湖北科技学院党政办公室文件

湖科办发〔2024〕52号

关于印发《湖北科技学院网络与信息安全管理办法（修订）》的通知

校内各单位、各部门：

经学校研究同意，现将《湖北科技学院网络与信息安全管理办法（修订）》印发给你们，请遵照执行。

湖北科技学院党政办公室

2024年6月4日

湖北科技学院网络与信息安全管理办法

第一章　总 则

第一条　为加强我校网络与信息安全工作，提高网络与信息系统安全防护能力和水平，保障我校各项工作安全、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》《互联网安全保护技术措施规定》等相关法律法规及《信息安全技术　网络安全等级保护基本要求（GB/T 22239-2019）》等相关国家标准，按照《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）等相关文件要求，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工作，是指对于支撑学校教学、科研、管理、服务等各项事业的校园网络、数据中心、信息系统以及各类校园网络接入终端开展的相关管理和技术工作，防止发生网络攻击、信息破坏、有害程序入侵、信息化设备设施故障等事件的发生。

第三条　本办法所指各单位包括学校各教学科研单位、管理服务部门、群团组织、派出机构、直属单位、附属单位。

第四条　学校按照国家有关网络安全和信息化政策法规，制定网络与信息安全总体规划，加强安全管理与技术研究，建立完

善的规章制度，并按照“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，各单位、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信息安全的责任和义务。

第五条 学校按照同步规划、同步建设、同步运行的原则，规划、设计、建设、运行、管理网络安全设施，建立健全网络安全防护体系，全面实施网络安全等级保护制度。

第二章 管理机构与职责

第六条 学校成立以党委书记、校长任组长的网络安全和信息化领导小组（以下简称“领导小组”），其主要职责包括：

1. 贯彻落实国家、教育部、省委、省政府、省教育厅、市委、市政府及市网信办网络安全和信息化战略部署；

2. 统筹协调学校网络安全和信息化重大问题，研究制定湖北科技学院网络安全和信息化发展战略、规划和政策；

3. 制定学校信息化及校园网建设的管理规范和技术标准，对执行情况进行监督管理；推进学校重大信息化建设工程的实施；

4. 统筹横向、纵向以及校内跨部门的信息化平台与数据的互联互通与共享；

5. 考核评估各部门信息化建设工作，监督各部门信息化工作实施；负责信息化建设项目与经费的管理工作；

6. 贯彻落实上级有关部门关于数据安全与个人信息保护工作的发展战略、宏观规划、重大政策和工作部署，部署学校的数

据安全与个人信息保护工作，统筹协调和决策学校数据安全与个人信息保护工作中的重大问题；

7. 完成上级网络安全和信息化领导小组交办的有关工作。

第七条 网络安全和信息化领导小组下设办公室（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：

1. 负责学校网络安全和信息化领导小组日常事务工作，定期向网络安全和信息化领导小组汇报工作，提出工作建议；

2. 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；

3. 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；

4. 负责协调处理学校网络安全、数据安全等重大突发事件有关应急工作；

5. 组织开展学校网络安全和信息化建设宣传普及、人员培训等工作；

6. 完成网络安全和信息化领导小组交办的其它工作。

第八条 信息中心是网络与信息安全技术支撑单位，负责学校网络安全防护体系的建设与运行维护，负责为全校各单位网络与信息安全工作提供技术指导与服务支持。

第九条 各单位是本单位网络安全和信息化工作的责任主

体，各单位主要负责人是本单位网络安全和信息化工作第一责任人，负责按本办法落实本单位网络与信息安全工作，推进信息化发展。

各单位应明确指定本单位信息系统的管理人员，信息系统管理人员是信息系统及其数据安全的直接责任人，其主要职责包括:

1.负责向网信办备案所管理的信息系统，并签订网络信息安全责任书，履行相应的安全责任与义务;

2.负责信息系统运行相关的操作系统、中间件、数据库系统的安全配置及漏洞修补，协助信息系统厂商进行信息系统的更新升级;

3.负责按“最小够用”原则对所有二级管理员和使用人员进行明确的权限划分;

4.信息系统管理人员须及时修改操作系统、数据库系统、信息系统等的初始密码，并制定高强度密码安全策略（如长度、复杂度、更换周期、尝试登录次数、账号锁定等），各级管理员和使用人员要杜绝使用弱口令、默认口令、通用口令，不得将账号借与他人使用；因弱口令造成的网络安全事件由账号所有人承担全部责任；通过账号发布的各类不良内容，由账号所有人承担全部责任;

5.负责信息系统的数据安全，落实数据安全管理和技术措施，确保信息系统数据在收集、存储、传输和使用等过程中的保

密性和完整性;

6.负责信息系统的内容安全,建立完善的信息系统信息发布与审核制度,明确审核与发布流程,保存相关操作记录;信息内容应当保证其不违反国家相关法律法规和学校有关规定,遵循学校信息化建设相关规定,确保其内容安全、真实、可靠、健康向上;严格遵守“涉密信息不上网,上网信息不涉密”,个人隐私信息须脱敏后方可发布;

7.确保信息系统所使用的脚本、程序、文字、图片、附件等资源必须安全可靠,避免传播带毒文件;引用、转发外部资讯时须做到严格审核,并注明来源;

8.根据数据重要性制定信息系统的数据备份和恢复机制,明确备份数据的备份方式、备份频度、存储介质、保存期等,定期对备份数据进行检查;

9.对发现或被通报的信息系统安全隐患要及时整改,受技术条件限制不能立即整改到位的,必须制定具有可操作性的应对方案,确保信息系统及其数据的安全;

10.负责信息系统的网络安全事件应急响应工作,如遇到网络安全事件,应立即采取果断措施进行处置,必要时要停止服务或断网,同时将网络安全事件报告信息化办公室,并启动网络安全事件报告与处置流程;

11.负责信息系统的版本管理,厂家部署运行的信息系统必须有对应软件版本号;当信息系统的软件版本发生变化时,需重

新向信息化办公室备案;

12.负责信息系统的安全监测工作，每日须对信息系统进行异常监测和检查，并对其运行状态和信息内容进行监控;

13.加强信息系统运维的安全管理,关闭远程桌面连接服务,对确需进行远程维护的信息系统,可向信息中心申请安全运维堡垒机和 VPN;系统管理员须对其申请的服务器运维堡垒机和 VPN 账号使用负责，因账号安全造成的一切后果由申请人承担;

14.做好信息系统对应服务器综合日志记录，日志留存时间不少于 180 天; 对于废弃或不再使用的网络资源，应及时报送信息化办公室登记备案。

各单位须将信息系统管理人员名单报备信息化办公室,人员变动时应及时调整并报备。

第十条 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全网络与信息安全责任体系，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。

第三章 校园网络安全管理

第十一条 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。

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 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制度。网络接入实名管理制度由信息中心负责实施。涉密信息系统不得接入校园网络。

第十五条 校园网用户必须遵守《中华人民共和国网络安全法》《中华人民共和国计算机信息网络国际联网管理暂行规定》《中华人民共和国计算机信息系统安全保护条例》等国家、地方和学校的网络与信息管理规定，并有义务向信息中心和学校有关部门举报任何网络违法犯罪行为。

第十六条 根据国家有关法律法规，禁止用户在使用校园网等网络资源时从事如下活动：

（1）利用校园网发布、传播、存放颠覆国家政权和破坏、影响社会稳定的言论、文章及声音图像，发布有损国家利益、学校利益的各种信息和散布各种谣言；

（2）利用校园网发布和传播属于国家秘密的各种文件资料，及泄露保密阶段的科研项目的有关资料、数据、图（照片）、音频、视频等校内文件资料；

（3）利用校园网发布、传播、存放传播有淫秽、暴力等内容的文章、图像、音频、视频等信息；

（4）在网络上散布计算机病毒，对他人进行恶意骚扰，包含恶意代码的邮件等;

（5）使用各类网络扫描软件、黑客软件等手段侵入或干扰校园网络系统的正常运行;

（6）利用系统漏洞牟取利益，或做出有可能危害系统安全或干扰系统正常运行的行为;

（7）国家相关法律法规规定的其它违法事项。

第十七条 严禁任何单位和个人利用校园网络开展一切不正当、非正常的活动，包括但不限于:

（1）未经允许，擅自提供 WWW、DNS、Mail、电子论坛、即时通信、网络代理及 VPN 等服务;

（2）未经允许，利用或变相利用校园网络资源及其网络设施从事商业及宣传活动;

（3）未经允许，擅自接入路由器等网络设备;

（4）盗用他人 IP 地址、账号或通过网络窃取他人信息;

（5）利用校园网络发送垃圾邮件等信息对其他用户造成干扰;

（6）将本人使用的账号转让、租借给他人不当使用;

（7）未经允许，设立游戏站点或纯娱乐性站点;

（8）利用网络造谣生事，进行人身攻击和侮辱;

（9）其他损害学校权益、违反学校规定的行为。

第十八条 因用户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　数据中心安全管理

第十九条　数据中心主要包括支撑学校各类信息系统运行的软硬件基础设施、云服务平台、学校基础数据库、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服务平台。

第二十条　信息中心负责数据中心的物理安全、网络安全和主机安全。数据中心的资源使用单位负责所使用的操作系统、业务数据库系统、信息系统和数据的安全。

第二十一条　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，负责各单位业务数据库与基础数据库之间完成数据交换和共享。

各单位负责建设、维护本单位业务信息系统所配套的业务数据库，对本单位业务数据库的系统安全、数据安全及所申请的共享数据的安全负责。

第二十二条　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。各单位建设面向师生服务的信息系统时，应与统一身份认证平台进行认证集成并备案系统信息。

信息中心负责统一身份认证平台的安全，各单位负责本单位信息系统的权限管理及安全。

第二十三条　各单位应依托学校数据中心实施本单位信息

系统建设，需要使用校外数据中心的须报网信办审批；严禁使用设置在境外的数据中心。涉及学校基础数据、师生个人信息或敏感信息的信息系统，禁止部署在校外数据中心（含云服务平台）。

第二十四条 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。

第二十五条 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系统安全的活动。

第五章 信息系统安全管理

第二十六条 学校鼓励优先采购安全可靠、技术成熟和服务优质的国产成品软件用于信息系统建设。没有相应成品软件或成品软件不适应实际需求的，可按照学校采购与招标相关管理办法，委托资质和信誉良好的软件开发商进行开发。

第二十七条 信息系统投入试运行后，由建设单位初步验收，出具初步验收报告，并向网信办申请开展信息系统安全检测。网信办组织开展信息系统安全检测，检测内容主要包括，信息系统源代码审计、系统漏洞扫描、安全基线配置核查等，形成检测报告；

第六章 二级域名安全管理

第二十八条 学校一级域名（hbust.edu.cn）由信息中心向

有关域名注册管理机构办理申请、注册手续，且仅能对湖北科技学院校园网 IP 进行解析。

学校二级域名的解析由信息中心负责技术实现，信息中心依规设立域名服务器；校内其他任何单位不得设立域名服务器。

信息中心有义务配合国家主管部门开展网站检查工作，必要时按要求暂停或停止相关的域名解析服务。

第二十九条 二级域名服务遵循“先注册先使用”原则；为维护学校和公众权益，信息中心对部分域名进行预留和保护。

域名注册申请单位应当提交真实、准确、完整的域名注册信息，经所在单位主要负责人审核同意，并通过党委宣传部审批、信息中心安全检测通过后，方可办理。

第三十条 二级域名使用单位应当遵守国家有关互联网络的法律法规。因二级域名使用造成不良影响的责任，由二级域名使用单位承担；二级域名注册信息发生变更的，二级域名使用单位应在 30 日内向信息中心申请变更。

第七章 网站安全管理

第三十一条 各单位建设的门户网站，应使用学校的互联网域名和学校站群系统。

第三十二条 各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。

第三十三条 各单位负责网站的内容安全，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。

第三十四条 遵守“涉密信息不上网，上网信息不涉密”和“谁发布、谁负责”的原则，确保发布的信息合法合规、真实有效、准确及时，符合信息公开相关要求。

第三十五条 各单位应定期备份其网站的重要信息数据，根据数据的重要性和系统运行需要，制定数据的备份和恢复策略与程序等。

第三十六条 各单位应进行相关活动日志记录，包括权限管理日志、账户管理日志、登录认证日志、业务访问日志、数据访问日志等；提供新闻、出版以及电子公告等服务的网站，还应记录并留存用户注册信息和发布信息审计日志；所有日志记录留存应至少保存 90 天。

第三十七条 对于使用频度不大、阶段性使用的网站，网站建设单位可采取非工作时间或寒暑假、节假日关闭的方式运行。对于无人管理、无力维护、长期不更新的网站，信息中心有权关闭其网站以降低安全风险。

第八章 电子邮件管理

第三十八条 信息中心为各单位、教师和研究生提供电子邮箱服务，并负责学校电子邮件的安全管理。电子邮箱使用者应遵守学校电子邮箱管理等相关规章制度。

第三十九条 信息中心有权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。

邮件用户应定期清理过期邮件，以确保整个电子邮件和该邮件账户能正常运作；邮件账户如出现安全漏洞、传播非法信息等情况，信息中心有权随时中断或终止向用户提供邮件服务。

第四十条 电子邮箱使用者须对使账号开展的所有活动负责，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，应立即通知信息中心处理。

第四十一条 教职工调离、学生毕业后其邮件账户将自动停用。

第九章 终端设备管理

第四十二条 终端设备是指使用校园网从事教学、科研、管理、服务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类终端等。

第四十三条 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。信息中心对终端设备的安全管理提供技术支持和指导，包括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。

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

第四十五条 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。

第四十六条 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。

第四十七条 终端设备使用人应做好终端设备的安全防范，如发现终端设备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，应立即断网后进行处置。

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，并由信息中心统一运行维护和管理。信息中心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 各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、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 信息中心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，可由信息中心集中销毁。

第十一章　人员管理

第五十五条　各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　各单位应加强人员离岗、离职管理，严格规范人员离岗、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　各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　教育培训

第五十八条　网信办负责组织开展学校网络安全宣传和教育培训工作，建立健全相关制度。

第五十九条　网信办联合相关单位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。

第六十条　网信办联合相关单位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。

第十三章　监督检查

第六十一条 各单位应定期开展本单位信息系统和数据安全状况、安全管理制度及技术措施落实情况的自查整改工作，对于自查中发现的问题要及时整改，并配合有关部门的安全监督检查工作。

第六十二条 网信办负责学校网络与信息安全工作落实情况的监督检查，建立健全安全监督检查机制。

第六十三条 网信办负责对年度网络与信息安全情况进行全面总结，并报领导小组。

第十四章 责任追究

第六十四条 各单位在收到网络安全限期整改通知书后，整改不力的，学校给予通报批评；造成严重安全后果，上级执法部门进行追责处罚的，本单位负责人为第一责任人。

第六十五条 各单位应按照学校网络安全事件应急预案和信息技术安全事件报告与处置流程，在发生网络安全事件时立即采取应急响应措施控制、降低损失，并及时、如实地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的，将对本单位予以通报并追究单位负责人的责任。

第六十六条 校园网用户违反网络与信息安全相关管理规定，未造成严重后果的，由信息中心或相关管理部门给予批评教育，责令改正；对拒不改正或者造成网络与信息安全严重后果的，根据学校有关规定予以处分。触犯法律时，由相关国家机关依法追究法律责任。

第十五章　附 则

第六十七条　涉及国家秘密的管理办法，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。

第六十八条　本办法解释权属信息中心。

第六十九条　本办法自发文之日起施行，原《湖北科技学院网络与信息系统安全管理办法》（湖科办发〔2016〕100 号）同时废止。

湖北科技学院党政办公室　　2024 年 6 月 4 日印发