兰州理工大学文件

兰理工发〔2021〕119号

关于印发《兰州理工大学网络安全管理办法》的通知

校属各单位、部门：

《兰州理工大学网络安全管理办法》经2021年6月17日党委常委会会议审定通过，现予以印发，请遵照执行。

兰州理工大学

2021年6月18日

兰州理工大学网络安全管理办法

第一章　总　则

第一条　为保证学校网络安全和信息化建设工作健康有序发展，进一步规范学校网络安全管理，提高网络安全能力水平，提供稳定、可靠、安全的网络空间环境，为学校人才培养、科学研究、管理服务、交流合作及文化传承提供有力保障，根据《中华人民共和国网络安全法》、《中华人民共和国保守国家秘密法》、《中华人民共和国密码法》、《网络安全等级保护条例》等有关法律法规以及教育部《高等学校数字校园建设规范（试行）》的要求，结合学校实际，制定本办法。

第二条　本办法所称网络安全管理是指为了保障学校网络与信息化建设相关基础设施、信息系统、应用服务及数据的完整性、可用性及保密性而开展的相关管理和技术工作，涵盖校园网基础设施安全、网络操作系统安全、信息系统安全、数据安全、内容安全、终端安全及安全管理等内容。

第三条　学校按照国家有关网络安全和信息化建设的法律法规要求，贯彻落实国家网络安全和信息化战略部署，落实网络安全责任制，建立健全校内网络安全相关规章制度，总体规划、设计并统一协调部署网络安全和信息化建设工作。

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负责贯彻落实中央关于网络安全的重大战略部署，研究学校网络安全和信息化领域重大事项，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要问题，指导监督学校网络安全工作，统筹推进网络安全和信息化建设相关工作。

第五条　学校网络安全和信息化领导小组办公室（以下简称“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，负责学校网络安全统筹规划、总体推进和检查考核，负责网络安全内容管理，协调、参与网络安全事件的处理，开展网络安全宣传教育。

第六条　学校保密办公室负责指导和监督校属各部门、单位（以下统称为部门）网络安全相关的保密工作，组织查处网络安全领域违反保密法律法规的行为和泄密事件。

第七条　学校网络与信息中心（以下简称“网信中心”）负责网络安全和信息化建设统一归口管理和技术支撑工作，制定学校网络安全和信息化管理制度，落实学校信息化基础设施和公共服务平台整体防护，推进学校网络安全和信息化建设工作。

第八条　学校保卫处负责对网络违规行为和事件进行调查、取证，根据事态影响或破坏程度，对违规者按照有关规定报网信

办处理，涉及刑事犯罪的移送司法机关处理；负责校园网和信息系统网络通讯基础设施、网络通讯设备间消防安全工作。

第九条 学校各部门须成立本部门网络安全工作领导小组，明确网络安全责任，制定网络安全相关管理制度，组织和实施本部门的网络安全和信息化工作，指定本部门网络安全和信息化工作联络员，确定本部门网站及信息系统管理员。

第十条 学校各部门主要领导是本部门网络安全第一责任人，负责规划、监督本部门网络安全工作；各部门分管网络安全工作的领导是直接责任人，负责组织、协调、落实本部门网络安全工作。

第十一条 校内广大师生作为校园网的使用者，有责任和义务遵守学校网络安全的相关规定，积极参与学校网络安全的建设和管理。

第十二条 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，建立网络安全工作责任制。各部门根据学校网络安全重点工作和防护要求，结合实际制定本部门的网络安全和信息化工作规划，落实网络安全工作。

第三章 网络安全工作保障

第十三条 网络安全工作是学校信息化建设的常规工作，校内各相关部门应通力合作，在人员、资金、技术、设备等方面提

供充足的支持与保障，为学校网络安全和信息化工作创造良好的环境和条件。

第十四条 学校每年定期召开网络安全和信息化工作会议，根据网络安全形势，研究评估网络安全风险隐患，确定年度重点工作，落实网络安全工作的各项保障，持续推进网络安全工作。

第十五条 学校在经费安排上切实保障网络安全等级保护测评、安全监测和检测评估、信息系统安全升级、信息系统防护加固、网络安全教育培训、网络安全事件处置和安全运维服务等网络安全常规工作预算。对于网络安全和信息化项目建设中出现重大安全问题的服务商，学校根据合同及其他规定做出延期验收等处理。

第十六条 网信办和网信中心根据上级部门要求及上一年度网络安全防护形势，制定下一年度网络安全重点工作，动态调整网络安全策略，构建多层次、多维度的网络安全保障体系，持续提升学校网络安全防护水平和保障能力。

第十七条 按照国家相关法律法规要求，及时开展校内网络安全等级保护工作。网信中心负责校内等级保护工作的组织协调及信息系统等级保护定级工作，各部门在网信中心指导下做好本部门信息系统等级保护测评、整改等工作的具体落实，确保学校等级保护工作按照国家法律法规要求有序开展。

第四章　保密管理

第十八条　校园网用户应遵守国家有关法律法规，严格执行安全保密制度，不得利用校园网从事危害国家安全、泄露国家和学校秘密等违法犯罪活动；不得利用校园网进行搜集、整理、窃取国家和学校秘密的活动。违反本条款的校园网用户，承担相应法律责任。

第十九条　坚持“谁上网谁负责”的原则落实上网信息保密工作。规范信息保密审查制度，分级负责。发布信息时对信息内容的保密性进行审核，防止秘密信息泄露。

第二十条　校园网用户发现国家及学校秘密泄露情况，应立即向学校保卫处或保密办报告。保卫处或保密办接到举报或发现网上有泄密情况时，应当立即组织查处，并采取处置措施，删除网上涉及国家和学校秘密的信息，并启动调查程序。

第四章　网络内容安全管理

第二十一条　学校网络内容安全管理范围包括各类信息系统、网站、学校官方微信公众号、各类具有宣传功能的校内电子屏、校园广播系统等各类多媒体媒介平台的管理。

第二十二条　学校各类系统、网站、平台要坚持正确的舆论导向，弘扬主旋律，传播正能量，确保舆论宣传安全可控，遵守网络安全相关法律法规，严禁发布违法、涉密信息，禁止发布损

害他人权益的信息，不得利用学校网络与信息系统相关资源从事经营性互联网服务。具体内容参照《兰州理工大学网站建设与安全管理办法》执行。

第二十三条 严格实行信息发布审核制。发布信息和上传文件前需对相关信息和文件的必要性、合法性和安全性进行审查，并确保相关信息准确无误。具体内容参照《兰州理工大学网站建设与安全管理办法》执行。

第五章 网络通讯基础设施安全管理

第二十四条 校园网络通讯基础设施包括弱电通讯管网、桥架、通讯线缆、网络通讯设备、网络通讯设备间、运营商通讯基站和机房等通讯资源。

第二十五条 网络通讯基础设施的安全管理，参照《兰州理工大学网络通讯基础设施管理办法》执行。

第六章 校园网安全建设与管理

第二十六条 校园网及相关基础设施由学校统一规划、建设、管理和防护，并提供统一网络出口，校内各部门及个人不得擅自建设、更改、损毁、挪用校园网及相关基础设施，不得私接外网出口。校内各部门确有需要通过专网、或者使用运营商互联网出口接入的，须向网信中心申请报备。

第二十七条 学校网络建设要充分考虑关键网络和安全设

备冗余设计，增强网络的健壮性和稳定性，避免因关键设备出现故障影响师生使用校园网络。网信中心应根据现有网络设备的实际情况，建立网络基础设施备品备件库，进行统一管理。

第二十八条 校园网接入实行实名认证和登记备案机制，校内用户必须在网信中心实名登记后方可按照入网要求接入校园网，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使用校园网。确因教学、科研、管理及服务等需要实行有线网络免认证接入的，由相关部门及个人向网信中心提出申请，制定安全方案，部署安全措施，方可实行有条件免认证，具体办法参照《兰州理工大学校园网账号管理办法》执行。

第二十九条 校园网络资产包括 IP 地址、校园网账号、域名、服务端口等，相关资产遵循全生命周期管理原则，一经申请，申请人应妥善保管账号密码信息，确保安全，未经允许不得对外开放互联网服务，不得借用校园网资产从事非法、违规或未经许可的其他活动。

第三十条 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，及时掌握使用情况，落实防范措施，加强安全监管，确保运行安全。

第三十一条 个人计算机或服务器使用人应做好系统安全防护。正版杀毒软件、办公软件及操作系统由学校统一购买，校园网用户通过统一身份认证平台登录学校正版软件管理平台下

载使用，不再单独购买。安装盗版软件带来的安全和法律责任由使用部门或个人承担。

第三十二条 教职工校外访问校园网资源统一使用学校VPN系统，该系统和学校数字化校园系统对接。图书馆VPN系统为学校VPN系统的有效组成部分，是访问图书馆资源的专用通道。禁止任何个人或部门以不安全方式连接校内系统，禁止任何单位或个人购买未经备案授权的国际VPN提供商的服务，否则造成的一切法律后果由相关单位或个人承担，具体办法参照《兰州理工大学VPN管理办法》执行。

第三十三条 学校为每一位教职工提供域名为lut.edu.cn的工作邮箱，任何个人或部门不得利用学校提供的邮箱从事非法活动。校园网用户要使用国内电子邮件服务商提供的电子邮件服务收发与工作相关的邮件，确保信息安全。

第三十四条 校园网用户应文明上网，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学校网络安全，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。

第七章 信息系统安全管理

第三十五条 学校信息系统的安全建设要与信息系统建设“同步规划、同步建设、同步运行”，信息系统建设要符合学校相关标准（包括数据标准、接口标准等）、规范和安全要求，技

术架构要符合安全防护要求，确保信息系统建设安全可控。具体内容参照《兰州理工大学信息系统管理办法》执行。

第三十六条 各部门新建、升级信息系统要严格落实网络安全等级保护制度，在信息系统建设、实施、验收等环节要进行安全评估和检查，确保信息系统达到安全要求。

第三十七条 网信中心负责向全校提供数据中心物理环境、通信网络、计算环境、数据存储等资源，各部门按照各类资源申请和管理制度按需申请，合理使用，确保本部门业务系统的应用安全和数据安全，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安全的活动。

第三十八条 新建信息系统若有身份验证需求，须与学校数字化校园统一身份认证系统无缝对接，实现跨平台用户统一单点登录。逐步实现以智能终端为载体的多因子认证，采用手机短信、移动协同签名等多种认证方式。

第三十九条 与学校、科研、管理和服务等业务无关和未经网信中心审核备案的信息系统不属于学校信息资产，不得使用学校中英文校名、校标等学校标识，否则一切网络安全责任由系统建设、使用部门承担。

第四十条 各部门网站应基于学校网站群平台进行建设。网信中心负责网站群平台的建设、运行和维护，提供网站建设技术支持，负责校内网站的技术监管，参与网站安全的应急处置，具

体内容参照《兰州理工大学网站建设与安全管理办法》执行。

第四十一条 各部门的移动互联网应用程序应基于学校统一的移动平台和入口建设、运行和服务，避免各部门建立多个移动互联网应用程序，并且应按照教育部、公安部有关要求履行备案程序，进行等级保护测评。

第四十二条 加强信息系统的密码安全管理，杜绝使用弱密码、默认密码和通用密码，具体内容参照《兰州理工大学信息系统密码管理办法》执行。信息系统对校内外有限开放服务端口，禁止私自对外开放所需端口以外的服务端口，确保信息系统开放最小化。

第四十三条 任何上传至信息系统的文件必须经过严格的安全杀毒和审查，确定没有任何病毒或木马方可上传，否则立即停止上传，禁止任何形式的存储设备、介质未经杀毒直接接入信息系统服务器。

第四十四条 物理服务器托管，是指将各部门所购置的为校内外提供公共服务的独立物理服务器安装部署在学校两校区校园网中心机房，统一提供信息服务。被托管服务器所属部门须由指定人员对服务器进行管理和维护，严格执行安全保密制度，定期进行病毒查杀、补丁升级和数据备份工作，不得上传未经杀毒的文件，禁止安装与业务无关的软件违规占用服务器和网络资源。具体内容参照《兰州理工大学信息系统管理办法》执行。

第八章　数据资源安全管理

第四十五条　数据资源安全管理是指学校办学过程中对数据资源制定标准与规范，对数据资源的采集、存储、交换、共享与应用等方面制定相关规章制度。具体内容参照《兰州理工大学管理信息数据编码规范》、《兰州理工大学信息化数据资源管理办法》执行。

第四十六条　信息化数据资源是学校的公共资源和战略资源，各部门应按照学校信息化数据资源相关管理规定，使用学校统一提供的数据库平台，业务系统与学校中心数据库有效、可靠对接，加强对信息系统数据的安全防护，对重要数据做好定期完整备份和实时增量备份。

第四十七条　共享学校数据资源只能用于部门履行职责和特定工作需要，数据资源使用部门要按照“谁使用谁负责”的原则加强对共享数据的全生命周期管理。

第九章　人员安全管理

第四十八条　人员安全管理，是指对信息化工作人员授权管理、人员离岗、人员培训、外部相关人员管理等方面提出管理要求。

第四十九条　学校信息系统管理人员在授权管理信息系统之前，应由系统所在部门对相关管理人员的身份、背景和工作履

历进行安全审查，审查通过后方可授权开展相关工作，并向网信中心报备相关管理人员信息。

第五十条 信息系统管理人员离岗时，所在部门应对离岗人员办理严格的离岗手续，及时终止离岗人员的所有访问权限，包括物理访问权限、网络设备访问权限、操作系统访问权限、数据库访问权限、应用系统访问权限、用户终端访问权限、VPN 访问权限等，并向网信中心报备。教职工调离学校时，须办理校园网账号销户手续及其他所有与工作相关的信息系统账号销户手续，终止校园网及相关信息系统访问权限。

第五十一条 对于信息系统由校外人员实施运维服务或协助运维的，信息系统所在部门应与运维服务商和相关工作人员签订安全保密协议，并向网信中心报备，安全保密协议涵盖保密范围、保密责任、违约责任、协议有效期限和责任人的签字等内容。相关运维人员的权限管理由系统所在部门按照本办法管理。

第十章 安全监测预警与应急处置

第五十二条 网信中心对校内各部门信息系统、网络和其他相关设备进行网络安全检测，检测结果向全校通报，对存在安全漏洞和安全问题的部门下发整改通知，将检测结果和整改情况定期报网信办。

第五十三条 网信办和网信中心负责对学校网络安全相关的各类安全情报搜集和分析，并结合学校信息化建设实际情况对

学校信息化资源开展网络安全预警。相关部门及人员应根据预警信息，认真落实网络安全自查及问题整改，避免预警相关的安全问题发生。

第五十四条 校内网络安全事件的处理由网信办协调相关部门实施。相关部门及人员应认真落实网络安全事件处置相关工作。为避免扩大安全事件的不良影响，网信中心可直接对安全事件相关的网络操作系统及信息系统进行断网、停止服务等应急处理。

第五十五条 网信办和网信中心负责组织校内网络安全事件处置应急演练，相关部门应全力配合，通过演练提高校内网络安全事件处置能力。

第五十六条 各部门应根据本部门信息化建设情况，制定相应的监控与值守制度及网络安全事件报告流程。发现网络安全问题时，应根据事件影响程度及时向网信办和网信中心报告，并进行必要的应急处置，不得在未授权情况下对外公布、测试和利用所发现的安全漏洞或安全隐患。

第五十七条 各部门应制定本部门网络安全应急预案，定期开展网络安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第十一章　宣传教育与培训

第五十八条　网信办每年制定学校网络安全宣传主题和内容，邀请校内外网络安全领域的管理和技术专家对师生进行网络安全宣传、教育及培训，不断提升师生网络安全防范意识。

第五十九条　各信息系统所在部门应根据学校培训计划结合本部门实际制定本部门培训计划，提高管理人员的网络安全工作能力，提升本部门师生网络安全防范意识。

第十二章　违规责任

第六十条　对于擅自建设、更改、损毁、挪用校园网及相关基础设施的，责令限期整改，恢复原状，造成损失的，予以赔偿。上述情况中情节较轻的，由网信办对责任单位或个人予以相应处理；情节较重或对学校造成影响的，由网信办提请学校处理。

第六十一条　对于以下违规行为，责令限期整改。其中，情节较轻、对学校未造成损失或影响的，由网信办对相关责任单位、个人约谈或通报批评；情节较重或对学校造成影响的，由网信办提请学校根据情节严重情况对相关责任单位或个人予以处理；涉及违法的，承担相应法律责任：

1、私接外网出口的；

2、未经登记私自接入校园网的；

3、盗用其他用户账号使用校园网的；

4、未经许可对外开放互联网服务的；

5、借用校园网络资产从事非法、违规或未经许可的其他活动的;

6、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的;

7、利用学校数据中心资源从事与申请项目无关或危害网络安全活动的;

8、在未授权情况下对外公布、测试或利用所发现安全漏洞或安全隐患的;

9、安装与业务无关的软件违规占用学校网络资源或从学校申请的服务器资源的。

第六十二条 对于以下违规行为，按照《兰州理工大学网站建设与安全管理办法》相关条款处理:

1、发布违法、涉密信息的;

2、发布损害他人权益信息的;

3、利用学校相关资源从事经营性互联网信息服务的。

第六十三条 对于有危害公共安全、国家安全、泄露国家秘密以及其他违反法律、法规行为的，由公安、国家安全、保密以及其他监督管理部门依法处理,构成犯罪的,依法追究刑事责任。

第十三章 附 则

第六十四条 本管理办法自发布之日起执行，由学校网信办、网信中心负责解释。

兰州理工大学办公室 2021年6月18日印发