齐鲁师范学院文件

齐鲁师院政综字〔2022〕2号　　签发人：林松柏

关于印发《齐鲁师范学院网络信息安全管理办法》的通知

各部门、单位：

《齐鲁师范学院网络信息安全管理办法》已经党委研究通过，现予以印发，请遵照执行。

齐鲁师范学院

2022年4月11日

齐鲁师范学院网络信息安全管理办法

第一章　总 则

第一条　为加强学校网络信息安全管理，推进学校信息系统(含网站)的安全等级保护工作，提高网络信息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《关于加强教育行业网络与信息安全工作的指导意见》（教技〔2014〕4号）、《关于全面推进教育行业信息安全等级保护工作的通知》（教技〔2015〕2号）等文件要求，结合学校实际，特制定本办法。

第二条　本办法所称网络信息安全工作，是指为保护由学校建设、运行、维护和管理并支撑学校教学、科研、管理等各项事业的信息资产(信息及信息系统)的机密性、完整性、可用性和不被破坏所开展的相关管理和技术工作。

第三条　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，建立健全网络信息安全责任体系，学校各部门（单位)和全体师生员工应依照本办法和相关标准规范履行网络信息安全的义务和责任。

第二章　管理机构及工作职责

第四条　学校党政主要负责人是学校网络信息安全的第一

责任人，分管网络安全和信息化工作的学校领导协助主要负责人履行学校网络信息安全职责。

第五条　学校成立网络安全和信息化工作领导小组，网络安全和信息化工作领导小组办公室(以下简称学校网信办)下设办公室，学校网信办统筹学校网络安全与信息化建设工作，负责学校网络信息安全防护体系的建设、运行维护、技术指导和服务支持。

第六条　学校各部门（单位）对本部门（单位）网络安全和信息化工作负主要责任，各部门（单位）主要负责人是本部门（单位）网络安全和信息化工作第一责任人，负责按本办法落实网络信息安全工作。

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终端的计算机网络，包括校园内由学校建设管理的有线网络和无线网络。

第八条　校园网络规划方案由学校网络安全和信息化工作领导小组制定。主要包括数据中心、弱电管网、认证计费、安全防护等方面建设方案的规划制定。

第九条　校园网运行维护的具体工作由网络信息中心负责。包括数据中心、综合布线、网络设施、网管系统、域名管

理、安 全防护、认证计费、网络接入等多个层面的运行维护。学校所有基建、改造修缮工程应将工程范围内校园网络建设纳入工程设计、实施和竣工验收范畴

第十条　校园网络与互联网及其他公共信息网络实行逻辑隔离，由网络信息中心统一出口、统一管理和统一防护。未经批准，学校各部门（单位）在校园内不得擅自通过其他渠道接入互联网及其他公共信息网络。

第十一条　网络信息中心应采取访问控制、安全审计、完整性检查、入侵防范、恶意代码防范等措施加强校园网络边界防护。

第十二条　校内师生员工接入校园网络，实行“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。网络接入实名管理制度由网络信息中心负责实施。涉密信息系统不得接入校园网络，应与校园网络物理隔离。

第十三条　严禁任何单位和个人未经学校同意，利用校园网络及设施开展经营性活动。

第四章　数据中心管理

第十四条　数据中心主要包括支撑学校信息系统的物理环境(其中包含网络中心机房)、软硬件设备设施、云计算平台、学

校中心数据库(其中包含基础数据库)、数据共享交换平台、统一身份认证平台及统一信息门户等信息化基础设施和平台。

第十五条　网络信息中心负责数据中心物理环境、软硬件设备设施和云计算平台的建设和安全管理;根据信息系统安全等级要求，采取必要的技术措施对数据中心进行分区、分域管理，对不同安全域之间实施访问控制，加强防护。

第十六条　网络信息中心负责学校中心数据库、数据共享交换平台的建设和安全管理，负责基础数据库与各部门业务数据库之间完成数据交换和共享。各部门负责建设、维护本部门业务应用系统所配套的业务数据库，并对本部门业务数据库及所申请的共享数据的安全负责。

第十七条　统一身份认证平台为学校信息系统提供统一的身份管理、安全的认证机制及标准接口。学校各部门建设面向师生服务的应用系统时，PC端应使用统一身份认证平台进行身份认证，移动端入口统一接入“智慧师院”APP。网络信息中心负责统一身份认证平台的安全，学校各部门负责本部门应用系统的权限管理及安全。

第十八条　学校各部门(单位)一般应依托学校数据中心开展信息系统建设。需使用校外数据中心的,须报学校网信办审批。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，不得部署在校外数据中心。未经批准，严禁使用境外数据中心。

第十九条　数据中心的使用部门（单位）应遵循数据中心相关管理制度和技术标准，按需申请、有序使用，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信息安全的活动。

第五章　信息系统建设、运行和维护管理

第二十条　学校按照“同步规划、同步建设、同步运行”的原则，规划、设计、建设、运行、管理信息安全设施，建立健全网络信息安全防护体系，全面实施信息系统安全等级保护制度。

第二十一条　学校网信办负责制定学校信息系统项目规划和顶层设计，学校各部门（单位）根据业务需求，提出信息系统建设申请。纳入学校规划的核心信息系统建设需求将优先支持。

第二十二条　学校网信办负责统筹学校信息系统安全等级保护工作，组织学校各部门（单位）开展信息系统定级、系统备案、等级测评、建设整改，具体负责信息系统台账管理、等级评审、系统备案、监督检查工作。按照“自主定级、自主保护”的原则，信息系统建设单位是信息系统安全等级保护的责任主体，具体负责系统定级、建设整改、安全自查，协助系统备案、等级测评并接受有关部门监督检查。网络信息中心是信息系统安全等级保护工作的技术支撑保障部门，负责信息技术安全防护体系建设和等级测评组织工作，参与监督检查工作，并协助学校各部门进行系统定级、

建设整改。

第二十三条　学校鼓励信息系统建设部门优先采购安全可靠、技术成熟和服务优质的成品软件。没有相应成品软件或成品软件不适应实际需求的，可按照学校采购与招标相关管理办法，委托资质和信誉良好的软件开发商进行开发。

第二十四条　信息系统在建设阶段应确定安全保护等级，同步落实安全保护措施和测评经费。信息系统投入试运行后，由建设单位初步验收，出具初步验收报告。对于安全等级第二级以上(含第二级)的信息系统，信息系统建设单位必须组织等级测评，向网络信息中心提交等级测评备案表及备案报告。信息系统通过初步验收和信息安全保护等级测评后，方可组织竣工验收。

第二十五条　信息系统开发环境、测试环境和运行环境应严格隔离，网络信息中心负责上述环境的建设、运行、维护和管理。

第二十六条　信息系统建设单位可自行或委托网络信息中心维护信息系统，亦可根据实际需要，委托校外单位维护信息系统。涉及重要业务或大量师生员工信息的核心信息系统以及安全等级第二级以上(含第二级)的信息系统，原则上必须托管在网络中心机房，日常更新由信息系统建设单位自行维护，服从网络信息中心的统一管理。

第二十七条　信息系统建设单位应定期对终端计算机和承担网络与信息系统运行的关键设备(服务器、安全设备、网络设

备、虚拟机、云主机、云空间等)进行安全检查，通过记录、检查系统和用户活动信息，及时发现系统漏洞，处置异常访问和操作。

第二十八条　信息系统建设单位应制定信息系统使用与维护的管理制度，规范信息系统使用者和维护者的操作行为。

第二十九条　对于安全等级第二级以上(含第二级)的信息系统，学校网信办将定期组织开展等级测评，查找、发现并及时整改安全问题、漏洞和隐患。根据国家和教育行业有关标准规范，三级以上系统每年进行一次测评，二级系统每两年进行一次测评。

第六章　信息系统数据安全管理

第三十条　信息系统数据是指信息系统收集、存储、传输、处理和产生的各种电子数据，包括但不限于网站内容、业务数据、网络课程、图书资源、日志记录等。

第三十一条　信息系统数据的所有者是数据安全管理的责任主体，应当落实管理和技术措施，规范数据的收集、存储、传输和使用，确保数据安全。

第三十二条　信息系统数据收集应遵循“最少够用”原则，　不得收集与信息系统业务无关的个人信息。按照“谁收集，谁负责”的原则，收集个人信息的单位是个人信息保护的责

任主体，应当对其收集的个人信息严格保密，并建立健全相关保护制度。

第三十三条　信息系统建设单位应制定数据备份与恢复计划，根据业务实际需要对重要数据和信息系统进行备份，定期测试备份与恢复数据，确保备份数据和备用资源的有效性。

第七章　互联网网站安全管理

第三十四条　学校各部门开办互联网网站应遵守相关规章制度并提交新入网申请。

第三十五条　网络信息中心统一建设学校网站集群平台并负责纳入该平台网站的技术安全。未纳入学校网站集群平台的网站，其技术安全由网站开办单位负责。学校各部门开办互联网网站应优先选择学校网站集群平台，集群平台不能满足需求时可委托其他供应商建设。网站投入试运行，须通过网络信息中心组织的安全检查后，方可正式上线。

第三十六条　学校各部门应建立完善的网站信息发布与审核制度，确定负责内容编辑、内容审核、内容发布的人员名单，明确审核与发布程序，保存相关操作记录。网站发布的信息安全由网站开办单位负责。

第三十七条　学校各部门应建立网站值守制度，组织专人对网站进行监测，发现网站运行异常及时处置。

第三十八条　学校各部门不得提供电子公告服务和匿名FTP 服务。

第八章　电子邮件安全管理

第三十九条　网络信息中心为学校各部门和师生员工提供电子邮箱，并负责学校电子邮件的安全管理。学校各部门和师生员工应将学校电子邮箱作为工作邮箱，使用时应遵守学校电子邮箱管理等相关规章制度。

第四十条　网络信息中心应采取必要的技术和管理措施，加强电子邮件系统的安全防护，减少垃圾邮件、病毒邮件侵袭。

第四十一条　师生员工须对使用其电子邮箱账号开展的所有活动负责，应妥善保管本人使用的电子邮箱账号和密码，确保密码具有一定强度并定期更换。师生员工如发现他人未经许可使用其电子邮箱，应立即通知网络信息中心处理。

第九章　终端计算机安全管理

第四十二条　终端计算机是指由学校师生员工使用并从事学校教学、科研、管理等活动的各类计算机及附属设备，包括台式电脑、笔记本电脑及其他移动终端。

第四十三条　终端计算机使用人按照“谁使用，谁负责”的原则，对其终端计算机负有保管和安全使用的责任。

第四十四条　终端计算机应定期进行系统补丁安装、安全防护软件安装升级及漏洞扫描等工作。

第四十五条　终端计算机应当设置系统登录账号和密码，禁止自动登录，登录密码应具有一定强度并定期更改。

第四十六条　终端计算机使用人应做好终端计算机的安全防范，如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网，及时处置。

第十章　网络信息相关人员安全管理

第四十七条　学校各部门（单位)应建立健全本部门（单位）的岗位信息安全责任制度，明确岗位及人员的信息安全责任，指定专人担任本部门（单位）的信息安全员。关键岗位的计算机使用和管理人员应签订信息安全与保密协议，明确信息安全与保密要求和责任。

第四十八条　学校各部门（单位）应加强人员离岗、离职管理，严格规范人员离岗、离职过程，及时终止相关人员的所有访问权限，收回各种身份证件、钥匙、徽章以及学校提供的软硬件设备，并签署安全保密承诺书。

第十一章　信息安全应急预案管理

第四十九条　学校网信办负责学校网络信息安全应急工作的统筹管理，网络信息中心负责信息安全应急工作的技术支撑和保障。

第五十条　学校网信办负责制定学校网络信息安全事件报告与处置流程，网络信息中心负责制定学校网络信息安全应急预案。

第五十一条　学校网信办定期组织网络信息安全应急演练。

第五十二条　学校各部门（单位）或师生员工均有义务及时向学校网信办报告网络信息安全事件，不得在未授权情况下对外公布、尝试或利用所发现的安全漏洞或安全问题。

第十二章　信息安全教育培训

第五十三条　学校网信办负责组织学校网络信息安全宣传和教育培训工作，建立健全相关制度。

第五十四条　学校网信办定期组织网络信息安全管理人员、技术人员以及信息员开展相关业务的专业技能培训，提高师生员工的安全和防范意识。

第十三章　信息安全检查监督

第五十五条　学校各部门（单位）应定期对本部门（单位）信息系统的安全状况、安全保护制度及措施的落实情况进行自查，如果本部门（单位）信息系统的等级保护内容发生变化，应及时报告网络信息中心。

第五十六条　学校网信办对学校各部门（单位）的网络信息安全工作落实情况进行检查，对发现的问题下达限期整改通知书，责成相关单位制订整改方案并落实到位。

第五十七条　学校网信办对年度安全检查情况进行全面总结，按照要求完成检查报告并报有关网络信息安全主管部门。

第十四章　信息安全责任追究

第五十八条　学校建立网络信息安全责任追究和倒查机制。

第五十九条　有关单位在收到网络信息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。

第六十条　学校各部门（单位）应按照网络信息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信息安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位责任人进行约谈或通报。

第六十一条　师生员工违反本办法规定的，由学校网信办

责令改正，并通报批评；拒不改正或者导致危害网络信息安全等严重后果的，根据学校有关规定给予纪律处分；触犯刑律的，移交司法机关处理。

第十五章　附 则

第六十二条　涉及国家秘密的信息系统，执行国家保密工作的相关规定和标准，由学校保密委员会办公室监督指导。

第六十三条　学校各部门（单位）可参照本办法制定相应的实施细则。

第六十四条　本办法由学校网络安全和信息化工作领导小组办公室负责解释，自发文之日起实施。学校原有相关规定与本办法不一致的，按本办法执行。

齐鲁师范学院院长办公室　　2022年4月11日印发