法

第一章　总　则

第一条 为规范学校信息化文档管理工作，提高信息化文档管理水平，实现学校信息化文档管理工作的规范化、制度化，根据《电子文件归档与管理规范》GB/T18894-2002、《南通师范高等专科学校档案管理办法》等有关管理规定并结合实际工作，特制定本办法。

第二条 本办法中的信息化文档专指校园网及各类信息系统建设、运行、使用、终止过程中产生的具有保存价值的纸质或电子的各种文档与历史数据。

第三条 信息化文档与信息系统密切相关，信息化文档管理是信息系统安全管理的重要组成部分。信息化文档按照“谁主管、谁负责”的原则由信息系统主管部门进行管理，各单位应指定人员负责本单位信息化文档的收集、整理、归档等工作。

第二章　信息化文档的归档、整理

第四条 校园信息化文档归档范围包括：校园网及各类信息系统的建设方案、投标说明书、采购与维护服务合同、立项与设计报告、设备资料、配置文件、需求说明书、会议纪要、运行维护日志、验收材料、管理手册、安全检查数据、系统定级与测评报告、管理制度、管理部门文件等。保存形式分纸质文档和电子文档。

第五条 校园信息化文档收集要求：1．主要收集各式文件和合同，收集时需落实必要的签字手续，明确公文拟稿、核稿、签发等环节的责任者。2．归档材料应当质地优良、书绘工整、声像清晰，符合有关规范和标准的要求。3．电子文件归档可依照电子文件归档与管理规范的规定实施，采用“实时捕获”、“远程归档”和“物理归档”三种方式。电子文件归档操作一般由形成部门和单位完成；

第六条 各类信息化文档中对学校和社会有长期保存价值的，需按照档案管理相关规定送学校档案馆存档。应定期对过期或失去保存价值的信息化文档进行清理。

第三章　信息化档案的管理和利用

第七条 信息化档案管理人员依据《高等学校档案实体分类法》对文档进行分类、编号、入藏。

第八条 信息化档案管理人员应落实防火、防盗、防虫、温度湿度控制等安全措施，确保档案安全。

第九条 信息化档案管理人员要建立档案统计、检查制度，定期对档案的收集、整理、保管、利用情况进行检查和统计。

第十条 对保管期限已满、已失去保存价值的档案，信息化档案管理人员应提出申请，经有关部门鉴定并登记造册批准后，予以销毁。未经鉴定和批准，不得销毁任何档案。

第四章 附　则

第十一条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第十二条 本办法自公布之日起实施。

附件 11

南通师范高等专科学校
计算机信息系统密码安全管理办法

第一章 总　则

第一条 为加强学校计算机信息系统密码的安全管理，提高计算机信息系统密码安全管理规范化、制度化水平，完善信息安全管理体系，特制定本管理办法。

第二条 本校计算机信息系统用户密码的安全管理适用本规定。

第三条 计算机信息系统密码是指用户在登录计算机系统过程中,用于验证用户身份的字符串,也称为计算机系统用户口令,主要为静态口令、动态口令等。静态口令一般是指在一段时间内有效，需要用户记忆保管的口令。动态口令一般是指根据动态机制生成的、一次有效的口令。计算机系统用户口令主要包括：主机系统、数据库系统、网络设备、安全设备等系统用户口令；前端计算机系统用户口令；应用系统用户口令；桌面计算机系统用户口令。

第四条 计算机信息系统密码的安全管理遵照统一规范、重在意识、技术控制与管理措施相结合的原则。

第五条 计算机信息系统密码持有人应保证密码的保密性，不应将密码记录在未妥善保管的笔记本以及其他纸质介质中(密码信封除外)，严禁将密码放置在办公桌面或贴在计算机机箱、

终端屏幕上，同时严禁将计算机信息系统用户密码借给他人使用。任何情况下不应泄漏计算机信息系统用户密码，一旦发现或怀疑用户密码泄漏，应立即更换。

第六条 计算机信息系统用户密码必须加密存储在计算机系统中，严禁在网络上明文传输计算机信息系统用户密码，在用户输入密码时，严禁在屏幕上显示密码明文，严禁计算机信息系统输出密码明文（密码信封除外）。

第七条 计算机信息系统用户密码持有人应保证密码具有较高安全性。选择使用安全强度较高的密码，不应使用简单的代码和标记，禁止使用重复数字、生日、电话号码、字典单词等容易破译的计算机信息系统用户密码。

第八条 任何人不得利用盗取、猜测、窥视、破解等非法手段获取他人计算机系统用户密码，盗用他人访问权限，威胁信息系统安全。

第九条 同一信息系统相同访问权限的用户应具有一致的密码安全要求。

第十条 具有登录计算机系统权限的用户必须设置用户密码或其它验证用户身份的方式，严禁不验证用户身份直接登录信息系统。

第二章　管理职责及权限

第十一条 重要核心设备（如核心交换机、防火墙、服务器等）应有专人统一管理，重要主机系统、核心网络设备、安全设备等超级用户以及重要系统中具有关键访问权限用户的密码，采

取两人互备制管理。

第十二条 计算机用户密码（专人管理的口令除外）持有人负责所持计算机用户密码在使用过程中的保密，负责设置、保存、更换计算机用户密码，负责密码自身的安全强度。

第十三条 系统管理（维护）人员、网络和安全设备管理（维护）人员负责启用计算机系统、网络和安全设备的密码安全管理相关功能；负责删除计算机系统、网络和安全设备多余用户和密码。

第十四条 应用系统开发人员应负责实现应用系统支持密码安全管理的相关功能和机制。

第十五条 计算机信息系统密码采用授权使用机制，非系统管理员因工作需要使用系统管理密码时，由系统管理员设置临时密码，使用完毕后修改密码，并对授权行为进行记录。

第十六条 涉及密码人员离职或发现密码泄露迹象及时修改密码，修改密码不能使用原密码。

第三章　密码（口令）基本安全要求

第十七条 计算机用户密码基本要求由密码长度、密码字符复杂度、密码历史，密码最长有效期组成：

（一）密码最小长度：8 位；

（二）密码字符组成复杂度：密码由数字、大小写字母及特殊字符组成，且至少包含其中两种字符（动态口令除外）；

（三）密码历史：修改后的密码至少与前 10 次密码不同；

（四）密码最长有效期限：30/60/90 天，可根据系统重要

性和用户权限采取不同的有效期。

第四章　主机系统、网络和安全设备用户密码安全要求

第十八条 系统用户密码主要包括主机系统、网络设备、安全设备等系统用户密码。

第十九条 主机系统、网络设备、安全设备等应启动密码管理相关功能、机制，满足第三章密码基本安全要求，对于原有系统不支持或不具备相关技术功能、机制的，必须逐步建立、完善相应的安全管理制度措施，弥补技术机制上的不足。

第二十条 主机系统、网络设备、安全设备等的超级用户密码以及重要系统中具有关键访问权限用户的密码应由专人设置与管理（一人设置，至少两人管理），超级用户密码应存档登记。

第二十一条 主机系统超级用户密码，网络设备、安全设备超级用户密码以及具有修改配置权限用户的密码应记录密码使用相关信息，至少包括：设备名称、用户名称、密码启用时间、密码更换时间、密码使用者等内容。

第二十二条 主机系统、网络设备、安全设备等超级用户以及其它用户密码的最长有效期应符合第三章密码基本要求。

第二十三条 当系统用户密码持有人岗位调整时，原则上应删除其使用的用户，因工作需要，需要保留原用户的，必须及时更换系统用户对应的密码，严禁使用原密码登录系统。

第二十四条 对于主机系统、网络设备、安全设备的用户密码以及具有系统配置权限的用户，可根据实际情况使用动态口令。

第五章　应用系统用户密码安全要求

第二十五条 应用系统用户密码是指只用于访问应用系统的用户密码，密码对应的用户为应用系统用户，在操作系统中并不存在相应用户。

第二十六条 应用系统在开发过程中必须同步实现满足计算机系统用户密码基本要求的机制和功能，通过技术手段实现安全管理要求。对于正在运行的、没有达到第三章密码基本要求的计算机系统的改造或升级，可结合具体情况稳步开展。同时，必须采用相应的管理措施，加强计算机系统用户密码的安全管理，保障应用系统的安全。

第二十七条 应用系统用户必须设置密码或使用其它身份认证方式，严禁不验证用户身份访问应用系统（对于信息网站中只浏览网页的用户，可不设置密码）。

第二十八条 应用系统必须提供用户密码更换机制，严禁应用系统代码中包含用户密码。

第二十九条 应用系统用户的密码应定期更换，密码最长有效期可根据应用系统的重要程度和用户的权限设定，同时符合第三章密码基本安全要求的最长有效期范围规定。

第三十条 对于应用系统的用户密码，可根据实际情况使用动态口令。

第六章　桌面计算机系统用户密码安全要求

第三十一条 桌面计算机系统用户密码主要是指用户使用计算机系统的登录密码，如台式微机、笔记本电脑及其它个人计算

设备的用户密码。

第三十二条 桌面计算机系统用户密码包括设备启动登录密码、操作系统登录密码、屏幕保护密码等。

第三十三条 桌面计算机系统用户密码应定期更换（操作系统不具有此功能除外）。

第七章　检查和监督

第三十四条 应定期对计算机系统用户密码安全管理的情况进行检查，包括岗位和职责情况、密码登记变更情况、密码安全管理相关功能及其启用情况、多余用户密码删除情况、密码安全管理规定的落实和执行情况。

第三十五条 对于安全检查中发现的问题和隐患，各计算机系统主管和使用部门及密码持有人要进行认真整改。对于违反本安全管理办法造成严重后果的，将上报学校信息安全办公室追究责任，情节严重触犯法律的将移交司法机关。

第八章　附　则

第三十六条 本办法由网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第三十七条　本办法自公布之日起实施。

附件 12

南通师范高等专科学校
计算机病毒防治管理办法

第一条 为加强校园计算机应用安全保障，预防和治理计算机病毒，保护计算机信息系统安全，根据国务院《中华人民共和国计算机信息系统安全保护条例》、公安部《计算机病毒防治管理办法》的规定，结合学校实际情况，制定本办法。

第二条 本办法中的计算机包括终端计算机、笔记本电脑、服务器、存储设备、高性能运算设备以及配套的设备设施等；计算机病毒，是指编制或者在计算机程序中插入的破坏计算机系统功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码（包括恶意软件和代码）。

第三条 本办法适用于校园范围内所有使用计算机的单位和个人。

第四条 信息化工作办公室总体指导校园计算机病毒防治管理工作，各单位具体负责本单位内的计算机病毒防治管理工作。

第五条 任何单位和个人不得制作、传播计算机病毒。

第六条 计算机信息系统的使用单位在计算机病毒防治工作中应当履行下列职责：

（一）采取计算机病毒安全技术防治措施，指定专人负责管理；

（二）定期对计算机设备进行计算机病毒检测、清除工作，

做好检测、清除记录；

（三）对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训；

（四）发现计算机病毒应及时隔离被感染机器；对于外来磁盘和硬盘应查杀病毒后才允许使用；

（五）使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品，并及时更新版本和特征库；

（六）对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向学校信息化工作办公室、公安机关报告，并保护现场。

第七条 任何单位和个人在从计算机信息网络上下载程序、数据或者购置、维修、接入计算机设备时，应当进行计算机病毒检测。

第八条 联网的计算机如果感染计算机病毒，为避免计算机病毒通过网络传播扩散，信息化工作办公室可采取应急断网隔离措施。

第九条 计算机病毒的清除原则

（一）清除病毒之前，注意备份所有重要数据，以防遭病毒破坏或误删除而遗失。

（二）清除病毒时，应保证整个清查病毒过程在无毒或安全防护环境下进行，以防病毒重新感染已清除病毒的文件或其他文件。

（三）清除病毒后，应采取相应的安全防护技术措施，如安装防病毒产品、更新病毒查杀特征库、修复系统漏洞等。

第十条 通过网络进行电子邮件或文件传输，应及时对传输媒体进行病毒检测，接收到邮件时也要及时进行病毒检测，以防止计算机病毒的传播。

第十一条 对违反本办法的行为，将根据所造成危害影响程度追究责任，上报学校信息化工作办公室，情节严重的移交司法机关处置。

第十二条 本办法由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

第十三条 本办法自公布之日起实施。

附件 13

南通师范高等专科学校网站建设与管理办法

为规范学校校园网站建设，加强学校校园网站信息发布和网络信息安全管理，提高学校网站建设与管理工作水平，保障学校信息化可持续发展，根据教育部、江苏省教育厅有关通知精神，结合学校信息化工作实际，制定本办法。

第一章　总　则

第一条 校园网站指网站域名对应 IP 地址为南通师范高等专科学校校园网 IP 范围的所有网站，包括以南通师范高等专科学校名义使用校外域名的网站。

第二条 校园网站建设与管理的总体目标是建立健全学校网站建设与管理的组织体系，指导和促进校园网站建设与信息发布工作规范、有序开展，保障学校信息安全及学校信息化可持续发展。

第三条 校园网站建设与管理的总体原则是“谁主管、谁负责，谁主办、谁负责”。

第二章　校园网站建设与管理组织体系

第四条 学校成立网络安全与信息化领导小组，每年须将校园网站建设与管理作为工作的重要内容加以研究和部署。学校成立校园网站建设与管理工作小组，负责学校日常校园网站建设与管理工作的组织实施。

第五条 在学校网络安全与信息化领导小组的指导下，学校党委组宣部负责学校中文主网站和学校新闻网站主页栏目、新闻、公告等内容的组织、审核、发布及管理，接受处理校内各学院、部门和直属单位新建网站的审批、备案及有害信息举报；对外合作交流处负责学校英文网站内容组织、审核、发布及校园网站外文信息发布的管理；信息化工作办公室负责校园网络及学校中英文主网站技术安全日常管理工作，并为校内各单位网站建设提供统一建站系统维护和其它必要的技术支持。

第六条 学校各单位是本单位主办的各种校园网站的主管单位，须明确一名领导分管本单位网站建设与管理工作，并指定一名在岗人员担任本单位网站管理员，具体负责网站信息安全、数据维护、内容更新、实名注册、实名登录等工作。各单位主要负责人是本单位网站建设与管理的第一责任人。

第三章　校园网站建设

第七条 各单位拟新建校园网站，须填写《南通师范高等专科学校校园网站建设申请表》，由所在单位主要负责人签署意见，并报学校党委组宣部对所建网站栏目和内容审批通过后，方可开始立项建设。

第八条 为保障校园网站系统安全，实现校园网站信息的共建共享，由信息化工作办公室提供统一的建站系统供各单位新建网站使用，建站系统包含统一的网站模板管理、网站内容维护、发布、审核等功能，网站主办单位不得另行开发相关网站后台管理程序。现有未使用建站系统的校园网站，主办单位应根据信息

化工作办公室安排，逐步迁移到统一的建站系统中。

第九条 所有校园网站均须明确主管、主办单位及网站负责人和联系人，并由各主管单位将学校党委组宣部审批后的《南通师范高等专科学校学校网站建设申请表》报送信息化工作办公室备案。

第十条 校园网站使用校徽、校名、校训等内容须严格按照《南通师范高等专科学校视觉形象识别系统》规定进行，网站页面设计制作要美观大方、简洁实用。

第十一条 新建校园网站在上线启用前，应经过安全检测，签署信息安全责任承诺书，检测报告和承诺书应交现代教育技术中心备案。

第四章　校园网站信息发布管理

第十二条 学校任何单位和个人不得在校园网站上发布涉密信息和《互联网信息服务管理办法》所禁止的有害信息，各单位须按照校园网站建设与管理的总体原则，加强对本单位所建网站信息发布和信息安全的管理，并及时更新网站内容。

第十三条 校园网站仅限发布公益性、共享性的网络信息，学校、企业等如依托校园网站进行经营性互联网信息服务，须经学校产业主管单位同意后，按《互联网群组信息服务管理规定》到主管部门办理手续，并将相关批件报学校信息化工作办公室备案。

第十四条 校园网站如需开设论坛等实时互动版块，须由主管单位报学校党委组宣部批准，并严格执行互动版块实名注册

制。

第五章　校园网站安全事件管理

第十五条 校园网站安全事件是指由于自然或人为的原因对校园网站信息系统或信息内容造成危害，对学校或社会造成负面影响的事件。校园网站安全事件管理包括应急预案管理、安全事件报告与协查、安全事件处置等。

第十六条 校园网站安全事件由学校网络安全工作组根据《南通师范高等专科学校校园网安全管理办法》《南通师范高等专科学校信息安全事件报告和处置管理办法》等规定研究处置。

第十七条 学校任何单位和个人发现校园网站出现涉密信息、有害信息等信息安全事件后，应立即报告党委组宣部和信息化工作办公室备案处理，信息化工作办公室须及时对有害信息进行备份、删除，必要时对事发网站进行关闭，同时上报学校网络安全工作组对责任单位和个人进行追查、处置。

第六章　考核与奖惩

第十八条 学校校园网站建设与管理工作小组根据校园网站建设与管理情况，并结合上级部门安排，不定期开展学校校园网站建设与信息安全管理检查评比工作，并对校园网站建设与管理工作成绩突出的单位和个人给予表彰奖励。

第十九条 对于玩忽职守或有意危害造成校园网站安全事件的，学校将根据其损失情况和不良影响的程度，对网站主管（办）单位负责人和当事者进行追责，构成犯罪的移送司法部门处理。

第七章　校园网站关停与启用

第二十条 校园网站因过期、改版等原因停止更新与服务的，主管、主办单位应主动向学校信息化工作办公室申请关停并履行相关手续。

第二十一条 存在严重安全漏洞等隐患的校园网站，主管、主办单位应在收到相关检测报告和整改通知后，在指定期限内停止网站服务，落实整改措施，及时反馈进展情况。如未能按时完成或无法完成整改，为保障校园网整体安全，现代教育技术中心在上报学校网络安全工作组后一周内实施强制关停管制。

第二十二条 在网站安全整改期间，如因特殊业务需要临时启用，网站主办方应签署信息安全责任承诺书，指定临时启用的起止时间，自行做好防护措施。按时完成整改的网站，经安全检测验证核实后，可重新启用。

第八章　附　则

第二十三条 本办法由学校网络安全与信息化领导小组组织制定，学校组织宣传部解释。

第二十四条　本办法自公布之日起实施。

附件 14

南通师范高等专科学校
教育移动应用管理制度（试行）

一、总体要求

为深入贯彻落实《教育部等八部门关于引导规范教育移动互联网应用有序健康发展的意见》（教技函〔2019〕55 号）和《教育部办公厅关于印发教育移动互联网应用程序备案管理办法》（教技厅〔2019〕3 号）部署要求，扎实做好南通师范高等专科学校教育移动互联网应用程序（以下简称教育移动应用）备案和管理工作，特制定本制度。

一、教育移动应用是指服务于学校教育教学和广大师生工作生活的管理服务类教育移动应用，包括：各单位自主开发、自主选用和上级部门要求使用的教育移动应用（基于 Android 系统和 iOS 系统的独立 APP 应用，以及小程序和公众号、企业号）。

二、南通师范高等专科学校教育移动应用归口管理部门为信息化工作办公室，其他各单位应按照“谁主管谁负责、谁开发谁负责、谁选用谁负责”的原则，建立健全教育移动应用管理责任体系，切实维护广大师生、家长和其他用户切身利益。

二、整合共享制度

各单位在开发、选用教育移动应用时应首先遵从整合共享制度。

原则上面向全校学生提供办事服务的整合成一个应用，面向教职工提供管理服务的整合成一个应用，面向校友及社会公众提供服务的整合成一个应用。鼓励各单位积极提供移动端服务，以整合的形式将移动端应用作为服务整合到学校的统一移动应用，对于不满足或不支持对接的移动应用，归口管理部门原则上不予以立项和验收。各单位在选用或开发教育移动应用时，应向信息化工作办公室提供全量数据接口以及数据库详细文档（包括表名、字段含义、表间关系等），同时应满足《南通师范高等专科学校公共信息标准编码规则》要求，所有教育移动应用使用个人基本信息应从数据中心基础数据库中共享，不得向用户重复采集个人基本信息。

信息化工作办公室负责在教育部、省教育厅关于教育移动应用治理的相关精神指导下，结合学校实际情况，对各单位管理服务类教育移动应用和小程序、公众号的数量进行深度治理和整合。

三、论证制度

各单位规划自行开发或选用的教育移动应用前，应经由信息化工作办公室组织立项、审核、论证通过后再进行开发或选用工作。

对于要求统一使用和大范围采集个人信息的教育移动应用，应在决策制度要求的基础上组织科学性、伦理性、安全性等多个方面的论证。

四、开发制度

各单位开发教育移动应用前应经由信息化工作办公室立项。各单位内设机构及下属部门不得擅自开发未经审核、立项的教育移动应用。

教育移动应用的开发应符合国家、教育部、行业、学校等制定的相关标准和制度。对于各单位自主开发的教育移动应用，应按照《网络安全法》和网络安全等级保护 2.0 的要求，完成所有自主开发教育移动应用的定级备案和测评整改。

五、选用和备案制度

各单位应规范教育移动应用的选用管理。

教育移动应用的选用应符合国家、教育部、行业、学校等制定的相关标准和制度。对于选用的教育移动应用，教育应用提供者应严格按照 ICP 备案标准和等级保护备案标准，对教育移动应用进行 ICP 备案和等级保护备案，并及时在公共服务体系上传、更新信息。

各单位选用教育移动应用应报由信息化工作办公室审核备案。单位内设机构及下属单位不得擅自选用未经审核、立项的教育移动应用，不得选用未完成提供者备案的教育移动应用。

六、决策制度

各单位应建立教育移动应用的决策机制。各单位要建立教育移动应用重大事项的决策机制，具体实施办法参照信息化建设项目立项决策机制。

对要求统一使用和大范围采集个人信息的教育移动应用，除

关系到国家安全、社会稳定、学校和师生的人身安全以外，应在履行立项流程和审核程序的原有基础上充分征求师生用户群的意见，并经南通师范高等专科学校网络安全和信息化领导小组审定同意。

七、退出机制

超过半年未更新的教育移动应用，不满足《南通师范高等专科学校教育移动应用管理制度》管理要求的教育移动应用，应予以整合、关停。

八、个人信息收集制度

对于各单位自主开发的教育移动应用，应对个人信息收集行为进行规范和管理，制定内部个人信息安全管理制度和操作规程，设置专门安全负责人，并对该负责人和关键岗位的人员进行安全背景审查，落实网络安全保护责任。原则上大范围采集个人信息的教育移动应用应通过移动应用个人信息安全认证，规范数据安全生命周期的管理。

对于选用的教育移动应用，应用提供者必须履行下列信息保护义务：

一、对教育移动应用运营过程的数据严格保密，建立健全用户信息保护制度；

二、不得违反法律、行政法规的规定，以及与选用方或用户的约定，收集、使用和处理其保存的个人信息；

三、不得泄露、篡改、毁损平台上的个人信息；未经用户同

意，不得向任何组织或个人提供用户个人信息。但下述二种情形除外：第一、经过处理无法识别特定个人且不能复原的；第二、根据法律、法规和规范性文件的强制性规定，或应司法或行政机关要求提供用户个人信息的。

四、应当采取技术措施和其他必要措施，确保平台上的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，并按照规定及时告知用户、选用方和向有关主管部门报告；

五、若发现被选用的教育移动应用不当收集、使用用户信息或业务信息，或者发现收集、存储的相关信息有错误的，学校有权要求乙方予以删除或更正，应用提供者应予立即删除或更正。

九　附　则

本制度由学校网络安全与信息化领导小组组织制定，学校信息化工作办公室解释。

本制度自公布之日起实施。