大连理工大学学校办公室文件

大工办发〔2019〕52号

关于印发《大连理工大学网络安全管理办法（修订）》的通知

校内各单位、机关各部门:

为保证学校网络安全与信息化建设工作的健康有序发展，规范校内网络安全建设管理工作，确保校内网络安全，根据《中华人民共和国网络安全法》等相关法律法规要求，结合学校实际，对《大连理工大学网络信息技术安全管理办法（试行）》（大工校发〔2017〕25号）进行了修订，经2019年6月26日校长办公会审定通过，现予以印发，请遵照执行。原《大连理工大学网络信息技术安全管理办法（试行）》（大工校发〔2017〕25号）同时废止。

附件：《大连理工大学网络安全管理办法（修订）》

2019年7月4日

学校办公室秘书科　　2019年7月4日印发

附件：

大连理工大学网络安全管理办法（修订）

第一章 总则

第一条 为保证学校网络安全与信息化建设工作的健康有序发展，规范校内网络安全建设管理工作，确保校内网络安全，根据《中华人民共和国网络安全法》等相关法律法规要求，特制定本办法。

第二条 本办法所称网络安全工作是指为保障学校网络安全与信息化建设相关基础设施、信息系统及数据的完整性、可用性及保密性，而采取的网络安全检测、防护、处置等技术措施，以及相关标准规范、管理制度的制定、执行等。

本办法主要是技术方面的管理，学校网络安全工作中涉及的内容安全、涉密信息安全管理等不在本办法范畴内，由学校相关单位根据相关规定进行管理。

第二章 组织机构及职责分工

第三条 学校网络安全与信息化建设管理委员会为学校网络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。委员会下设的网络与信息安全工作组负责制定学校网络安全的总体规划、网络安全工作检查及考评机制，协调重大网络安全事件的处理。

第四条 网络与信息化中心（以下简称网信中心）为学校网络

安全工作的技术管理机构，负责学校网络安全的日常规划及建设工作、组织协调与管理监督信息化项目中的网络安全建设工作、校园网安全建设与管理、网络安全管理制度的起草与执行，以及其他与学校网络安全相关事务的处理。

第五条 校内各单位按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，分别负责本单位主管、运维、使用的各信息系统及内部网络的安全工作。校内各单位应根据本单位信息化建设情况，建立本单位的网络安全管理制度和应急处置预案。

第六条 校内各单位信息化负责人为本单位网络安全的责任人，负责规划、监督本单位的网络安全工作；信息化专干负责组织、协调本单位的网络安全具体工作。

第七条 信息化项目的主管单位为该项目网络安全工作的主管单位，项目组负责该项目网络安全工作的具体落实与实施。

第八条 校内广大师生作为校园网的使用者、信息化建设的参与者，同样也是网络安全工作的参与者，有责任和义务遵守学校网络安全的相关规定，积极参与网络安全的建设和管理。

第三章 网络安全工作的支持与推进

第九条 网络安全工作是学校信息化建设的常规工作，校内各相关单位应通力合作，在人员、资金、技术、设备等方面提供充足的支持与保障。

学校在经费安排上切实保障网络安全等级保护测评、网络安全监测和检测评估、信息系统安全升级和防护加固、网络安全教

育培训、网络安全事件处置和安全运维等网络安全常规工作预算；新增信息化项目预算中须包含网络安全专项预算。

对于信息化项目建设中，出现重大安全问题的厂商，学校根据合同及其他规定做出延期验收等处理，对于此类情况造成的预算执行率问题学校应予充分考虑。

第十条 按照国家相关法律法规要求，学校应及时开展校内网络安全等级保护（以下简称等保）工作。网信中心负责校内等保工作的组织协调，各单位负责本单位主管信息化项目等保定级、等保测评、等保整改工作的具体落实，确保学校等保工作按照国家法律法规要求正常开展。

第十一条 按照国家相关法律法规要求，学校应积极开展关键信息基础设施保护工作。网信中心负责关键信息基础设施的认定、网络安全评估及网络安全建设工作。

第十二条 积极提高校内相关人员的网络安全工作能力，增强校内广大师生的网络安全意识。网信中心负责在校内开展网络安全相关的各类宣传、培训、演练等活动，校内各单位信息化建设相关人员应积极认真参与，并做好在本单位的宣传推广工作，工作情况列入信息化考核指标。

第四章 校园网安全建设与管理

第十三条 校园网及相关基础设施由网信中心统一规划、建设、管理，并提供统一网络出口，校内各单位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。

第十四条 校园网主要服务于学校教学、科研及校务管理等，用户不得将校园网用于其他用途，严禁利用校园网开展各类未经许可的其它活动。

第十五条 校园网入网实行实名制，校内用户必须通过学校统一身份认证接入校园网，未经登记不得以任何方式私接校园网，严禁盗用其他用户上网账号使用校园网。

第十六条 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维护及校园网个人资源相关网络安全管理维护。校园网用户的上网行为不得危害到学校网络安全和正常秩序，严禁利用校园网从事任何无授权的探测、破坏、信息窃取等互联网攻击活动。

第十七条 校园网用户 IP 地址未经许可不得对校园网以外提供互联网服务，如在科研上确有特殊需求，需要用户 IP 地址对外开放服务（限于非 WEB 信息发布类服务），经网信中心审批后可开放，由申请人员承担相关全部网络安全责任。

第十八条 对于违反上述规定的用户，经网信中心查实，可对违规用户暂停一切网络与信息化服务，并可根据本办法进行追责处理。

第五章 信息化建设中的网络安全建设与管理

第十九条 学校信息化建设实行网络安全一票否决制。对于不符合网络安全要求的各类信息化项目必须先进行整改，整改完成

后方可继续进行建设或继续提供服务。

第二十条 学校信息化项目建设应遵循校内网络安全相关制度、技术规范、标准流程开展，信息化项目全生命周期内各环节均需要完成相关网络安全建设工作。各信息化项目上线、验收前必须通过必要的网络安全检测，未通过检测擅自上线或验收的，一切网络安全责任由项目主管单位自行承担。

第二十一条 校内各类信息化应用原则上应依托于学校数据中心建设，使用学校 IP 地址及域名，并进行登记备案。

第二十二条 对于必须使用校外云服务建设的特殊信息化项目，也应按照学校信息化项目建设要求完成立项等流程，在采购文件和合同中应明确要求由云服务提供商负责项目的网络安全建设，由校内项目主管单位及云服务提供商共同承担网络安全责任。未按上述要求建设的此类系统，不属于学校官方行为，不得使用学校资金建设，不得使用校名、校徽、域名等学校标识，一切网络安全责任由系统校内相关单位（包括建设使用单位、资金提供单位、宣传推广单位等）及所有参与人员承担。

第二十三条 为保证学校信息化建设项目网络安全建设工作及安全运维工作正常开展，应采用安全规范、质量和售后服务优良的软、硬件产品或服务厂商，不得由自然人承担信息化项目建设任务。

第二十四条 校内各信息系统面向在校师生的用户认证必须使用学校统一身份认证，不得单独建立用户认证系统。

第二十五条 校内各信息系统应按照学校信息化数据资源相关管理规定，采取必要的安全措施，确保数据安全。

第二十六条 信息化建设中所涉及到的个人信息，必须按照国家相关法律法规及学校个人信息保护相关规定进行严格保护，任何单位及个人不得违法违规采集、存储、使用和处理校内各类个人信息。

第六章 检测预警与网络安全事件的处置

第二十七条 网信中心作为校内网络安全技术管理单位，代表学校对校内各类信息系统、网络、其他相关设备开展网络安全检测工作。网信中心可根据检测结果启动校内网络安全事件处置流程或发布安全预警。

第二十八条 网信中心负责学校网络安全相关的各类安全情报搜集工作，并结合校内信息化建设实际情况对校内开展网络安全预警。针对不同受众，安全预警将通过网信中心网站、邮件等不同方式发送，相关单位及人员应根据预警信息，认真落实网络安全自查及问题修复，避免预警相关安全问题的发生

第二十九条 校内网络安全事件的处理由网信中心负责组织实施，按照学校网络安全事件处置预案进行分级、分类处理。安全事件相关单位及人员应积极配合，认真落实网络安全事件处置相关工作。为避免安全事件不良影响扩大，网信中心有权直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。

第三十条 校内各单位应根据本单位信息化建设情况制定相

应的监控与值守制度，发现网络安全问题应及时向网信中心报告并进行必要的应急处置。

第三十一条 网信中心负责组织校内网络安全事件处置应急演练，相关单位应积极参与，通过演练提高校内网络安全事件处置能力。

第七章 奖励与追责

第三十二条 学校每年组织网络安全建设先进单位及个人的评选表彰，具体评选办法由网信中心另行制定。

第三十三条 对于违反本办法及相关网络安全制度的校内单位及个人，取消当年信息化建设评优资格。网络安全事件及其他安全问题的责任认定，将提交网络安全与信息化建设管理委员会讨论处理意见，进行处理。

第三十四条 对于违反法律、法规，造成国家、学校和个人损失的，学校将依法配合公安、网信等主管部门进行处理。

第八章 附则

第三十五条 本办法为校内网络安全建设的基本规定，校内其他涉及网络安全的相关规定应以本办法为依据，如有不同之处以本办法为准。

第三十六条 本办法由网络与信息化中心负责解释。

第三十七条 本办法自发布之日起施行，原《大连理工大学网络信息技术安全管理办法（试行）》（大工校发〔2017〕25 号）

同时废止。