校办〔2019〕25号

泉州师范学院办公室关于印发

《泉州师范学院网络安全和信息化管理办法（2019年修订）》的通知

各学院、机关各部（处、室）、各直属单位：

现将《泉州师范学院网络安全和信息化管理办法（2019年修订）》印发给你们，请遵照执行。

泉州师范学院办公室

2019年11月15日

泉州师范学院党政办公室 2019年11月15日印发

# 泉州师范学院网络安全和信息化管理办法

# （2019年修订）

## **第一章 总则**

**第一条** 为加强对学校网络安全和信息化工作的统筹管理，提高学校网络安全能力和水平，推进信息化健康有序发展，根据《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》《互联网信息服务管理办法》等法律法规以及学校相关规定，制定本办法。

**第二条** 本办法所称网络安全和信息化，是学校信息化的基础设施、数据、信息系统等和为保障其完整性、可用性、保密性等得到保持、不被破坏所开展的相关管理和技术工作，以及相关技术标准规范、管理制度的制定等。

**第三条** 涉及国家秘密的和信息内容安全的不在本办法管理范畴内，由学校相关部门根据相关规定进行管理。

## **第二章 管理体制**

**第四条** 网络安全和信息化领导小组是学校网络安全和信息化的领导机构，负责学校网络安全和信息化建设的战略决策、实施监督，负责重大网络安全事件处理的决策指导，统筹网络意识形态工作等。

**第五条** 网络安全和信息化领导小组组成如下：

（一）组长：校党委书记、校长；

（二）常务副组长：分管网络安全和信息化工作的校领导；

（三）副组长：相关副职校领导

（四）成员：学校相关职能部门、图书馆和数学与计算机科学学院负责人

**第六条** 网络安全和信息化领导小组下设办公室（简称网信办）。网信办挂靠党委宣传部，主任由党委宣传部负责人兼任，副主任由网络中心负责人兼任。党委宣传部负责统筹学校网络安全和信息管理、网络意识形态工作；网络中心是学校网络安全和信息化的技术支撑单位，负责网络安全和信息化的建设实施、运维管理、技术指导和服务支持。

**第七条** 网信办是学校网络安全和信息化的管理机构，负责学校网络安全和信息化的总体规划与实施，组织制定和实施技术标准规范、用户使用协议，落实网络安全等级保护制度，开展日常监督检查与考评，应急协调和处置重大网络安全事件，落实网络意识形态工作责任制等。

**第八条** 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各单位负责本单位主管、运维、使用的信息系统和内部网络。各单位应根据本单位信息化建设情况，按照学校相关规定，建立网络安全和信息化管理制度和应对措施。

**第九条** 各单位主要负责人是本单位网络安全和信息化的第一责任人，负责规划、监督本单位的网络安全和信息化建设；本单位网络安全和信息化的分管负责人是直接责任人，负责组织、协调、落实本单位的网络安全和信息化管理工作；信息系统和网络的管理员是相关系统的直接责任人。

**第十条** 关键岗位的管理人员和技术人员应与网信办签订网络安全保密协议，明确保密要求和责任。

**第十一条** 各单位和用户作为校园网和数据的使用者、信息化建设的参与者，有责任和义务遵守学校网络安全的相关规定。

## **第三章 校园网管理**

**第十二条** 校园网由网信办统一规划、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、挪用校园网设施。

**第十三条** 校园网涉及光缆布线、网络机房、网络地址分配、域名管理、安全防护、认证计费、网络接入与运维等方面，由网络中心统一负责建设、运行、维护和管理。学校规划建设部门负责校园地下管网的统一规划建设和维护管理。学校所有基建、改造、修缮工程应将工程范围内的校园网建设纳入工程设计、实施和竣工验收范畴。

**第十四条** 校园网与互联网及其他公共信息网络实行逻辑隔离，由网络中心统一出口、统一管理和统一防护。未经批准，各单位不得擅自通过其他渠道接入互联网及其他公共信息网络。

**第十五条** 校园网和信息系统接入互联网须采取访问控制、安全审计、访问日志记录、完整性检查、入侵防范、恶意代码防范、身份认证等措施加强技术防护直至符合相关法定规范。

**第十六条** 校园网入网实行实名制，实行“实名注册、认证上网、一人一号”。用户必须通过网络中心实名登记后方可按照入网要求使用校园网，未经登记不得以任何方式私接校园网，严禁盗用其他用户信息使用校园网。

**第十七条** 学校非涉密信息系统接入校园网，实行接入审批、备案、年审登记制度。涉密信息系统不得接入校园网。

**第十八条** 校园网接入单位负责提供本单位所需的网络设备间和电源保障，协助解决网络布线和设备安装所需空间，负责安防和消防安全管理。

**第十九条** 校园网主要服务于学校教学、科研及管理等，用户不得将校园网用于其他用途。用户未经许可不得直接或间接地向校外提供校园网的任何资源，严禁利用校园网开展各类未经许可的活动。

## **第四章 数据中心管理**

**第二十条** 数据中心主要包括支撑校园网、信息系统和互联网应用等运行的物理环境（包含机房）、软硬件设备设施、云计算平台等信息化基础设施和平台。

**第二十一条** 数据中心的建设单位负责数据中心物理环境、软硬件设备设施等的建设和安全管理；根据网络安全等级保护的不同，对数据中心进行分区、分域管理，采取必要的技术措施对不同等级分区进行防护、对不同安全域之间实施访问控制。

**第二十二条** 数据中心的使用单位应按需申请、规范使用数据中心资源，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安全和信息化工作的活动。

**第二十三条** 各单位原则上应依托学校数据中心开展信息系统建设。未经批准，不得部署在校外数据中心，严禁使用境外数据中心。

**第二十四条** 学校数据中心的使用实行准入管理，网络中心负责制定数据中心的技术规范和标准，符合规范标准并检测合格方可上线。

**第二十五条** 机房应设专人负责安全检查工作，定期进行机房基础设施设备安全检查。严禁无关人员进出机房，严禁与机房工作无关的人员直接或间接操作机房任何设备。

## **第五章 互联网应用管理**

**第二十六条** 学校对互联网应用实行接入审批、备案、年审登记制度，由有关部门制定相应管理规范(办法)。

**第二十七条** 互联网应用的内容安全由主办单位负责，信息发布应遵守《泉州师范学院校园网络信息发布管理办法（试行）》及相关规章制度。

**第二十八条** 互联网应用主办单位应建立值守制度，制订应急处置流程，组织专人监测，及时处置异常情况。

**第二十九条** 网络中心统一建设学校网站群平台并负责该平台网站的网络技术安全。未纳入学校网站群平台的网站，其网络安全由网站主办单位负责。

**第三十条** 各单位开办互联网网站应优先选择学校网站群平台。网站投入试运行后，须通过网络中心组织的安全测评方可正式上线。

**第三十一条** 各单位原则上不得提供留言板、电子公告服务。

**第三十二条** 网络中心为各单位和在籍在岗的师生员工提供电子邮箱，并负责学校电子邮件的安全管理。用户应遵守学校电子邮箱管理相关规章制度及用户使用协议。

**第三十三条** 网络中心应采取必要的技术和管理措施，加强电子邮件系统安全防护，减少垃圾邮件、病毒邮件侵袭。

**第三十四条** 用户须对使用其电子邮箱帐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的密码，确保密码具有一定强度。如发现他人未经许可使用其电子邮箱，应立即通知网络中心进行处理。

**第三十五条** 对于使用频度不大、阶段性使用的互联网应用，开办单位可采取非工作时间或寒暑假、节假日关闭的方式运行。对于无人管理、无力维护、长期不更新的互联网应用，开办单位应予以关闭。

## **第六章 信息系统管理**

**第三十六条** 网信办负责制定学校信息系统项目规划和顶层设计。各单位根据本单位业务需求，向网信办提出信息系统的建设申请。

**第三十七条** 为确保项目质量，信息系统建设单位在立项阶段应组织由网信办参与的需求、技术、预算等方面的专家论证。网信办组织专家对建设项目进行网络安全等级保护论证和定级；网络安全等级保护二级及以上的信息系统，由各建设单位配合，网信办统一组织办理系统定级备案。

**第三十八条** 信息系统在建设阶段应同步落实安全保护措施。信息系统投入试运行后，建设单位应委托有资质的测评单位进行第三方安全性测试，并出具风险评估报告，风险等级符合学校网络安全标准后方可进入验收环节。未经测评或测评不合格的信息系统不得上线。

**第三十九条** 信息系统开发环境、测试环境和运行环境应严格隔离，信息系统建设单位负责上述环境的建设、运行、维护和管理。

**第四十条** 信息系统项目验收时，建设单位应根据交付清单对所交接的硬件、软件和文档等进行清点，指定专人负责信息系统的运行维护，并加强技术人员的技能培训。

**第四十一条** 信息系统建设单位应定期对网络与信息系统运行的关键设备（服务器、安全设备、网络设备等）进行安全审计，通过记录、检查系统和用户活动信息等，及时发现系统漏洞，处置异常访问和操作。

**第四十二条** 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。

## **第七章 数据管理**

**第四十三条** 数据管理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。

**第四十四条** 数据收集应遵循“最少够用”原则，不得收集与业务系统无关的个人信息。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。

**第四十五条** 各单位所运营的信息系统资产要指定专人负责，并对责任人赋予相应的职责。责任人根据资产的不同作用进行分类，编制资产清单，妥善保管，确保资产随时可以核查；并在资产变更时及时更新，确保可以对资产进行有效的保护。

**第四十六条** 各单位须制订数据的备份与恢复计划并组织实施。根据业务实际需要对重要数据和信息系统进行备份，定期测试备份数据，保证信息系统出现故障时，能够满足数据恢复的要求。

**第四十七条** 各单位应对存储介质进行有效的管理，防止非授权的使用和破坏。

**第四十八条** 使用存储介质存储重要数据时要进行登记、追踪审计等，并对不再需要的存储介质进行安全处置，降低信息泄漏的风险。

**第四十九条** 存储介质在接入终端计算机和信息系统前，应当查杀病毒、木马等恶意代码等。

## **第八章 终端计算机管理**

**第五十条** 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。

**第五十一条** 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。

**第五十二条** 终端计算机使用人须做好数据日常管理和保护，定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

**第五十三条** 终端计算机须安装防木马、病毒软件并实时运行，及时更新特征库。严禁制造、引入或传播恶意软件（例如病毒、蠕虫、木马、邮件炸弹等）。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，应立即断网后进行处置，必要时报网信办及主管部门处置。

**第五十四条** 使用终端计算机查收邮件的附件或者网络通讯工具的附件，在打开之前须进行病毒检测，收到来历不明的邮件时不要打开附件，应确认文件安全或直接删除。

**第五十五条** 终端计算机使用人须定期检查各种补丁状况，当出现修复风险漏洞的补丁时，应在第一时间组织补丁的安装。在安装补丁前应对补丁的兼容性和安全性进行评估和检测，确保不影响正常运转。

## **第九章 网络安全应急管理**

**第五十六条** 网信办负责学校网络安全应急工作的统筹管理、制定网络安全事件应急预案，网络中心负责网络安全应急工作技术支撑和保障。

**第五十七条** 网信办定期组织网络安全应急演练，各单位应建立健全本单位安全事件应急处置机制，必要时制定本单位网络安全事件应急预案，定期组织应急演练。

**第五十八条** 网络中心负责组建学校网络安全应急技术支撑队伍，完善应急值守制度，提高网络安全事件的预防、预警和应付能力，预防和减轻网络安全事件造成的损失和危害。

**第五十九条** 各单位应按照学校网络安全事件报告与处置流程，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。做到网络安全事件早发现、早报告、早控制、早解决。

**第六十条** 各单位和用户均有义务及时向网络中心报告网络安全事件，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。

## **第十章 培训教育**

**第六十一条** 网信办负责组织学校网络安全和信息化教育和培训工作，建立健全相关制度。

**第六十二条** 各单位根据实际制定网络安全和信息化教育和培训计划，相关人员负责记录培训内容、培训结果以及参加培训人员，在培训结束后把相关记录材料整理归档。

**第六十三条** 各单位要采取有效措施，加强网络安全事件预防和处置的有关法律、法规和政策的学习宣传，开展网络安全基本知识和技能的宣讲活动。

**第六十四条** 各岗位人员要积极参与校内外网络安全和信息化交流和培训，定期对各岗位人员进行安全理论知识和安全技能水平的考核。

## **第十一章 检查监督**

**第六十五条** 全面实施网络安全等级保护制度，信息系统的建设单位是网络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，系统备案、等级测评并接受有关部门监督检查。

**第六十六条** 各单位建立日常检查机制，对终端计算机、服务器、应用软件、保护制度及措施落实情况等定期开展安全检查，查找安全漏洞和隐患（检查内容包含且不限于漏洞扫描、渗透测试、代码审计等）。

**第六十七条** 网信办定期组织开展全校网络安全等级保护测评。对各单位的信息系统进行安全检查，对发现的问题下达整改通知书，责成相关单位制订整改方案并落实到位。

**第六十八条** 各单位应及时对发现的问题进行整改并回复，对于暂时存在高风险隐患难以修复的或不回复不整改落实的，网信办将采取措施进行下线处置，直至修复完成。

## **第十二章 责任追究**

**第六十九条** 学校建立网络安全责任追究和倒查机制。

**第七十条** 各单位在收到网络安全整改通知书后，应立即组织技术力量进行整改；对于整改不力的，学校给予通报批评；对于玩忽职守、失职渎职造成严重后果的，依法依规追究相关人员的责任。

**第七十一条** 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措施，发现网络安全问题应及时进行处理，启动应急预案并及时向上级报告。对在处置工作中作出突出贡献的集体和个人，学校给予表彰和奖励；对于在处置工作中有其他失职、渎职行为的，根据其性质和造成后果的严重程度，依规给予党内、行政处分或处理；对于构成犯罪的，依法移送司法机关追究刑事责任。

**第七十二条** 用户违反规定使用校园网的，由网信办责令改正，并通报批评；拒不改正或者危害网络安全造成严重后果的，根据学校有关规定给予纪律处分，情节严重的，依法移交司法机关处理。

**第七十三条** 各单位建立完善的奖励机制，对网络安全工作表现突出的人员，给予适当激励。

## **第十三章 附则**

**第七十四条** 本办法下列用语的含义：

校园网，指校园范围内连接各种信息系统及终端计算机的计算机网络，包括校园有线网络、无线网络、业务专网和虚拟专网。

各单位，指学校各机关部（处、室）、二级学院、直属单位、附属单位、有关科研和以学校名义开展活动的机构以及在学校运营的电信运营商等。

用户，指学校网络与数据的使用者。

互联网应用，指互联网的网站、电子邮箱、留言板、电子公告服务、移动互联网应用程序（APP）等应用，以学校名义开设的微博、微信等及其附属应用程序等。

终端计算机，指接入校园网的各类计算机及附属设备，包括台式电脑、笔记本电脑及其他终端设备。

信息系统资产，指应用于信息系统的所有资产，包括硬件、软件、数据、服务文档、外设以及相应的配件、耗材、工具等。

存储介质，指是用于信息系统相关业务的电子信息输出、存放的物理介质、可移动和不可移动的磁盘、光盘、硬盘、磁盘阵列等。

**第七十五条** 本办法由网信办负责解释。

**第七十六条** 各单位可参照本办法制订本单位的实施细则。

**第七十七条** 本办法自发布之日起生效执行。学校原有相关规定与本办法不一致的，按本办法执行。