河南科技大学文件

河科大信〔2021〕7号

关于印发《河南科技大学网络信息安全管理办法》的通知

校属各单位：

为加强学校网络信息安全管理，推进学校信息系统安全等级保护工作，提高网络信息安全防护能力和水平，保障学校各项事业健康有序发展，特制定《河南科技大学网络信息安全管理办法》，请遵照执行。

二〇二一年一月四日

河南科技大学网络信息安全管理办法

第一章　总则

第一条 为加强学校网络信息安全管理，推进学校信息系统安全等级保护工作，提高网络信息安全防护能力和水平，保障学校各项事业健康有序发展，根据《中华人民共和国网络安全法》、《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》（教技〔2014〕4 号）、《教育部关于进一步加强直属高校直属单位信息技术安全工作的通知》（教技〔2015〕1 号）、《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》（教技〔2015〕2 号）、《河南省教育厅公安厅关于深入开展教育行业信息系统安全等级保护工作的通知》（教科技〔2015〕710 号）等文件要求，结合我校实际，特制定本办法。

第二条 本办法所称网络信息安全工作，是指为使学校建设、运行、维护或管理并支撑的学校教学、科研和管理等各项事业的信息资产的安全性、完整性、可用性等得到保持、不被破坏所开展的相关管理和技术工作。

本办法所指学校各二级单位包括各机关部、处、室、学院、直属机构、附属单位以及有关科研机构。

第三条 学校按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全网络信息安全责任体系，学校各二级单位、全体教职工生应依照本办法要求及学校相关标准规范

履行校园网络信息安全的义务和责任。

第二章　组织机构与职责

第四条 学校网络安全和信息化领导小组（以下简称“校网信领导小组)是学校网络信息安全的领导机构，负责统一领导、统一谋划、统一部署全校网络安全和信息化发展，统筹制定网络安全和信息化发展战略、宏观规划和重大政策，研究解决网络安全和信息化重大问题。

第五条 学校网络安全和信息化领导小组办公室（简称“校网信办”） 是校网信领导小组常设办事机构，负责网络与信息安全管理与监督工作。 具体职责包括：

（一）负责学校网络安全与信息化领导小组日常事务工作，向领 导小组提出工作建议；

（二）负责与上级部门网信办的工作对接；

（三）制定网络与信息安全总体规划，并组织实施；

（四）拟定网络与信息安全管理规章制度，制定网络与信息安全 标准规范；

（五）组织开展网络安全等级保护工作；

（六）负责网络安全事件应急管理，协调处理与政府安全管理部门的关系；

（七）组织网络与信息安全宣传和教育培训工作；

（八）负责网络与信息安全监督检查工作；

（九）学校网络与信息安全的其他工作。

党委宣传部负责校园网舆论环境管理、官方微博和官方微信等融媒体管理，指导学校校园网络文化建设和网络精神文明建设，履行对网络意识形态工作的组织、协调等职责。

网络信息中心是网络信息安全技术支撑单位和技术监督单位，负责学校网络信息安全防护体系的建设、运行维护、技术指导和服务支持，负责网络安全事件和安全漏洞的技术处置。

第六条 学校各二级单位是本单位网络安全和信息化工作的责任主体，各二级单位的网络安全员是本单位网络安全和信息化工作第一责任人，负责按本办法落实网络信息安全工作。

第三章　校园网络安全管理

第七条 校园网络是指校园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，包括校园有线网络、无线网络、各种物理专网和各种虚拟专网。

第八条 校园网络的需求制定和使用管理由网络信息中心负责。 涉及光缆布线、网络机房、网络设备、网管系统、域名管理、安全防护、认证计费、网络接入与运维等方面，由网络信息中心负责建设、运行、维护和管理。校园规划管理部门和建设部门负责地下管网的规划和建设， 应在建设施工前按照《河南科技大学通信业务与通信设施管理办法》有关规定向校网信办报备。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， 应在建设施工前按照《河南科技大学通信业务与通信设施管理办法》有关规定向

校网信办报备。

第九条 校园网络与互联网及其他公共信息网络实行逻辑隔离，由网络信息中心统一出口、统一管理和统一防护。未经批准，学校各二级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信息网络。

第十条 网络信息中心应采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施加强校园网络边界防护。

第十一条 全体教职工生接入校园网络，实行“实名认证上网”制度；学校非涉密信息系统接入校园网络，实行接入审批和备案登记制度。网络接入实名管理制度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。

第十二条 严禁任何单位和个人利用校园网络及设施开展经营性活动。

第四章　信息系统建设及安全管理

第十三条 学校按照“同步规划、同步建设、同步运行、同步安全”的原则，规划、设计、建设、运行和管理信息安全设施，建立健全网络信息安全防护体系，全面实施信息系统安全等级保护制度。

第十四条 网信领导小组负责制定学校信息系统项目规划和顶层设计。学校各二级单位根据本单位业务需求，提出信息系统建设申请，纳入学校规划的核心信息系统建设需求的将获学校信息化安全等级保护的优先支持。

第十五条 校网信办负责学校信息系统安全等级保护工作，组织学校各二级单位开展信息系统定级、系统备案、等级测评、建设整改，具体负责信息系统台账管理、等级评审、系统备案、监督检查工作。按照“自主定级、自主保护”的原则，信息系统建设单位是信息系统安全等级保护的责任主体，具体负责系统定级、建设整改、安全自查，协助系统备案、等级测评并接受有关部门监督检查。网络信息中心是信息系统安全等级保护工作的技术支撑保障部门，负责网络信息安全防护体系建设和等级测评组织工作，参与监督检查工作，并协助学校各二级单位进行系统定级、建设整改。

第十六条 各信息系统建设单位在立项阶段应确定安全保护等级，由校网信办对建设方案进行安全论证和等级评审。对于安全等级预定在第二级以上（含第二级）的信息系统，由校网信办统一办理系统备案。

第十七条 信息系统在建设阶段应按已确定安全保护等级，同步落实安全保护措施。信息系统建设完成后，由建设单位初步验收，出具初步验收报告。对于安全等级第二级以上（含第二级）的信息系统，由校网信办会同网络信息中心组织等级测评。信息系统通过初步验收和信息安全保护等测评后，网信领导小组方可进行竣工验收和进入试运行阶段。

第十八条 新建信息系统应使用学校数据中心提供的云服务，不再单独购置服务器及网络设备，但应在年度预算时将所

需计算资源和存储资源上报网络信息中心。如有特殊需求，需在立项阶段提出，经专家论证通过后进行采购，并托管于学校数据中心机房。

第十九条 信息系统建设单位需自行维护信息系统，并对信息系统的网络信息安全负责。使用学校数据中心云服务的信息系统，建设单位需签署《河南科技大学云服务使用安全责任书》。进行服务器托管的信息系统，建设单位需签署《河南科技大学托管服务器安全责任书》。涉及重要业务或大量师生员工信息的核心信息系统以及安全等级第二级以上（含第二级）的信息系统，原则上应由网络信息中心参与维护。

第二十条 信息系统建设和管理单位应制定信息系统使用与维护的管理制度，规范信息系统使用者和维护者的操作行为。指定专人（称为“***系统管理员”）负责管理本单位的信息系统。

第二十一条 对于安全等级第二级以上（含第二级）的信息系统，校网信办将定期组织开展等级测评，查找、发现并及时整改安全问题、漏洞和隐患。根据国家和教育行业有关标准规范，四级系统应每年进行两次测评，三级系统每年进行一次测评，二级系统每两年进行一次测评。

第五章　数据中心安全管理

第二十二条 数据中心主要包括支撑学校信息系统的物理环境 （其中包含机房）、软硬件设备设施、云计算平台、学校

中心数据库 （其中包含基础数据库）、数据共享交换平台、统一身份认证平台及 统一信息门户等信息化基础设施和平台。网络信息中心负责数据中 心的建设、运行、维护和管理。

第二十三条 网络信息中心负责数据中心物理环境、软硬件设备设施和云计算平台的建设和安全管理；根据信息系统安全等级的不同，对数据中心进行分区、分域管理，采取必要的技术措施对不同等级分区进行防护、对不同安全域之间实施访问控制。

第二十四条 网络信息中心负责学校中心数据库、数据共享交换平台的建设和安全管理，负责基础数据库与各二级单位业务数据库之间完成数据交换和共享。各二级单位负责建设、维护本单位业务信息系统所配套的业务数据库，并对本单位业务数据库及所申请的共享数据的安全负责。

第二十五条 统一身份认证平台为学校信息系统提供统一的身份管理、安全的认证机制、审计及标准接口。学校各二级单位建设面向师生服务的信息系统时，应使用统一身份认证平台进行身份认证。网络信息中心负责统一身份认证平台的安全，学校各二级单位负责本单位信息系统的权限管理及安全。

第二十六条 原则上，学校各二级单位应依托学校数据中心开展信息系统建设。需使用校外数据中心的，须报校网信办审批。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，不得部署在校外数据中心。未经校网信领导小组批准，

严禁使用境外数据中心。

第二十七条 网络信息中心对学校数据中心的使用实施准入管理， 负责制定使用数据中心的技术规范和标准，在信息系统上线前进行安全检测，符合技术规范标准并检测通过的信息系统方可上线运行。

第二十八条 数据中心的使用单位应遵循数据中心相关管理制度和技术标准，按照“最小够用”原则，按需申请、有序使用，不得利用数据中心资源从事任何与申请项目无关或危害网络与信息安全的活动。

第六章　信息系统数据安全管理

第二十九条 信息系统数据是指信息系统收集、存储、传输、处理和产生的各种电子数据，包括但不限于网站内容、业务数据、网络课程、图书资源、日志记录、用户信息等。

第三十条 信息系统数据的所有者是数据安全管理的责任主体，应当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。

第三十一条 信息系统数据的收集应遵循“最少够用”原则，不 得收集与信息系统业务服务无关的个人信息。按照“谁收集，谁负 责”的原则，收集个人信息的单位是个人信息保护的责任主体，应当对其收集的个人信息严格保密，并建立健全相关保护制度。

第三十二条 网络信息中心负责学校核心信息系统的容灾

备份管理，制订容灾备份计划，根据业务实际需要对重要数据和信息系统进行灾备，定期进行灾备演练，确保备份数据和备用资源的有效性。各信息系统的所有者应制定系统数据的备份方案并定期进行灾备演练，确保备份数据和备用资源的有效性。

第七章　网站安全管理

第三十三条 学校各二级单位开办的互联网网站，应使用学校的互联网域名和互联网 IP 地址，并遵守《河南科技大学互联网网站管理办法》及相关规章制度，不得有“双非网站”存在。

第三十四条 网络信息中心统一建设学校网站群平台并负责纳入该平台网站的技术安全。原则上，学校各二级单位网站应纳入网站群平台统一管理。未纳入学校网站集群平台的网站，其技术安全由网站开办单位负责。

第三十五条 各二级单位网站由本单位自行管理维护。各网站的内容安全由网站开办单位负责。各二级单位的网络安全员对本单位网站内容安全负责。网站开办单位应建立完善的网站信息发布与审核制度，确定负责内容编辑、内容审核、内容发布的人员名单，明确审核与发布程序，保存相关操作记录。

第三十六条 各二级单位应建立网站值守制度，制订应急处置流程，组织专人对网站进行监测，发现网站运行异常及时处置。

第三十七条 全校所有网站实行备案管理。网站正式上线前，

网站责任单位需向网络信息中心申请备案，签署《河南科技大学网站信息安全责任书》，并通过网络信息中心组织的安全检查后方可正式上线。

第八章　电子邮件安全管理

第三十八条 网络信息中心为学校各二级单位和师生员工提供电子邮箱，并负责学校电子邮件的安全管理。学校各二级单位和全体教职工生使用学校电子邮箱应遵守学校电子邮箱管理等相关规章制度。

第三十九条 网络信息中心应采取必要的技术和管理措施，加强电子邮件系统安全防护，减少垃圾邮件、病毒邮件侵袭。

第四十条 全体教职工生须对使用其电子邮箱帐号开展的所有活动负责，应妥善保管本人使用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本人电子邮箱，应立即通知网络信息中心处理。

第九章　终端计算机安全管理

第四十一条 终端计算机是指使用校园网络的、由学校师生员工使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括台式电脑、 笔记本电脑及其他移动终端。

第四十二条 终端计算机使用人按照“谁使用，谁负责”的原 则，对其终端计算机负有保管和安全使用的责任。网络信息中心对接入校园网络的终端计算机的安全管理提供技术支持和指导。

第四十三条 网络信息中心建立终端计算机统一管理平台，实现常用正版软件下载分发、系统补丁安装、病毒软件安装升级及漏洞管理等功能。

第四十四条 终端计算机设备上安装、运行的软件须为正版软件。 在终端计算机上使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第四十五条 终端计算机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。

第四十六条 终端计算机使用人应做好数据日常管理和保护， 定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

第四十七条 终端计算机使用人应做好终端计算机的安全防范， 如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其 他安全问题，应立即断网，然后联系网络信息中心进行处置。

第十章　存储介质安全管理

第四十八条 存储介质是指存储数据的载体，主要包括硬盘、存储阵列、磁带库等不可移动存储介质，以及移动硬盘、U 盘等可移动存储介质。

第四十九条 原则上，存储阵列、磁带库等大容量介质应托管在 学校数据中心，并由网络信息中心统一运行、维护和管理。网络信息中心应采取必要技术措施防范数据泄漏风险，确保存

储数据安全。

第五十条 学校各二级单位应建立移动介质管理制度，记录介质领用、交回、维修、报废或损毁等情况。介质使用人按照“谁使用， 谁负责”的原则，对其移动介质负有保管和安全使用的责任。

第五十一条 非涉密移动存储介质不得用于存储涉密信息，不得 在涉密计算机上使用。

第五十二条 移动存储介质在接入终端计算机和信息系统前，应 当查杀病毒、木马等恶意代码。

第五十三条 介质使用人应注意移动存储介质的内容管理，对送出维修或销毁的介质应事先清除敏感信息。

第五十四条 网络信息中心应配备必要的电子信息消除和销毁 设备。存储介质履行必要的审批程序后，可由网络信息中心集中销 毁。

第十一章　网络安全人员管理

第五十五条 学校各二级单位应建立健全本单位的岗位及网络信息安全责任制度，明确岗位及人员的网络信息安全责任。关键岗位的计算机使用和管理人员应签订信息安全保密协议，明确信息安全与保密要求和责任。

第五十六条 学校各二级单位应加强人员离岗、离职管理，严格规范网络安全人员离岗、离职过程，及时终止相关人员的所有访问权限，收回各种身份证件、钥匙、徽章以及学校提供

的软硬件设备，并签署安全保密承诺书。

第五十七条 学校各二级单位应定期对网络与信息技术安全岗位的人员进行安全知识和技能的考核，并对考核结果进行记录和保存。

第五十八条 学校各二级单位应建立外部人员访问机房等重要区域的审批制度，外部人员须经审批后方可进入，并安排工作人员现场陪同，对访问活动进行记录和保存。

第十二章　外包服务安全管理

第五十九条 信息技术外包服务是指信息系统的开发和运维的 外包。

第六十条 外包服务需求单位应与信息技术外包服务提供商签订服务合同和信息安全保密协议，明确信息安全保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何信息资产，不得以服务为由强制要求委托方购买、使用指定产品。信息技术外包服务合同和信息安全保密协议应按学校合同管理办法的有关要求，报校网信办审核。

第六十一条 信息技术现场服务过程中，外包服务需求单位应安 排专人陪同，并详细记录服务过程。

第六十二条 外包开发的系统、软件上线应用前,外包服务需求 单位应组织安全检查，要求开发方及时提供系统、软件的升级、漏洞等信息和相应服务。

第十三章　网安全教育培训

第六十三条 校网信办负责组织学校网络安全宣传和教育培训工作，建立健全相关制度。

第六十四条 校网信办定期组织开展针对师生员工的网络安全教育，提高师生员工的安全和防范意识。

第六十五条 校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，提高网络安全工作能力和水平。

第十四章　信息安全检查监督

第六十六条 学校各二级单位定期对本单位信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合有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。

第六十七条 校网信办联合网络信息中心对学校各二级单位的网络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，责成相关单位制订整改方案并落实到位。

第六十八条 校网信办对年度安全检查情况进行全面总结，按照要求完成检查报告并报网信领导小组。

第十五章　信息安全责任追究

第六十九条 学校建立信息安全责任追究和倒查机制。

第七十条 有关单位在收到网络信息安全限期整改通知书后，整改不力的，学校给予通报批评；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。

第七十一条 学校各二级单位应按照网络信息安全事件报告与处置流程及时、如实地报告和妥善处置网络信息安全事件。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。

第七十二条 师生员工违反本办法规定的，由校网信办责令改正，并通报批评；拒不改正或者导致危害网络信息安全等严重后果的，上报网信领导小组，予以纪律处分。触犯刑律的，移交司法机关处理。

第十六章　附则

第七十三条 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，由学校保密办公室监督指导。

第七十四条 本办法用语含义：

（一）网络是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络数据是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（四）个人信息，是指以电子或者其他方式记录的能够单独

或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账户密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

（五）个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全， 极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

第七十五条 学校各二级单位可参照本办法制订本单位的实施细则。

第七十六条 本办法自 2021 年 1 月 1 日起实施，由校网信办负责解释。学校原有相关规定与本办法不一致的，按本办法执行。

网络安全和信息化领导小组办公室

二〇二一年一月四日

河南科技大学校长办公室　　主动公开　　2021 年 1 月 4 日