大连理工大学研究生院文件

大工研发〔2020〕13 号

研究生院网络安全管理办法

为落实《中华人民共和国网络安全法》以及《大连理工大学网络安全管理办法》（大工办发〔2019〕52 号），保障研究生院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；维护内容安全，涉密信息等，现将有关办法规定如下：

1.组织机构及职责分工

研究生院信息化负责人为研究生院网络安全的责任人，负责规划、监督本单位的网络安全工作；研究生院信息化专干负责组织、协调本单位的网络安全具体工作，各业务办公室专干负责各业务办公室的网络安全具体工作，各专干工作安排由信息化负责人统筹和协调。

研究生管理信息系统的使用者（学生、导师、管理人员）有责任和义务遵守网络安全的相关规定，积极参与网络安全的建设和管理。

2.办公密码安全

各类办公密码包括但不限于研究生院各类办公密码包括信息

管理系统及数据库，办公计算机，打印机，led屏幕，网络设备，wifi及摄像头，微信公众号，微博等软硬件设备和自媒体平台的密码。

办公密码保护要清理弱密码，确定密码管理及使用人员，定期修改密码，避免密码泄露。其中弱密码包括简单密码、默认密码、通用密码、长期不变密码等。

研究生管理人员须做好办公密码保护以及电脑安全，不得造成密码泄露，不得私自授权他人使用密码。

3.个人信息保护

个人信息包括电子或者其他方式记录的能够单独或者与其他信息结合识别研究生、导师、管理人员或者反映研究生、导师、管理人员情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

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，严禁私自泄漏、贩卖、非法传播、非法获取，或通过信息网络或者其他途径发布、存储、使用和处理个人信息。

4.对于违反法律、法规，造成国家、学校和个人损失的，研究生院将依法配合学校、公安、网信等主管部门进行处理。

2020 年 10 月 17 日

大连理工大学研究生院　　2020 年 10 月 17 日印发