湖北铁道运输职业学院（武汉铁路技师学院）
校园网络和信息安全管理办法（试行）

第一章 总则

第一条 为了深入贯彻习近平总书记关于网络安全系列重要讲话精神，进一步加强校园网络和信息安全的管理，保障学校网络和信息安全，促进学校信息建设健康有序发展，根据《中华人民共和国网络安全法》等相关法律法规和《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》《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》等文件要求，结合学校实际，制定本办法。

第二条 本办法所称网络和信息安全工作，是指为使学校建设、运行、维护或管理的网络基础设施、网站、新媒体（微信公众号）、信息系统及业务数据信息的机密性、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。

第三条 网络和信息安全按照“谁建设谁负责、谁主管谁负责，谁运营谁负责，谁使用谁负责”的原则进行管理，各部门和全体师生员工应严格遵守国家相关法律法规，并按照本办法要求及学校相关标准规范履行网络和信息安全的义务和责任。

第二章 组织保障

第四条 学校党委对网络和信息安全工作负主体责任。学校成立网络和信息安全工作领导小组，负责校园网络信息安全全面工作，贯彻落实中央和上级单位关于网络安全战略部署，组织领导学校网络安全工作，统筹、沟通、协调学校网络安全工作中的重大事项、重大问题，提出相关方案或建议。

组　长：党委书记、院长；

副组长：校领导班子成员；

成　员：各处室、系部负责人。

第六条 学校网络和信息安全工作领导小组下设办公室（以下简称校网信办）。校网信办是学校网络安全工作的管理监督、统筹协调和组织实施部门，设在承担学校信息中心职能的部门。具体职责包括:

（一）负责制定网络和信息安全相关规章制度。

（二）负责学校网络和信息安全技术防护体系的建设、运行维护、技术指导和服务支持，为统筹管理和避免资源浪费，各部门不得再另行采购网络安全系统。

（三）负责与上级部门的沟通协调、网络和信息安全管理政策发文、学校重大突发网络安全事件的统筹协调等工作。

（四）指导、监督、检查各部门网络安全各项重点任务落实，负责系统安全检测并发布安全预警信息，督促整改各类安全隐患。

（五）建立网络安全联络机制，负责联系学校相关部门、构建安全高效的联络渠道。

（六）加强和规范网络安全信息汇集、分析和研判工作，建立网络安全专家咨询机构，分析、研判网络安全态势，服务网络安全决策。

（七）负责对校内各处室系部网络信息平台建设申请的审定和备案工作。

（八）负责学校网络安全事件的处置工作。

第七条 相关部门职责:

（一）党委宣传部负责网络意识形态阵地的舆情管理，负责管理和监督信息发布，对校园网络信息内容的维护、语言使用规范等进行指导和监督。

（二）保卫处负责协助重大网络安全事件的调查处理，负责网络和信息安全应急处置期间安全保卫等工作。

（三）各部门主要负责人是本部门网络信息安全工作的第一责任人，负责本部门网络信息安全管理工作。各部门须明确一名网络信息安全管理员，负责本部门应用系统及网站（网页）的运行维护和网络信息安全的具体工作。

第三章 网络（网站）管理

第十一条 学校官网（校园网）由校网信办主导建设、使用和运维，应按照国家和学校相关要求，开展学校官网的网络安全等级保护相关工作，并接受学校和上级有关部门监督检查。

第十二条 未经批准，任何部门及个人不得以“湖北铁道运输职业学院（武汉铁路技师学院）”在公网注册域名和开办网站。

为保证唯一性、规范性和权威性，域 https://www.hcrt.edu.cn/是我校对外的唯一域名，是学校在因特网上的重要标志。

第十三条 各部门及个人不得擅自建设、更改、损毁和挪用校园网设施，不得私自接入其他网络的出口，不得私自提供给校外人员使用。

第十四条 校园网接入实行登记备案制，使用网络实行实名制，校内用户必须通过网信办实名登记后方可按照入网要求使用校园网，未经登记不得以任何方式私自接入校园网，严禁盗用其他用户账号信息使用校园网。

第十五条 校园网络主要用于学校教学、科研、管理和服务等各项业务，严禁任何部门和个人利用校园网络及相关基础设施开展各类未经许可的其他活动。

第十六条 业务专网中的任何设备不得接入校园网、互联网，校园网的任何设备也不得私自接入业务专网。

第十七条 校园网 IP 地址未经许可不得对校园网以外提供互联网服务，如在教学、科研上确有特殊需求，需要 IP 地址对外开放服务（限于非信息发布类服务），应经校网信办审批后方可开放。

第四章 信息系统管理

第十八条 信息系统是指为学校教学、科研、管理等提供网络服务的各类软硬件平台。信息系统建设须经校网信办进行项目论证及审批，信息系统由各建设部门负责运行、维护与管理。

第十九条 各部门应按照国家网络安全等级保护的相关法律法规、标准规范以及《教育行业信息系统安全等级保护定级工作指南》要求，落实网络安全等级保护制度。

第二十条 各部门应准确掌握本部门信息系统情况，规范系统建设、运行维护、信息管理等方面的工作流程和机制，建立健全信息系统档案。

第二十一条 各部门要保证信息系统安全和数据安全，制定重要数据库和系统主要设备的容灾备份措施，记录并保留不少于六个月的系统维护日志。

第二十二条 各部门必须严格遵守国家、行业、地方相关法律法规和学校相关规章制度，自觉使用正版软件，保证信息系统数据的完整性和保密性，同时不得利用信息系统从事法律法规和学校相关规章制度禁止的活动。

第五章 数据管理

第二十三条 湖北铁道运输职业学院（武汉铁路技师学院）信息系统数据作为学校的无形资产和资源，包括但不限于：各类信息平台、各类业务系统、各类服务支持系统以及各类网站产生的数据。

第二十四条 各部门对产生和使用的数据安全负责，不得收集与业务无关的个人信息，应当按照网络安全等级保护要求落实安全管理和技术措施，规范数据的收集、存储、传输和使用，确保数据安全。未经审批，不得对外发布和提供数据信息。

第二十五条 各部门应严格管理业务数据的增加、修改、删除等变更操作，按照数据的重要程度，分公开、内部、敏感三级，根据级别确定保障措施；适时进行业务数据有效性检查，做好数据备份工作。

第六章 信息管理

第二十六条 校园网所有用户必须遵守国家有关法律法规和学校的有关管理办法，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。

第二十七条 党政办公室为学校信息公开的权威部门，信息公开工作要严格按照学校信息公开相关制度执行，未经批准，任何部门和个人不能擅自发布学校信息。

第二十八条 任何部门及个人不得利用校园网制作、复制、查阅和传播下列信息:

（一）煽动抗拒、破坏宪法和法律、行政法规实施的;

（二）煽动颠覆国家政权，推翻社会主义制度的;

（三）煽动分裂国家、破坏国家统一的;

（四）煽动民族仇恨、民族歧视，破坏民族团结的;

（五）煽动非法集会、结社、游行、示威、聚众扰乱社会秩序的;

（六）捏造或者歪曲事实，散布谣言，扰乱社会秩序的;

（七）宣传封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪的;

（八）公然侮辱他人或者捏造事实诽谤他人的;

（九）损害国家机关和学校信誉的;

（十）以非法民间组织名义组织活动的;

（十一）其他违反宪法和法律、行政法规、地方和学校规定的。

第二十九条 各部门要按照国家及学校有关规定，严格信息发布审核制度，未经审核的信息内容不得发布。凡涉及国家机密的信息严禁上网。

第三十条 校园网用户必须自觉配合国家和学校有关部门依法进行的监督、检查。用户若发现违法有害信息，有义务向学校有关部门报告。

第三十一条 校园网用户不得违反法律规定，利用网络获取和盗用他人信息。

第七章 账号密码与密钥管理

第三十二条 各部门应落实账号密码与密钥使用管理责任，账号应采用分级授权管理，根据用户角色创建相应级别账号，重要账号应建立 AB 角工作责任制。账号的权限设置应遵循“最小化”原则，即给用户能完成工作的最小权限。

第三十三条 不得使用默认账号密码，禁止所有匿名账号，应设置强密码，并定期更换密码，不得共享、公开账号密码。各部门应及时收回离岗、离职人员的管理账号密码以及学校提供的数据存储介质、软硬件设备，并签署安全保密承诺书。

第八章　设备、人员等管理

第十五条　各部门负责本部门安装使用的网络打印机、LED电子显示屏等物联终端及其控制系统的安全防护，应掌握使用情况、落实防范措施、加强安全监管、确保运行安全，并向网信办备案。

第十六条　终端计算机使用人应做好终端计算机的安全防范，终端计算机上安装、运行的软件须为正版软件，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。

第十七条　各部门和教职工、学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，并对使用其电子邮箱账号开展的所有活动负责，禁止使用电子邮箱传播恶意程序和不良信息，禁止使用电子邮箱存储、处理、传输涉密信息和工作敏感信息。

第十八条　各部门应指定在岗在编的专职人员担任网信工作人员，并向校网信办备案；关键岗位的信息系统使用和管理人员应签订网络安全保密协议；离岗、离职人员的访问权限应及时终止。

第十九条　校网信办负责组织开展学校网络安全宣传、教育和培训工作，各部门应积极参与，并做好在本部门的宣传推广工作。

第二十条　校园网络用户应文明上网，规范网络行为，并做好个人网络安全防护和隐私信息保护。校园网络用户的上网行为不得危害到学校、集体的整体网络安全，严禁利用校园网络从

事任何无授权的探测、破坏、信息窃取等网络攻击活动。

第九章　监测预警与应急处置

第二十一条　各部门应加强对所属网站和信息系统的日常监管，做到安全事件早发现、早报告、早控制、早解决。对发现的网络安全问题及时整改并报告校网信办。

第二十二条　校网信办对学校网络信息安全情况进行监测与检查，对于检查不合格的网站和信息系统，视其安全问题级别进行关停、限制校内访问等处理。

第二十三条　校网信办负责制定网络信息安全事件应急预案，定期组织网络信息安全突发事件应急演练。学校各部门应做好网络信息安全应急响应工作。

第十章　附则

第二十四条　对于违反本办法的，产生网络信息安全事件的部门及个人，给予通报批评；情节严重的，追究其主管领导、相关部门负责人及直接负责人的责任；构成犯罪的，依法追究刑事责任。网络信息失泄密事件按照国家和学校相关法律法规和规章制度处理。

第二十五条　本办法由校网信办负责解释。

第二十六条　本办法自印发之日起施行。