青岛理工大学文件

青理工校发〔2018〕15号

关于印发
《青岛理工大学网络安全管理办法》的通知

各部门、学院、单位，临沂校区：

经学校研究同意，现将《青岛理工大学网络安全管理办法》印发给你们，请遵照执行。

青岛理工大学

2018年7月5日

青岛理工大学网络安全管理办法

第一章　总 则

第一条　为加强学校网络安全管理，提高网络安全防护能力和水平，保障学校各项事业健康有序发展，根据《中华人民共和国网络安全法》、《教育部关于加强教育行业网络与信息安全工作的指导意见》、《教育部、公安部关于全面推进教育行业信息安全等级保护工作的通知》等法律法规，结合学校实际，制定本办法。

第二条　本办法所称网络安全工作，是指为使由学校建设或管理并支撑学校教学、科研和管理等各项事业的信息资产的机密性、完整性、可用性等得到保持、不被破坏，为防止发生网络攻击、信息破坏、有害程序入侵、信息化设备设施故障等发生而开展的预防和防御工作。

第三条　学校按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，建立健全网络安全责任体系，学校各单位、全体师生员工应依照本办法要求及学校相关标准规范履行网络安全的义务和责任。

第二章　组织机构与职责

第四条　学校网络安全领导小组负责统一领导、统一谋划、统一部署全校网络安全工作。

第五条　学校网络安全领导小组设网络安全领导小组办公室，办公室设在信息化建设与管理中心，具体负责学校网络安全

管理工作。职责包括：

1、 制定网络安全总体规划，并组织实施；

2、 拟定网络安全管理规章制度，制定网络安全标准规范；

3、 组织开展信息系统安全等级保护工作；

4、 负责网络安全应急管理，协调处理与政府网络安全管理部门的关系；

5、 组织网络安全宣传和教育培训工作；

6、 负责网络安全监督检查工作；

7、 负责网络安全的其他工作；

第六条 学校各单位是本单位网络安全工作的责任主体，各单位主要负责人是本单位网络安全工作的第一责任人，负责按本办法落实网络安全工作。各单位要明确指定本单位各应用系统、互联网站和所申请数据中心资源的运行、维护和安全责任人，将责任人名单报备网络安全领导小组办公室，人员变动时应及时调整并报备。原则上，安全责任人变动一年内不得超过两次。

第三章 校园网络管理

第七条 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。

第八条 校园网络与互联网及其他公共信息网络实行逻辑隔离，由信息化建设与管理中心统一出口、统一管理和统一防护。任何单位和个人在校园内不得擅自通过其他渠道进入互联网及其他公共信息网络。

第九条 校园网络接入单位负责提供本单位所需的网络设备间，协助解决网络布线和设备安装所需空间，网络设备电源保障由后勤处负责。

第十条 师生员工接入校园网络，实现“实名注册，认证上网”制度；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。

第十一条 由学校引入的第三方校园网络运营服务单位，须与学校网络安全领导小组办公室签订网络安全责任书。第三方运营范围内发生的网络安全事件由其负全部责任。信息化建设与管理中心负责巡查监督，对于未经学校允许或服务合同到期或未与学校网络安全领导小组办公室签订网络安全责任书的第三方校园网络运营服务单位，有权采取立即停止对其设备供电等措施，后勤处应给予协助。

第四章 数据中心管理

第十二条 数据中心主要包括支撑学校信息系统或网站的物理环境、软硬件设备设施、云计算平台、学校中心基础数据库、统一数据交换平台和统一身份认证平台等信息化基础设施和平台。信息化建设与管理中心负责数据中心的建设和运行维护管理。

第十三条 信息化建设与管理中心负责数据中心的物理安全、网络安全和主机安全。数据中心的资源使用单位负责所使用的操作系统、业务数据库系统、应用系统和数据的安全。

第十四条 信息化建设与管理中心负责学校基础数据库和统一数据交换平台的建设和安全管理，负责各单位业务数据库与基础数据库之间完成数据交换和共享。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；对本单位业务数据库的系统安全、数据安全及所申请的共享数据的安全负责。

第十五条 信息化建设与管理中心负责统一身份认证系统的建设运行和安全管理，校内各单位负责本单位应用系统的权限管理及安全，建设面向师生服务的应用系统时，要与统一身份认证系统进行认证集成并向信息化建设与管理中心备案。

第十六条 全校各单位应依托校内数据中心实施本单位应用系统或互联网站建设，需要使用校外数据中心的须报网络安全领导小组办公室审批；严禁使用设置在境外的数据中心。涉及学校基础数据、师生个人信息或敏感信息的应用系统和互联网网站，禁止放置在校外数据中心。

第十七条 学校数据中心实行准入管理，信息化建设与管理中心负责制定数据中心的技术规范和标准，对各单位拟上线系统进行安全检测，符合技术规范标准并检测通过的系统方可准许上线运行。

第十八条 数据中心使用单位须遵守数据中心使用管理规定，执行相关技术标准，按需申请、有序使用数据中心资源，不得利用数据资源从事任何危害网络安全的活动。

第五章 信息系统安全管理

第十九条 各单位要按照国家信息系统等级保护制度的相关法律法规、标准规范和要求落实信息系统安全等级保护制度。

第二十条 各业务主管部门为相应业务系统（含移动客户端软件）的责任部门，应制定专门人员负责系统的建设、运维维护和安全管理。信息系统原则上由业务管理部门运维，特殊情况可以委托信息化建设与管理中心运维。

第二十一条 各业务主管部门新建的信息系统必须符合由信息化建设与管理中心统一制定的建设规范和编码标准。

第二十二条 各业务信息系统经试运行后，由业务主管部门组织初步验收，出具初步验收报告，并向网络安全领导小组办公室申请进行信息安全等级保护测评。网络安全领导小组办公室组织开展信息安全等级保护测评，形成测评报告；未进行信息安全等级保护测评或测评不合格的业务系统不能接入校园网络。

第二十三条 各单位要保留不少于6个月的系统维护日志。各单位管理员或个人要妥善保管好账号和密码，定期更新密码，防止密码外泄，因此导致的网络安全事件由各单位负责。运维服务需要外包的信息系统，应选择具备相应资质的服务商，并签订服务合同和保密协议。

第六章 互联网站安全管理

第二十四条 学校各单位是所属网站建设、运行、维护、安全和内容审查的直接责任主体，负责所属网站建设、日常管理和安全维护等工作。

第二十五条 信息化建设与管理中心为网站建设、运行和维护的技术支撑单位，负责学校网站群平台建设、运行和维护，负责网站安全监测、检测和预警，参与网站安全应急处置。

第二十六条 各单位设立互联网站，原则上基于学校网站群平台建设。未运行在学校网站群平台的网站，须按信息安全等级保护的相应规范落实信息安全防护措施。未依托学校网站群平台新建的网站，须通过信息化建设与管理中心组织的安全检查方可正式上线。

第二十七条 保密办公室是网站内容保密审查的管理部门，对网站执行保密法律法规的情况进行定期或不定期检查。

第二十八条 党委宣传部是网站内容建设的管理部门，负责对校内单位网站内容建设进行业务指导。学校中文主页总体框架设计、图片更换、内容建设由党委宣传部负责。学校英文主页总体框架设计、图片更换、内容建设由国际交流处负责。

第二十九条 信息化建设与管理中心负责建立网站安全监测平台，监控校内各单位网站的安全性和可用性，对异常情况及时通报预警，并可视情况实施暂时关停网站或关闭网站互联网服务。各单位在接到通报后应主动配合，及时处置异常情况。逾期未按要求整改的，信息化建设与管理中心将关停网站。

第三十条 信息化建设与管理中心、网站开办单位应加强技术服务外包管理。对需要进行服务外包的网站，应选择具备相应资质的服务提供商，并签订服务合同和保密协议。

第三十一条 重要时期或重大活动安全保障期间，信息化建设与管理中心可依据有关部门要求并根据实际需要临时关停网站或关闭网站互联网服务。

第七章 应急处置

第三十二条 各单位要按照学校网络安全事件报告与处置流程，做好应急事件处置工作。

第三十三条 各单位要按照安全事件早发现、早报告、早控制、早解决的要求建立本单位网络安全值守制度，制定安全事件应急预案和处置方案，组织应急演练。

第九章 保障措施

第三十四条 学校保障网络安全及信息化发展所需的人员编制和经费投入，建设高水平网络安全技术支撑队伍。

第三十五条 网络安全领导小组办公室负责制定网络安全教育培训规划，开展面向全校的培训和宣传教育，提高师生员工的安全和防范意识，培养良好的媒介素养和规范、文明的用网行为。

第三十六条 信息化建设与管理中心负责组织开始网络安全管理和技术人员专业培训。

第三十七条 学校建立完善网络安全工作检查考核、责任追究和倒查制度，将网络安全列为各单位领导班子和领导干部目标管理、业绩评定、年度考核、奖励惩处和干部选拔任用的重要内容和依据。

第九章　责任追究

第三十八条　有关单位在收到网络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。

第三十九条　各单位要按照网络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安全事件。如有瞒报、缓报、处置和整改不力等情况，由网络安全领导小组进行约谈或通报。

第十章　附则

第四十条　本办法自公布之日起实施，由网络安全领导小组办公室负责解释。

青岛理工大学校长办公室　　2018 年 7 月 5 日印发