中共山东理工大学委员会办公室文件

鲁理工大党办发〔2019〕14号

党委办公室　校长办公室关于印发《山东理工大学网络安全管理规定》的通　知

各部门、各单位：

《山东理工大学网络安全管理规定》业经研究同意，现印发给你们，请认真遵照执行。

党委办公室

校长办公室

2019年7月1日

山东理工大学网络安全管理规定

第一章　总　则

第一条 为贯彻落实《中华人民共和国网络安全法》，建立健全学校网络安全管理体系，落实校园网络安全工作责任制，提升校园网络安全整体水平，进一步保障校园网络正常运行，特制定本规定。

第二条 本规定所称网络安全是指山东理工大学校园网内和经学校备案在公有云上构建的网络基础设施、网站、信息系统及数据内容等受到保护，以保证网络、系统及内容的安全性、完整性、可用性和可控性。

第三条 任何单位和个人不得利用学校网络和信息系统泄露国家或学校秘密、危害国家或学校安全，不得侵犯国家、集体和个人的合法权益，不得从事违法犯罪活动。使用校园网络系统或信息系统的用户，应接受并配合上级主管部门、公安司法机关或学校的网络安全检查。

第四条 依据“谁主管谁负责，谁运营谁负责，谁使用谁负责”的原则，落实网络安全分级责任制，实现明确责任、突出重点、自主防护、保障安全的目标。

第二章　管理机构与职责

第五条 学校网络安全与信息化工作领导小组全面负责学校网络安全与信息化工作，负责制定网络安全相关政策，统筹指导学校网络安全建设和人员岗位设置，提出学校网络安全工作的任务和要求，审定学校网络安全工作计划和经费投入机制，研究处

理重大网络安全事件等。

第六条 学校网络安全与信息化工作领导小组办公室（以下简称“网信办”），执行上级网络安全部门的政策和要求，落实网络安全与信息化工作领导小组的任务要求，负责学校网络安全具体管理工作。主要职责如下：

1.根据网络安全实际情况，拟订学校网络安全工作计划；

2.统筹协调和监督管理各单位网络安全工作，审核各部门、各单位网络安全管理制度，检查网络安全管理制度落实情况；

3.组织监测全校网络运行情况，评估网络安全现状，形成全校网络安全报告；负责委托网络安全服务机构对学校信息系统进行安全风险检测评估，落实相关改进措施；

4.组织审核拟在校园网内实施的网络安全方案和方法，组织论证拟在校园网内部署的网络安全设备和系统；

5.核定校园网内信息系统安全等级及其安全管理制度；

6.发布涉及网络安全的通知、公告；

7.组织开展面向各单位网络安全管理人员的技术培训；组织开展全校网络安全宣传教育；

8.协助公安司法机关查处各种有关网络安全的违法违纪行为。

第七条 网络信息中心负责学校主干网络和关键信息系统的安全，同时负责所属各信息系统的安全。主要职责如下：

1.拟订学校主干网络和关键信息系统的安全管理制度。切实落实安全管理制度，保障学校主干网络和关键信息系统的安全；

2.建立健全和落实所属各信息系统的安全管理制度；

3.加强技术人员队伍建设，不断提高防范、应对校园网络安全事件的能力；

4.为校内其他单位提供网络安全相关技术支持和协助。

第八条 各部门、直属单位、学院和其他单位负责本部门单位的网络安全工作。主要职责如下：

1.负责本部门单位所属信息系统和自建网络系统的安全，包括设备设施安全、系统运行安全和内容数据安全；

2.建立健全和落实本部门单位网络安全管理制度；

3.监控本部门单位所属信息系统和自建网络系统的运行状态，及时发现和消除安全隐患。如果发现危及全校网络安全的情形或者有害信息后，必须及时向网信办报告；

4.组织开展对本部门单位师生员工的网络安全教育。

第九条 各部门、各单位的党政主要负责人是本部门单位的网络安全第一责任人，对本部门单位的网络安全负领导责任。

第十条 各部门、各单位必须指定网络安全管理员，承担本单位网络安全的具体工作。各部门单位应当及时向网信办报备网络安全管理员相关信息。网络安全管理员一般应具有相关专业知识背景，掌握网络安全相关技术，积极参加学校组织的安全培训。

第三章　网络系统安全

第十一条 学校网络系统分为学校主干网络和单位自建网络两级。

第十二条 学校主干网络由学校统筹建设和管理。网络信息中心负责学校主干网络的线路铺设与维护、设备部署与运维、流量监测与管控，保障学校主干网络的安全畅通。各校区间网络链

路应当实现冗余互联，做到核心设备冗余热备。校园网络应当部署相关网络安全设备，实现对网络攻击行为的实时监测和告警，实现对恶意代码的实时检测和防护。

第十三条 校园网络系统对外采用统一出口，实现一体化管理。网络信息中心负责管控校园网络对外的统一出口，负责统一管理所有出口链路的公网 IP 地址。校园网络实现多出口链路，所有出口链路需接入防火墙、入侵防御系统等安全设备防护。

第十四条 校园网络系统对内实行按需接入，采取实名管理。网络信息中心负责校园网络的接入管理，接入校园网络的每个系统和每件设备都应具有明确的属主。根据工作需要，各单位自建网络可以申请接入学校主干网络。

第十五条 各单位根据工作需要建设内部网络系统。各单位内部网络系统如果需要接入学校主干网络，应向网络信息中心提供内部网络系统的拓扑结构、系统组成和功能应用等要素，并通过网络信息中心的综合评估。

第十六条 在建筑物设计与施工过程中，建设单位就弱电工程部分应征求网络信息中心意见，相关设计方案须经过网络信息中心审核，报网络安全与信息化工作领导小组审批。在建筑物施工完成后，弱电工程部分须由网络信息中心参与工程验收。

第十七条 在维修或拆除涉及校园网络的建筑物时，在维护或开挖涉及校园网络的道路时，须事先通知网络信息中心，以保护校园网络设备设施的安全。

第十八条 加强各楼宇内弱电间的管理，涉及校园网络的弱电间原则上由网络信息中心单独使用。学校自建或与校外合作单

位建设的弱电管网由网络信息中心统一管理，任何单位使用弱电管网需提供设计和施工方案，并经网络信息中心审核，报网络安全与信息化工作领导小组审批，方可施工。

第十九条 除网络信息中心外，严禁其他单位或个人以任何方式登录校园网络主干的各类设备，实施修改、设置、删除等操作。严禁任何施工单位或个人以任何理由损毁校园网络设备设施。

第二十条 师生员工使用校园网络，采取“实名注册、认证上网”制度，由网络信息中心负责实施。

第四章 信息系统安全

第二十一条 学校各信息系统实行安全等级保护。由网信办参照国家标准《信息系统安全等级保护基本要求（GB/T 22239-2008）》，审核确定校园网内各信息系统的安全等级。信息系统包括关键信息系统、重要业务系统、各类应用业务系统和各级各类网站系统。

第二十二条 关键信息系统由学校统筹建设和管理。网络信息中心负责由统一身份认证平台、云计算平台、共享数据中心等构成的关键信息系统的具体建设和运营工作。

第二十三条 各部门、各单位负责所属信息系统的运营，应签订网络安全承诺书（附件 1），按网络安全等级保护的要求，制定安全管理制度和操作规程，采取相应的安全保护技术措施，保障信息系统免受干扰、破坏或者未经授权的访问，防止信息系统数据泄露或者被窃取、篡改。相关安全管理制度等须经过网信办审核。

第二十四条 信息系统安全管理制度应当明确安全负责人、

各项安全保护责任和安全保护技术措施。

第二十五条 信息系统的注册用户应实名认证，由信息系统的运营者负责实名认证的实施。

第二十六条 各部门、各单位在建设、升级网站或信息系统时，须同步建立网络信息安全体系，充分考虑信息系统的安全防护，在技术方案、经费预算及运行维护等方面予以落实。关键信息系统和各部门单位所属重要信息系统，应当具有支持业务稳定、持续运行的性能，并且安全技术措施必须同步规划、同步建设、同步使用。

第二十七条 根据工作需要新建或升级在校园网内运行的信息系统时，各部门、各单位应事先向网信办提出申请；同时应就信息系统设计方案向网络信息中心征求意见。在上线运行前，信息系统须通过由网络信息中心组织的安全检测。

第二十八条 根据有关要求，学校所有信息系统、网站均需办理审批备案手续。*.sdut.edu.cn 域名已由学校统一备案，网站域名非以上格式的，由建设单位报网络信息中心和政府有关部门备案。未经审批备案的信息系统不属于学校官方行为，不得使用校名、校徽等学校标识，一切责任由建设单位和个人承担。

第二十九条 学校电子邮件系统是师生的工作邮箱，开户需实行实名制。一个用户只能开设一个邮件账号；一个单位原则上开设一个公共邮箱。用户停止账号使用时，必须通知网络信息中心注销其账号。

第三十条 电子邮件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。用户必须对用户名和密码的安全负责，

并对以其用户名进行的所有活动负责。用户若发现任何非法使用其用户账号或存在安全漏洞情况，应立即报告网络信息中心。

第三十一条 网络信息中心负责对校园网电子邮件系统使用情况进行监督、检查。对于非法使用其用户账号发送垃圾广告邮件、存在安全漏洞的账户，网络信息中心有权停止和注销其账号。

第三十二条 网络信息中心定期对全校的网站及信息系统开展安全检查，检查不合格的网站或信息系统，视其漏洞级别暂停其外网访问，同时通知责任单位限期整改并提交《网络安全事件整改情况表》。整改完成并经复查合格后，方可恢复正常访问。

第五章 数据安全

第三十三条 学校所有信息系统的数据作为学校的无形资产和战略资源，纳入学校统一管理，实现数据的统一管控，为学校教学、科研、管理等提供信息服务和支撑。数据管理部门包括数据统筹管理、数据生产、数据使用三部分。

第三十四条 网络信息中心是学校数据资产的统筹管理部门，负责主数据中心、数据仓库平台、数据共享平台的安全管理，并规范数据服务流程，确保数据流向清晰，实现数据可控、可管、可查。

第三十五条 数据生产部门为权威数据的单一来源部门，负责数据收集、维护、使用、备份、归档等全程安全，需遵循学校信息标准规范及数据服务规范。同时，向网络信息中心提供数据字典、数据接口以及数据库访问权限。

第三十六条 数据使用部门需根据自己的需求填写《山东理工大学数据使用申请表》（附件 2），向数据生产部门提出数据使

用申请，获得数据生产部门批准后由网络信息中心提供数据交换接口。获得数据的使用单位要切实做好数据的安全保护工作，不得将数据用于申请用途以外的活动。

第三十七条 学校数据信息主要用于教学、科研、管理等工作，各部门单位和个人要对自己所管理的数据负责，保证数据安全，防止数据泄漏和丢失。未经学校批准，任何部门单位和个人不得擅自对他人或校外单位提供信息系统数据。

第三十八条 校园网所有用户通过校园网发布信息必须严格遵守有关法律法规和学校的管理规定，并对所发布的信息负责。

第三十九条 各部门、各单位要按照国家及学校有关规定，严格执行信息发布审核制度，严禁在校园网上发布或传递涉及国家秘密的信息，未经审核的信息内容不得发布。

第四十条 党委宣传部负责对校园网信息进行监督、检查。对于不良有害信息，在第一时间联系相关部门进行处理；涉及违法行为的，应立即向公安机关报案。

第六章　应急处置

第四十一条 网信办按照规定通报网络安全监测预警信息。各部门、各单位应当根据国家、地方网络安全部门发布的预警信息及时做好相应防范工作，必须按照网信办通报的预警信息，做好相应处置工作。

第四十二条 网信办协调网络信息中心和各部门单位，制定网络安全事件应急预案。网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第四十三条 各部门、各单位网络安全管理人员须熟悉本部门单位网络安全事件应急处置措施。各部门单位应当定期开展网络安全事件应急预案演练。

第四十四条 校园网内发生网络安全事件，应当立即启动网络安全事件应急预案，各部门单位和相关人员须按照应急预案规定进行处置。

第七章　奖 惩

第四十五条 网信办定期开展全校网络安全工作的检查，每年向学校网络安全与信息化工作领导小组汇报各部门单位网络安全工作汇总信息。对网络安全工作成绩显著的部门单位和个人，学校给予表彰和奖励；对违反网络安全管理制度、网络安全工作存在不足和隐患且逾期不改的部门单位，学校给予通报批评。

第四十六条 对拒不执行网络安全管理相关制度、漠视网络安全工作以至造成重大事故和案件的部门和单位，学校将追究该单位主要负责人和直接责任者的责任。对触犯法律的，将移送公安司法机关处理。

第四十七条 对损坏校园网络系统或信息系统设备设施的个人，学校将视其情节轻重追究责任，如触犯法律应移交公安司法机关处理。

第八章　附　则

第四十八条 违反本管理规定的，将视情节采取以下措施处理：

（一）限期整改；

（二）封账号或端口至安全问题排除；

（三）报学校有关职能部门或当事人所在单位处理；

（四）触犯法律法规的，移交司法等相关部门处理。

第四十九条 本规定由党委宣传部、网络信息中心负责解释。

第五十条 本规定自印发之日起执行。原《山东理工大学网络安全管理暂行规定》（鲁理工大党办发〔2017〕10 号）同时废止。

附件：1.山东理工大学网络安全承诺书

2.山东理工大学数据申请表

附件 1

山东理工大学网络安全承诺书

本单位郑重承诺遵守本承诺书所列事项，对所列事项负责，如有违反，由本单位承担由此带来的相应责任。

一、遵守《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际互联安全保护管理办法》和《信息安全等级保护管理办法》，遵守国家其他信息技术安全的有关法律、法规和行政规章制度，以及学校相关规章制度。

二、成立本单位网络信息安全小组，设立网络信息安全负责人和安全员并向学校网络与信息安全领导小组办公室报备，小组人员变动时及时重新报备。

三、不利用所属网络与信息系统危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

四、党政主要责任人已明确属地管理责任，知悉本部门单位集体和个人对所属网络与信息系统的管理义务和管理责任。

五、完善本单位的网络安全管理，建立健全网络安全责任制和相关规章制度、操作规程，责任落实到人。

六、妥善管理本单位及其下属科室部门、中心、科研院所、课题组及学术会议等利用校园网络举办活动、开通网站及使用校园无线网络、应用系统等情况，加强人员安全教育，配合网络信息中心完成上网人员管理、日志留存等相关安全工作。

七、完善本单位的信息系统安全，落实信息系统安全等级保

护制度，提高信息系统安全防护能力。

八、对所属信息系统进行安全监测，留存六个月以上网络状态、安全事件等相关网络日志，并对监测发现和通报的安全问题及时整改。

九、加强终端计算机安全，落实软件正版化，推进具有自主知识产权的软硬件应用，规范工作人员的使用行为。

十、规范本单位数据采集和使用，不采集超越职能范围的数据，保障数据安全。

十一、提升应急响应能力，制定本单位应急预案，组织开展应急演练。

十二、保障网络安全工作经费，将经费纳入年度预算并确保落实到位，保障信息技术安全工作开展。

十三、加强本单位网络安全教育，组织工作人员参加培训，提高管理人员的安全意识和技术人员的防护能力。

十四、当信息系统发生网络安全事件，迅速进行报告与处置，将损害和影响降到最小范围，并按照要求及时进行整改。

十五、若违反本承诺书有关条款和国家相关法律法规的，本单位愿承担责任。

十六、本承诺书自签署之日起生效。

单位盖章

单位负责人（签字）：

年　　月　　日

附件 2

山东理工大学数据使用申请表

日期：　　年　月　日

<table>
<tr><td>申请单位</td><td colspan="5"></td></tr>
<tr><td>数据清单</td><td colspan="5"></td></tr>
<tr><td>申请用途</td><td colspan="5"></td></tr>
<tr><td colspan="6">申请单位联系人</td></tr>
<tr><td>姓名</td><td></td><td>Email</td><td></td><td>电话</td><td></td></tr>
<tr><td colspan="6">申请单位审批意见：

单位公章：　　负责人（签字）：　　日期：　　年　月　日</td></tr>
<tr><td colspan="6">数据生产部门审批意见：

单位公章：　　负责人（签字）：　　日期：　　年　月　日</td></tr>
<tr><td colspan="6">网络信息中心办理情况：

办理人（签字）：　　日期：　　年　月　日</td></tr>
<tr><td colspan="6">说明：1.网络信息中心提供的数据信息均为来源于各业务系统的权威数据，例如,本科生数据来源于教务处，研究生数据来源于研究生院，留学生数据来源于国际教育学院，教职工数据来源于人力资源处。
2.网络信息中心为我校各单位提供统一的数据交换接口，申请数据获取的单位不得将获取数据传播给其他单位使用。
3.学校数据信息主要用于教学、科研、管理、后勤服务等，申请数据获取的单位不得将数据信息用于申请用途外的活动。
4.违反上述约定，申请单位将负相关责任。
5.此表由网络信息中心备案。</td></tr>
</table>

中共山东理工大学委员会办公室　　2019 年 7 月 1 日印发