中北大学文件

校信〔2023〕1号

关于印发
《中北大学网络与信息安全管理办法》的通知

全校各单位：

《中北大学网络与信息安全管理办法》经2023年10月13日第4次校长办公会审议通过，现印发给你们，请遵照执行。

中北大学

2023年10月23日

（此件主动公开）

中北大学网络与信息安全管理办法

第一章　总则

第一条 为加强学校对网络与信息安全工作的组织管理，提高网络信息安全防护能力和水平，保障各项事业健康有序发展，根据《中华人民共和国网络安全法》等国家相关法律法规并结合我校实际情况，制定本办法。

第二条 网络与信息安全是指网络基础设施、网站、信息系统及数据内容等受到保护，保证网络、信息及内容的安全性、完整性、可用性、可控性。

第三条 网络与信息安全管理的基本原则是“谁主管谁负责、谁建设谁负责、谁运维谁负责、谁使用谁负责”，明确责任、突出重点、保障安全。

第四条 网络与信息安全管理的总体方针是以国家标准《信息系统安全等级保护基本要求》（GB/T22239-2019）、《教育行业信息系统安全等级保护定级工作指南》、《高等学校数字校园建设规范（试行）》为指导，预防为主、综合防范。

第五条 网络与信息安全管理的目标是建立健全网络与信息安全保障体系，提高安全防护能力，确保学校网络与信息安全工作规范、有序开展，保障学校信息化可持续发展。

第六条学校任何组织或个人，不得利用网络及计算机信息系统从事危害国家利益、学校利益和师生合法利益的活动，不得危害校园网络及信息系统的安全。

第七条 在学校校园范围内建设、运营、维护和使用的网络信息化基础设施、网站及信息系统；在互联网上以中北大学名义建设、运营、维护、使用网站及信息系统和网络信息安全的监督管理，均适用于本办法。

第二章 管理机构及职责

第八条 学校网络安全与信息化领导小组（以下简称“网信领导小组”）是负责统筹学校网络安全与信息化工作的领导机构，负责学校网络安全与信息化建设的统筹规划、协调部署、重大问题的决策和监督检查。学校网信领导小组办公室设在信息中心，负责日常管理工作。

第九条 网络与信息安全工作主要由信息内容安全和信息技术安全两部分组成。

办公室、宣传部牵头负责网络信息内容安全工作。负责学校门户网站信息内容管理，审核门户网站的信息发布、转载和链接内容；负责学校新媒体内容管理及学校网络舆情监控、引导。

信息中心牵头负责信息技术安全工作。联系办公室、安全

保卫部等相关部门，统筹信息系统（含网站）和信息技术安全事件的报告、处置与通报工作；组织开展网络安全检查和培训；建立健全信息技术安全防护体系；负责统筹学校网络信息基础设施、公共信息服务平台和应用信息系统的建设、运维与安全管理工作；管理中北大学电子邮件系统，规范用户注册和账户管理；管理中北大学域名系统，规范域名注册、管理及 IP 地址分配；建设中北大学数据中心并建立健全数据灾备解决方案，确保全校重点数据安全；协助党委宣传部做好舆情监控的技术支持工作。

第十条 学校各单位主要负责人为本单位网络与信息安全工作的第一责任人，负责制定本单位信息化建设规划，监督本单位信息化项目建设、使用、维护，负责本单位信息化项目的信息安全工作。

第十一条 各单位应明确网络安全和信息化管理员，负责本单位网络与信息安全工作的具体实施。

第三章 校园网络安全

第十二条 校园网络是指连接学校各单位信息系统及信息终端的计算机网络，包括校园有线网络、无线网络和各种虚拟专网。

第十三条 校园网络与互联网及其他公共信息网络实行逻辑隔离，由信息中心统一出口、统一管理和统一防护。未经批准，

学校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信息网络。

第十四条 校园各区域的网络设备，其管理、维护等均由信息中心统一负责，未经信息中心批准，不得以任何方式试图登录、修改、设置、破坏校园网内的交换机、路由器和服务器等。

第十五条 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。

第十六条 师生员工接入校园网络，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，实行接入审批和备案登记制度。涉密信息系统不得接入校园网络。任何单位和个人不得窃取或盗用他人的用户名、口令、IP 地址和 MAC 地址等。

第十七条 接入校园网的机房、电子阅览室等场所禁止对社会开放。机房必须安装管理软件，自动记录上网人员身份和上下网时间、机号、IP 地址等，网络使用日志保留时间不得少于 180 天。

第十八条校园网络接入单位负责提供本单位所需的网络设备间和电源保障，负责其安防和消防安全管理。

第四章 信息系统及其数据安全

第十九条 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、日志记录等。

第二十条 信息化公共基础服务、跨部门信息系统、业务部门管理信息系统等面向师生公开服务的信息系统原则上应使用统一门户、统一数据库、统一认证等学校统一的软硬件平台。

第二十一条 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。

第二十二条 信息系统数据收集应遵循“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。

第二十三条 信息中心负责学校核心信息系统的备份与恢复管理，制订备份与恢复计划，根据业务实际需要对重要数据和信息系统进行备份，定期测试备份与恢复计划，并确保备份数据和备用资源的有效性。

第二十四条 服务器资源实现集中化管理。学校各类服务器需托管至学校中心机房，由学校统一提供虚拟服务器进行服务；原则上各单位不允许单独采购服务器、存储等相关设备，相关计算与存储资源由学校统一调配；因技术原因（如外置加密设备）确需存放在单位自建服务器上的，须及时向信息中心提交申请报告，获批并作出安全承诺方可保留，并将服务器托

管到学校中心机房，提高信息系统运行环境的安全防护能力。

第二十五条 财务管理系统、校园一卡通管理系统等涉及校内资金管理流通的信息系统应搭建专用的软硬件平台和专用传输网络，实现与校园网的物理隔离，确保系统运行环境安全。

第二十六条 各单位是本单位所有网站与信息系统的网络与信息安全责任部门。网站与信息系统在规划设计和建设时，应按照所处等级保护级别同步进行安全规划设计和建设，校内网站与信息系统在委托第三方进行开发时，应注重对代码审计、运维和安全修复方面条款的要求，确保使用中出现问题时能迅速解决。

第五章 互联网网站安全

第二十七条 学校各单位开办互联网网站，应使用学校互联网域名和互联网 IP 地址，并遵守学校相关规章制度。

第二十八条 党委宣传部负责学校网站站群平台建设并负责其内容审核，信息中心负责纳入该平台所有网站的技术安全。

第二十九条 各单位的宣传类、门户类的网站必须使用网站站群平台，以减少网站安全漏洞，提升网站的安全防护能力，确保网站风格的统一。未纳入学校网站站群平台的网站，其网

络与信息安全由网站开办单位负责。

第三十条 互联网网站运行维护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。

第三十一条 互联网网站的内容安全由网站开办单位负责。互联网网站开办单位应按照“三审三校”要求，建立完善的网站信息发布与审核校对制度，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。发生内容安全事件应立即向党委宣传部报告并按应急预案处置。

第六章 电子邮件安全

第三十二条 信息中心为学校各单位和师生员工提供电子邮箱服务，并负责学校电子邮件的安全管理。学校各单位和师生员工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。

第三十三条 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。

第三十四条 全校师生员工须对使用其电子邮件账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。师生员工如发现他人

未经许可使用其电子邮箱，应立即通知信息中心处理。

第七章 终端计算机安全

第三十五条 终端计算机是指由学校师生员工使用并从事校教学、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。

第三十六条 终端计算机使用人按照“谁使用，谁负责”的原则，对其终端负有保管和安全使用的责任。信息中心对终端计算机的安全管理提供技术支持和指导。

第三十七条 终端计算机设备上安装、运行的软件原则上应为正版软件。在终端上使用盗版软件带来的安全和法律责任由终端使用人承担。

第三十八条 终端计算机应当设置系统登录账号和密码，登录密码应具有一定强度并定期更改。

第三十九条 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。

第四十条 终端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，应立即断网后进行处置。

第八章 安全制度

第四十一条 系统上线安全审查。校内各单位网站或信息

系统在上线前，必须开展安全自查工作，并请第三方软件测评机构进行软件代码审计，提供审计报告，由本部门主要负责人签字确认后，提交信息中心。网站与信息系统按照公安机关信息系统等级保护备案要求，完成备案并提供备案编号。

信息中心对申请上线的网站和信息系统进行安全检查，使用漏洞扫描设备对网站和信息系统进行主机服务器和 WEB 应用服务安全扫描。对于存在安全风险或审计不通过的系统不予上线，整改后重新申请。申请上线的系统应标明系统的使用期限，对于短期使用的网站和信息系统，在使用期限到期后将自动关闭。

第四十二条 安全监测评估。信息中心对校内网站和信息系统进行日常安全管理，根据网站和信息系统的安全防护级别，定期进行安全扫描和风险评估，并将评估报告发送给网络安全和信息化管理员。对于存在高风险的网站和信息系统，将停止其互联网访问，通告负责人和网络安全和信息化管理员，相关单位应在 5 个工作日内修复，过期未修复的网站和信息系统将被关闭。对于出现严重安全事件的网站和信息系统，将立刻关闭，并通知负责人和网络安全和信息化管理员，责令整改需提交整改报告。对于出现问题的网站和信息系统，无法联系到负责人和网络安全和信息化管理员时，将视为无人维护，进行关闭处理。

第四十三条 学校各外包服务需求单位应与网络信息系统开发和运维服务提供商签订网络信息安全与保密协议，明确网络信息安全与保密责任，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和各类电子数据，不得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。各单位签署外包服务合同时，应将学校统一制定的网络信息安全与保密协议作为合同附件。

第四十四条 年审。校内网站和信息系统实行年审制，每年定期对网站和信息系统备案情况进行核查修订。年审期间管理员应检查所管理网站和信息系统的各项备案信息是否有变更，重点确认负责人和网络安全和信息化管理员的联系信息是否准确，并提交修改或确认。在年审过程中，超过规定期限没有进行备案信息确认的网站和信息系统，将视为无人维护，进行关闭处理。

第四十五条 安全事件处理。各单位发现网络与信息安全件要及时报告、处理（参照《中北大学突发事件应急预案》），保障校园网信息安全，堵塞有害信息，及时解决信息安全漏洞问题。

第九章 岗位管理

第四十六条 学校各单位应建立健全本单位的岗位信息安全

责任制度,明确岗位及人员的信息安全责任。关键岗位的计算机使用和管理人员应签订信息安全与保密协议,明确信息安全与保密要求和责任。

第四十七条 学校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，收回学校提供的软硬件设备，并签署安全保密承诺书。

第四十八条 学校各单位应定期对网络信息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。

第四十九条 学校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。

第十章 教育培训

第五十条 学校网信领导小组负责全校网络与信息安全宣传和培训工作的规划，建立健全相关制度。

第五十一条 信息中心定期组织开展针对师生员工的网络信息安全教育(每年至少一次),提高师生员工的安全和防范意识。

第五十二条 信息中心定期开展针对网络安全和信息化管理员和技术人员的专业技能培训（每半年至少一次），提高网络信息安全工作能力和水平。

第十一章 责任追究

第五十三条 学校建立网络信息安全责任追究和倒查机制。

第五十四条 有关单位在收到网络信息安全限期整改通知后，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。

第五十五条 学校各单位应按照网络信息安全事件报告与处置流程及时如实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。

第五十六条 师生员工违反本办法规定的，由学校网信领导小组责令改正，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，根据学校有关规定给予以纪律处分。触犯法律的，移交司法机关处理。

第十二章 附则

第五十七条 未经批准，任何单位和个人不得私自利用校网络建立网站、论坛、信息系统等，不得利用校园网对外提供商业服务或提供非法网站链接，不得擅自安装拆卸、或改变网络设施。

第五十八条 涉及国家秘密的信息系统及相关工作，执行国家保密工作的相关规定和标准，由学校保密工作办公室监督指导。

第五十九 条本办法在实施中若与国家有关法律、法规有不

一致的，以国家法律、法规为准。

第六十条 本办法由学校网信领导小组办公室负责解释，自发布之日起施行。

中北大学办公室　　2023 年 10 月 23 日印发