中共内蒙古师范大学委员会文件

内师党发〔2019〕42号

关于印发《内蒙古师范大学信息化建设管理办法》和《内蒙古师范大学网络信息安全管理办法》的通知

各院级单位党委、党总支，各学院、各部门：

《内蒙古师范大学信息化建设管理办法（试行）》和《内蒙古师范大学网络信息安全管理办法（试行）》已经第22次党委会研究通过，现予以印发，请遵照执行。

特此通知

附件：1. 内蒙古师范大学信息化建设管理办法（试行）

2. 内蒙古师范大学网络信息安全管理办法（试行）

2019年11月21日

附件 1

内蒙古师范大学信息化建设管理办法
（试行）

第一章　总　则

第一条　为进一步规范学校信息化建设，全面提升学校信息化工作管理水平，有序推进信息化工作的开展，根据相关法律、法规、标准和规范的要求，结合学校实际，特制定本办法。

第二条　贯彻“统一领导、统筹规划、统一标准、统一平台、归口管理”的原则，实行学校、业务主管部门、使用部门分级管理制度，明确责任，逐步实现“硬件集群、数据集中、应用集成、安全可靠”的建设目标。

第二章　组织机构与职责

第三条　学校网络安全和信息化委员会是学校信息化建设的审议决策机构，负责审议学校信息化建设发展的中长期规划与经费预算；审议学校信息化建设、运维管理及信息安全规章制度；审议信息化建设各部门的责任分工、资源分配以及考核机制；对学校信息化建设中的重大问题和政策性问题进行审议和决策。

第四条　学校网络安全和信息化委员会办公室负责制定学校信息化建设发展的中长期规划、信息标准规范、经费预算；制

定学校信息化建设、运维管理及信息安全规章制度；负责分期实施学校信息化建设规划，对具体项目进行组织协调与实施推进；负责对各业务系统信息资源进行集成与整合；负责对学校各单位申报的信息化新建和改造项目进行审核，为各单位信息化建设提供技术指导和支持；负责健全和完善信息化工作管理体系；负责统一管理校园信息基础设施；负责公共信息平台应用的推广与培训等。

第五条 学校各有关单位应明确具体负责信息化工作的分管领导与信息员。分管领导具体负责本单位业务系统建设、推广，监督学校信息化建设相关规章制度在本单位的执行；信息员负责本单位相关业务系统数据的更新和维护，保证信息的准确性、实时性、完整性和安全性，负责本单位信息化基础设施的日常管理。根据工作需要可设置双聘信息员，采用所在单位与信息中心双聘制度，共同开展信息化建设工作。

第三章 信息标准和编码管理

第六条 信息中心负责制定并发布信息的共享和交换标准，对信息标准的编制过程实施统一管理，落实相关编制代码的具体编制单位，协调编制之间的冲突，有权责令编制冲突相关单位进行整改。

第七条 各单位新开发的信息系统须使用统一的信息编码，

不符合标准的信息系统，将不予验收，不予上线使用。

第八条 各单位须保持学校信息编码的唯一性，严格执行统一的信息编码，不得随意增加、删除编码。如需修订，须报信息中心审批后方可修订。

第九条 在已上线的信息系统中，若所包含的信息编码规则与统一编制的信息编码规则不一致，暂时通过代码转换接入使用的，须在系统升级时更正。

第四章 信息系统建设与管理

第十条 信息中心牵头建设、管理及维护学校公共信息支撑平台，包括信息门户、统一身份认证、中心数据库、校园数据中心、邮件系统、公共服务软件、一卡通系统等学校层面的软硬件平台。

第十一条 中心数据库是学校集成、共享公共基础数据的平台，为保证其权威性、唯一性、准确性和实时性，学校所有信息系统均须向中心数据库开放数据读取，以便实现各业务系统之间的数据共享，同时为各类公共服务和管理决策系统提供数据支持。

第十二条 各单位的信息系统建设项目立项纳入学校信息化建设项目统一管理，均须通过学校网络安全和信息化委员会办公室审核或专题论证方可立项建设。

第十三条 各单位信息系统建设工作须按照学校信息化建设统一标准、统一平台的原则，遵循数据交换接口规范进行建设。信息中心对建设项目的实施进行技术监督和指导。

第五章 数据中心建设与管理

第十四条 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。

第十五条 信息中心负责学校数据中心的建设、运行、维护和管理。

第十六条 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管理，负责基础数据库与各单位业务数据库之间的数据交换和共享。

第十七条 学校各单位应依托学校数据中心开展信息系统建设。

第十八条 信息中心对利用学校数据中心部署的信息系统实施准入管理，负责制定使用数据中心资源的技术规范和标准。

第十九条 数据中心的用户单位应遵循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所申请业务不符的活动。

第六章　信息基础设施建设与管理

第二十条　校园信息基础设施是指由内蒙古师范大学和各电信运营商在校园范围内建设的各类通讯管线、通讯电缆和光缆、通讯基站、弱电机房、竖井、网络设备、楼内弱电布线、无线网络接入设备、物联网设备等。

第二十一条　校园信息基础设施建设与管理工作由信息中心统一归口负责。

第二十二条　为避免重复和不规范建设，新建、扩建、改建楼宇时涉及校园信息基础设施，须经信息中心确认建设方案并严格按照建设方案执行。

第七章　二级域名管理

第二十三条　信息中心负责学校二级域名的分配与管理。校内各单位的应用系统须使用内蒙古师范大学二级域名（*.imnu.edu.cn）。

第二十四条　二级域名管理实行备案制和年审制，各单位须将域名用途、责任人、联系方式等信息提交信息中心备案。信息中心每年对所有二级域名进行清查，有权对无责任人、一年内无更新内容的予以关停。

第八章　附　则

第二十五条 本办法自印发之日起施行，由学校网络安全和信息化委员会办公室负责解释。

附件 2

内蒙古师范大学网络信息安全管理办法（试行）

第一章 总 则

第一条 为规范校园网络信息安全建设与管理工作，提高网络与信息安全防护能力和水平，保障校园网络信息安全，根据《中华人民共和国网络安全法》等相关法律法规，结合学校实际，特制定本办法。

第二条 本办法所称网络信息安全工作，是指为保证学校信息资产（与教学、科研和管理等各项事业相关的网络、信息及信息系统）的保密性、完整性、可用性而开展的管理和技术工作。

第三条 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，学校建立健全网络信息安全责任体系，各单位及全体师生员工应依照本办法要求和学校相关标准规范履行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委员会是学校网络信息安

全工作的领导机构，负责学校网络安全工作的战略决策、实施监督及重大网络安全事件处理的决策指导，协调全校网络与信息安全保障体系建设。

第五条 学校网络安全和信息化委员会办公室是学校网络信息安全工作的执行机构。具体职责包括:

1. 制定网络信息安全工作总体规划，并组织实施;

2. 拟定网络信息安全管理制度，制定学校网络信息安全标准规范;

3. 组织开展信息系统安全等级保护工作;

4. 负责网络信息安全应急管理，做好与上级部门的协调处理工作;

5. 组织开展网络信息安全宣传和教育培训工作;

6. 负责网络信息安全监督检查工作;

7. 负责学校网络信息安全的其他工作。

第六条 信息中心是网络信息安全技术支撑单位，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;负责组织协调与管理监督信息化项目中的网络安全建设;负责保存网络运行日志，配合有关部门调查取证;负责其他与学校网络信息安全相关事务的处理。

第七条 党委宣传部负责网络信息内容的安全监管，负责网络舆情的监测和研判处置，开展网上舆论疏导和正面宣传工作。

第八条 学校各单位是本单位网络信息安全工作的责任主体，各单位党政主要负责人是本单位网络信息安全工作的第一责任人，负责按本办法落实网络信息安全工作。

第九条 网络信息系统的主管单位承担安全监管责任，包括内容安全监管、技术安全保障和监督检查等职责；网络信息系统的使用单位和个人对系统操作与信息内容的安全监管承担直接责任。网络信息系统通过外包服务方式进行维护，其安全监管责任主体仍为该主管单位，由其负责督促外包服务单位做好网络信息系统安全运维工作。

第三章 校园网络安全管理

第十条 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，包括校园有线网络、无线网络和各种虚拟专网。

第十一条 信息中心负责运维、管理校园网络所涉及的网络基础设施和安全管理系统。

第十二条 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。

第十三条 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。

第十四条 学校各单位及师生员工接入校园网络，实行“实名注册，认证上网”原则，由信息中心负责实施。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。

第十五条 校内各楼宇校园网络接入所用的网络设备间由信息中心统一管理，负责安防和消防安全，严禁占用。

第十六条 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 数据中心安全管理

第十七条 信息中心负责学校数据中心物理环境、软硬件设备设施和云计算、云存储平台的安全管理；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，统一部署备份、恢复策略。

第十八条 信息中心负责学校中心数据库、数据共享交换平台的安全管理。各单位负责建设、维护本单位业务应用系统所配套的业务数据库，且仅可部署于数据中心所提供的软硬件平台之上。各单位须对本单位业务数据库及所申请的共享数据的安全负责，严禁将业务系统数据导出，严禁使用 U 盘等移动存储介质或

微信、邮件等网络应用传递数据。

第十九条 各单位涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，不得在校外部署。

第五章 信息系统安全管理

第二十条 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。

第二十一条 网络安全和信息化委员会办公室负责统筹学校信息系统安全等级保护工作，组织学校各单位开展信息系统定级、备案、测评、整改和监督检查工作。各学院、各部门作为信息系统建设单位，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。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，并协助学校各单位进行系统定级、建设整改。

第二十二条 为确保信息系统建设项目的安全质量，信息系统建设单位应在立项前向网络安全和信息化委员会办公室提交书面系统数据使用情况、用户范围、身份认证方案、服务器、网络及其他相关资源的需求说明；在立项阶段申请网络安全和信息

化委员会办公室组织需求、技术等方面的专家论证；项目招标阶段应要求软件开发商同时提交其在安全方面的相关资质证明、软件安全情况说明（包括但不限于历史安全情况、安全风险及应对策略）、系统部署实施及后期维护的方案（包括但不限于如人员、方式、场地），以及安全承诺书；信息系统开发环境、测试环境和运行环境应严格隔离，信息系统建设单位负责开发环境、测试环境、运行环境的建设、运行、维护和管理；在系统测试、开发阶段，严禁使用真实生产数据；在系统部署、测试完成后，应出具有资质的第三方安全机构安全检测报告，其后方可组织验收；系统升级、修改应采取补丁形式，严禁直接修改生产作业中的信息系统。在项目实施前，信息系统建设单位、软件开发商应签署保密协议及安全责任书。

第二十三条 新建信息系统在上线前须进行安全检测，在完成网络安全等级保护定级并经测评通过后方可正式上线运行。

第二十四条 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。学校各单位建设面向师生服务的应用系统时，应使用统一身份认证平台进行身份认证，并彻底关闭自有的认证入口。信息中心负责统一身份认证平台的安全，学校各单位负责本单位应用系统的权限管理及安全。

第二十五条 新建信息系统原则上使用学校数据中心提供

的云计算资源，不再单独购置服务器及网络设备。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，并托管于信息中心 。

第二十六条 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《内蒙古师范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《内蒙古师范大学托管服务器安全责任书》。

第二十七条 信息系统建设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。

第二十八条 对于安全等级第二级以上（含第二级）的信息系统，网络安全和信息化委员会办公室将定期组织开展等级保护测评，查找、发现并及时整改安全问题、漏洞和隐患。

第六章 网站安全管理

第二十九条 信息中心负责网站群系统运行技术支持、建设与安全运行维护、运维队伍培训等工作。各单位网站须纳入网站群平台，实行统一管理。

第三十条 二级网站的内容管理由二级网站主管单位负责，各行政单位主管领导和各学院党委（党总支）书记为第一责任人，负责组织制定单位网站信息安全管理制度，落实专人负责信息审

核和日常管理。

第三十一条 各单位须签署《内蒙古师范大学网站信息安全责任书》，报党委宣传部和信息中心备案。

第七章 电子邮件安全管理

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 师生员工对通过自己电子邮箱所开展的活动负责，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。

第三十五条 不得使用网络邮箱存储、处理、传输涉密信息和工作敏感信息，不得将邮件自动转发至私人邮箱或境外邮箱。

第八章 终端计算机安全管理

第三十六条 按照“谁使用，谁负责”的原则，终端计算机使用人对网络终端设备（包括个人计算机、无线路由器、手机、交换机等）负有安全使用责任。

第三十七条 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。

第三十八条 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。

第三十九条 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，应立即断网并进行处置。终端用户要使用正版软件，保障操作系统以及相关的应用的安全，定期清理病毒、木马等恶意程序。

第九章 存储介质安全管理

第四十条 学校各单位应建立信息系统专用存储介质安全管理制度，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，对其存储介质负有保管和安全使用的责任。

第四十一条 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。

第四十二条 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，确保安全。

第四十三条 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。

第十章 人员安全管理

第四十四条 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。

第四十五条 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信息系统和设备的访问权限并签署离岗安全保密承诺书。

第四十六条 学校各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培训与考核，并对结果进行记录和保存。

第四十七条 学校各单位应建立外部人员访问机房等重点区域的审批制度，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。

第十一章 外包服务安全管理

第四十八条 信息技术外包服务是指信息系统的开发和运维的外包。

第四十九条 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与保密协议，明确信息安全与保密责任。

第五十条 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。

第十二章　网络信息安全应急管理

第五十一条　网络安全和信息化委员会负责学校网络信息安全应急工作的统筹管理，信息中心负责网络信息安全应急工作的技术支撑和保障。

第五十二条　网络安全和信息化委员会办公室负责制定学校网络信息安全事件报告与处置流程，信息中心负责制订学校网络信息安全应急预案；若学校网络信息安全应急预案不能满足需求，相关单位可制订本单位网络信息安全应急预案，但须及时报送网络安全和信息化委员会办公室备案。

第五十三条　网络安全和信息化委员会办公室定期组织网络信息安全应急演练、评估，并适时对网络信息安全应急预案进行修订。学校各单位应组织开展网络信息安全应急预案的宣传、教育和培训工作，确保相关人员熟悉应急预案。

第五十四条　信息中心负责组建学校信息安全应急技术支援队伍，完善应急值守制度，提高信息安全事件的预防、预警和应对能力，预防和减轻信息安全事件造成的损失和危害。

第五十五条　信息中心负责建立学校网络信息安全检查、巡查机制，定期或不定期组织开展信息系统安全演练，查找安全漏洞和隐患；对检查中发现安全漏洞和隐患的，应及时下达《隐患

告知书》，逾期未采取措施和提交处理报告的，应及时下达《隐患整改通知书》。对于一时难以修复或整改落实的，应当立即采取措施进行隔离，直至修复完成。

第五十六条 各单位应按照学校网络信息安全事件报告与处置流程，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。做到安全事件早发现、早报告、早控制、早解决。

第五十七条 各单位或师生员工均有义务及时向信息中心报告信息安全事件，不得在未授权情况下对外公布或利用所发现的安全漏洞和安全问题。

第十三章 信息安全责任追究

第五十八条 学校建立网络信息安全责任追究和倒查机制，并将网络信息安全工作情况纳入领导干部年度考核范畴。

第五十九条 有关单位在收到网络与信息系统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。

第六十条 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；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。

第六十一条 对违反本规定者，学校将予以通报批评；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。具有违法行为的，移交司法机关处理。

第十四章 附 则

第六十二条 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，由学校监督指导。

第六十三条 各单位可参照本办法制订本单位的实施细则。

第六十四条 本办法自印发之日起施行，由网络安全和信息化委员会办公室负责解释。学校原有相关规定与本办法不一致的，按本办法执行。

抄送：学校领导。

内蒙古师范大学党政办公室　　2019年11月21日印发