信阳师范大学文件

校发〔2025〕66号

关于印发《信阳师范大学
网络与信息安全管理办法》的通知

各单位：

《信阳师范大学网络与信息安全管理办法》已经学校研究同意，现印发给你们，请认真组织学习，贯彻落实。

信阳师范大学

2025 年 9 月 25 日

信阳师范大学网络与信息安全管理办法

第一章　总　　则

第一条 为深入贯彻总体国家安全观，全面规范学校网络与信息安全管理，切实提高网络安全防护能力和水平，保障我校信息化工作安全、可靠、有序进行，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规和上级有关工作要求，结合我校实际，制定本管理办法。

第二条 本办法所称网络与信息安全管理是指通过采取必要措施，保护学校网络与信息化建设基础设施、信息系统及信息数据的安全，使其不受到破坏、篡改、泄露等。

第三条 学校按照“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，建立健全网络与信息安全责任体系，逐级落实网络与信息安全管理责任。各单位及全体师生应依照本办法要求及学校相关标准规范履行网络与信息安全的责任和义务。

第四条 任何单位和个人不得利用学校网络和信息系统泄露国家或学校秘密、危害国家或学校安全，不得侵犯国家、集体和个人的合法权益，不得从事违法犯罪和违纪违规等活动。

第二章　组织机构与职责

第五条 学校设立网络安全与信息化领导小组（以下简称“领导小组”），负责贯彻落实上级关于网络信息安全工作的部署和要求，加强学校网络与信息安全工作的领导，统筹指导

网络与信息安全建设，定期召开网络与信息安全工作会议，研究处理重大网络与信息安全事件。

第六条 网络安全和信息化领导小组办公室（以下简称“网信办”）是网络安全和信息化领导小组常设办事机构，其主要职责包括：

（一）负责学校网络安全和信息化领导小组日常事务工作，定期向领导小组汇报网络与信息安全工作，提出工作建议；

（二）组织落实学校网络安全和信息化领导小组的各项决议与工作部署，督促检查各单位网络安全和信息化工作落实情况；

（三）研究制定学校网络安全和信息化工作发展规划、工作计划、规章制度和标准规范，统筹协调学校网络安全和信息化建设推进实施工作；

（四）负责协调处理学校网络安全重大突发事件有关应急工作；

（五）组织开展学校网络安全和信息化建设宣传普及和教育培训等工作；

（六）完成网络安全和信息化领导小组交办的其它工作。

第七条 学校各单位是本单位网络与信息安全工作的责任主体，单位主要负责人是本单位网络与信息安全工作第一责任人。各单位须明确本单位网络安全与信息化负责人和联络员，负责管理和协调本单位的网络安全和信息化工作。各单位主要职责包括：

（一）负责本单位网络与信息安全管理工作，配合学校开展

网络与信息安全建设、检查、整改及培训与宣传工作；

（二）落实学校网络与信息安全管理制度，制定本单位相关管理制度、工作规范及应急预案；

（三）负责建立健全本单位的网络与信息安全责任制，明确岗位及人员的安全责任；

（四）负责本单位业务服务器、网站、信息系统及数据的安全建设、运行、维护和监管；

（五）做好本单位网络信息发布内容的审核和监控；

（六）配合学校处理网络与信息安全事件，积极协助有关部门开展安全调查取证工作等。

第三章　校园网络安全管理

第八条 校园网络是指学校所有校区范围内连接各种信息系统及信息终端的计算机网络、公用通信网络和专用通信网络，其中计算机网络和公用通信网络统一归口网络信息中心管理，专用通信网络由其建设单位负责管理。

第九条 校园网络的规划建设、运行维护和使用管理由网络信息中心负责；学校所有基建、修缮工程应将工程范围内校园网络建设纳入工程设计实施和竣工验收范畴。

第十条 校园网络所有设备（包括各类网络线缆、地上和地下线路基础设施、交换机、服务器、无线 AP、光纤模块、设备箱和网络接口等）由网络信息中心负责管理。网络设备的安装、维护、迁移和拆除由网络信息中心负责，任何人不得私自挪用或擅自拆装。

第十一条 未经允许，任何单位和个人不得私自改装网络线路或更改网络设备（如交换机、无线路由器等）的配置。

第十二条 校园网络与互联网及其他公共网络实行逻辑隔离，由网络信息中心统一出口、统一管理和统一防护。未经批准，各单位在校园内不得擅自通过其他渠道接入互联网及其他公共网络。

第十三条 网络信息中心采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施以加强校园网络边界防护。

第十四条 校园网络接入实行“实名注册、认证上网”制度；学校非涉密信息系统接入校园网络，实行网络接入审批和信息系统备案登记。网络接入实名管理由网络信息中心负责实施。涉密信息系统不得接入校园网络。

第十五条 严禁任何单位和个人利用校园网络及设施开展颠覆国家政权、泄密、传播不良内容、恶意攻击等不正当活动。因违规行为造成的经济损失或法律纠纷，由违规者承担。

第四章　信息系统安全管理

第十六条 各单位在申请建设网站和信息系统时，必须同步建立起相应的安全保障体系，在技术方案、经费预算及运行维护等方面形成全周期安全闭环。

第十七条 网络信息中心负责统筹建设学校网站群系统和技术安全管理工作。学校各单位新建网站，应使用学校互联网域名及 IP 地址，纳入学校网站群系统管理。网络信息中心对新

上线系统进行安全测评，测评合格后方可上线发布。

第十八条 网络信息中心负责统筹学校信息系统安全等级保护工作，并组织各单位开展相关工作。信息系统建设单位是信息系统安全等级保护的责任主体，负责系统定级、建设整改、安全自查，协助系统备案、等级测评等工作。网络信息中心负责信息系统台账管理、等级评审、系统备案、监督检查、安全防护体系建设和等级测评组织工作，协助学校各单位进行系统定级、建设整改工作。

第十九条 各单位应定期对本单位的网站和信息系统的安全状况、版本更新以及内容更新等情况进行自查，并根据学校安排将本单位网站与信息系统安全检查情况提交网络信息中心备案。配合有关部门做好系统安全检查、信息内容检查、保密检查等工作。

第五章　数据安全管理

第二十条 数据是指信息系统收集、存储、传输、处理等产生的各种电子数据，包括但不限于网站内容、业务数据、数字资源、日志记录及用户信息等。

第二十一条 网络信息中心负责学校基础数据库和数据共享交换平台的建设和安全管理，根据全校信息系统的数据需求，规范数据库结构和内容，对外提供统一的访问接口和数据服务。

第二十二条 各单位负责本单位信息系统的数据安全，按照“谁收集，谁负责”的原则，严格落实管理和技术措施，规范数据的收集、存储、传输和使用，确保数据安全。

第二十三条 数据实行申请使用制度，申请使用单位应遵循相关管理制度和技术标准，按需申请、规范使用。申请使用单位有责任和义务保护所获得数据的安全，未经允许，不得将数据用于其他用途。

第二十四条 网络信息中心负责学校核心信息系统的数据备份与恢复管理，根据业务实际需要对重要数据和信息系统进行备份，并确保备份数据和备用资源的有效性。各单位要根据本单位信息系统实际情况自行做好数据备份。

第二十五条 未经批准，任何单位和个人不得擅自对外提供信息系统产生的内部数据。对于非法泄露或擅自对外提供数据的单位或个人，依照相关法律法规予以处理。

第六章　终端设备安全管理

第二十六条 终端设备是指使用校园网络从事教学、科研、管理、服务等活动的各类计算机及相关设备，主要包括台式电脑、笔记本电脑及其他移动类终端等。

第二十七条 终端设备使用人按照“谁使用，谁负责”的原则，对其终端设备负有保管和安全使用的责任，并承担相关法律责任。

第二十八条 终端设备应当设置系统登录账号和密码，禁止自动登录，登录密码应具有一定强度并定期更改。终端设备上安装运行的软件须为正版软件。

第二十九条 终端设备使用人应做好数据日常管理和保护，定期进行数据备份。非涉密终端设备不得存储和处理涉密信息。

第三十条 终端设备使用人应做好终端设备的安全防范，安装杀毒软件并定期进行病毒查杀。如发现终端设备出现异常、感染病毒、遭受攻击，应立即断开网络，并采取妥善措施处置。

第七章　电子邮件安全管理

第三十一条 网络信息中心为各单位和师生提供电子邮箱服务，并负责学校电子邮件的安全管理。各单位和师生使用学校电子邮箱应遵守法律法规和学校相关规章制度。

第三十二条 网络信息中心采取必要的技术和管理措施，加强电子邮件系统安全防护。邮件用户应定期备份重要邮件，清理过期邮件，提高邮件账号安全。邮件账户如出现违反法律法规和学校相关规章制度行为，网络信息中心有权随时中断或终止该账号邮件服务。

第三十三条 各单位和师生对其使用的电子邮箱账号所有活动负责，应妥善保管本人的电子邮箱账号和密码，确保密码具有一定强度并定期更换。如发现他人未经许可使用其电子邮箱，应立即通知网络信息中心处理。

第三十四条 在校师生可申请办理个人邮件账户，办理成功后邮件账户 ID 不可更改。学生毕业、教职工调离后其邮件账户将自动停用。

第八章　内容安全管理

第三十五条 任何单位和个人必须遵守《信息网络传播权保护条例》等国家有关法律法规和学校有关管理规定，严格执行信息安全保密制度，并对所提供和发布的信息负责。

第三十六条 任何单位和个人不得利用校园网络及学校各系统制作、下载、复制、查阅、发布、传播有害信息，不得侵犯国家、社会、集体利益和公民合法权益，不得从事违法犯罪活动。

第三十七条 各单位按照“谁发布，谁负责”原则，严格遵循内容审核机制，规范信息发布审批流程，加强信息安全监管，防止出现内容篡改等安全事故。

第九章　保障措施

第三十八条 学校负责网络与信息安全机构及人员岗位设置等保障工作，采取有效措施建立高水平的网络与信息安全管理专职队伍和技术支撑专业队伍。学校保障网络与信息安全发展的经费投入和必要的软硬件基础设施

第三十九条 网信办定期开展针对网络安全管理人员和技术人员的专业技能培训，提高相关人员的网络安全工作能力和水平；定期组织开展针对学校师生的网络安全教育，提高师生的安全意识和防范技能。

第十章　应急管理

第四十条 网信办负责学校网络安全应急工作的统筹管理，网络信息中心负责网络安全应急工作的技术支撑和保障。

第四十一条 网络信息中心定期对校内网站、信息系统、网络及相关设备开展网络安全检测工作，并发布检测报告，各单位应根据检测报告，及时落实网络安全自查和问题修复，避免网络安全事件发生。

第四十二条 网信办负责组织校内网络与信息安全处置应急演练，相关单位应积极参与。对于发现网络安全问题应及时向网络信息中心报告，并协助做好网络安全事件的应急响应和处置工作。

第四十三条 各单位定期对本单位信息系统、互联网站安全状况、安全保护制度及措施的落实情况进行自查，并配合相关部门的信息安全检查、信息内容检查、保密检查与审批等工作。

第四十四条 网信办对各单位网络与信息安全工作落实情况进行检查，对发现的问题下达限期整改通知书，对网络安全事件进行调查处置。相关单位应按照网络安全事件报告与处置流程及时、如实报告和妥善处置网络安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位责任人进行约谈或通报；对于玩忽职守、失职渎职造成严重后果的，依纪依法追究相关人员的责任。

第十一章　附　则

第四十五条 涉及国家秘密的信息系统，执行国家保密工作的相关规定和标准，由学校保密委员会办公室监督指导。

第四十六条 本管理办法自印发之日起执行，由网信办负责解释和修订。

信阳师范大学校长办公室　　2025 年 9 月 25 日印发