四川师范大学文件

川师信〔2019〕1号

关于印发《四川师范大学网络安全管理办法》的通　知

校内各单位:

为加强学校网络安全管理，提高学校网络安全防护能力和水平，保障学校信息化可持续发展，维护学校信息化相关各方的合法权益，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》《信息安全等级保护管理办法》和《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》（教技〔2014〕4号）的精神，结合学校实际，制定了《四川师范大学网络安全管理办法》，现印发给你们，请遵照执行。

特此通知。

附件：四川师范大学网络安全管理办法

四川师范大学

2019年8月27日

政务公开选项：主动公开

四川师范大学学校办公室　　2019年8月27日印发

附件

四川师范大学网络安全管理办法

为加强学校网络安全管理，提高学校网络安全防护能力和水平，保障学校信息化可持续发展，维护学校信息化相关各方的合法权益，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》《信息安全等级保护管理办法》和《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》（教技〔2014〕4号）的精神，制定本办法。

第一章　总　则

第一条　学校网络安全是指学校信息基础设施、各类信息系统及其承载的信息（含数据）内容受到保护，不因偶然的或者恶意的原因而受到泄露、更改、破坏、未经授权访问和使用，保证信息系统和信息内容的机密性、完整性、可用性、可控性和不可否认性。

第二条　网络安全管理的总体目标是建立健全学校网络安全保障体系，提高网络安全防护能力和水平，确保学校网络安全工作规范、有序开展，保障学校信息化可持续发展。

第三条　网络安全工作的总体方针是以网络安全等级保护制度为指导，预防为主、综合防范。

第四条　网络安全工作的总体原则

（一）主要领导负责原则。学校网络安全工作由学校主要领导总负责，从学校全局出发制定网络安全政策、调动并优化配置

必要的资源，协调网络安全管理工作与各部门工作的关系，确保学校网络安全管理制度得到有效落实。各学院、各单位主要领导对本学院、本单位网络安全工作负总责。

（二）保护重点与适度安全原则。根据信息系统所承载信息的重要性对信息系统进行分级，优化网络安全资源配置，做到重要系统重点保护和适度安全。

（三）管理与技术并重原则。根据相关网络安全制度和技术规范对信息系统进行自主保护，将科学有效管理与安全技术结合起来进行综合防范，同时接受上级安全部门的监管和指导，全面提高信息系统安全防护能力。

（四）分权和授权原则。根据特定职能或责任领域的管理工作需要对相关人员及实体（如用户、管理员、进程、应用或系统）进行授权，仅授予该人员及实体完成其任务所必须的权限，限制其享有任何多余权限，避免权限过分集中所带来的隐患。

第二章　网络安全管理组织体系

第五条　学校网络安全和信息化领导小组负责制定贯彻落实中央、教育部和四川省关于网络安全和信息化的工作部署，统筹协调全校网络安全和信息化重大问题，研究制定学校网络安全和信息化发展战略、总体规划和重要政策。

第六条　领导小组下设网络安全和信息化办公室，挂靠在网络与信息化管理处，具体承担日常工作。

第七条　网络安全和信息化办公室设主任 1 名、副主任 2 名和成员若干名。其中，网络安全和信息化办公室主任由分管信息化工作的校领导担任，副主任分别由网络与信息化管理处和党

委宣传部的主要负责人担任。成员包括学校办公室、党委组织部、纪委办公室•监察处、学生工作部、校团委、人事处、外事处、教务处、研究生院、科研处、计财处、实验室与设备管理处、保卫处、继续教育学院、教师培训学院、计算机科学学院、后勤集团的主要负责人。

第八条 网络安全和信息化办公室的职责是贯彻落实领导小组制定的发展战略、方针政策、总体规划，研究拟定相应实施方案；审定信息化建设项目年度计划；负责网络安全和信息化建设的监督、检查、协调和宣传工作；负责编制相关技术标准、规范和管理办法；在重要时间节点，根据上级要求和工作需要牵头组织成立网络安全保障工作组。

第三章 网络安全人员管理

第九条 网络安全人员包括网络安全责任人、网络安全员及各类信息系统关键岗位人员。各部门、各学院网络安全责任人由其主要负责人担任，各部门、各学院须指定一名专（兼）职网络安全员，信息系统关键岗位人员包括系统管理员、网络管理员、数据库管理员、系统应用开发人员、系统维护人员等岗位人员。

第十条 网络安全人员必须政治可靠、业务素质高、遵纪守法、恪尽职守、技术过硬。网络安全人员应严格遵守国家有关法律、法规和学校有关规章制度，严守单位秘密。违反国家法律、法规和行业规章以及受过处罚的人员，不得从事网络安全管理与相关技术工作。

第十一条 网络安全人员任职前应在学校网络安全和信息化办公室进行备案管理各类网络安全人员的任职、调动、离岗等

应履行相关手续，若调离应向网络安全和信息化办公室变更备案信息并承诺其调离后的保密义务。

第十二条 网络安全责任人全面负责本单位的网络安全管理工作，承担安全事故管理责任。

第十三条 网络安全员应履行以下职责：负责本单位网络安全管理的日常工作；规范本单位信息发布流程，确保单位网站或信息系统信息发布合规合法，防止有害信息传播和涉密信息泄露；配合学校网络安全和信息化办公室与公安机关开展网络安全检查工作，对重要信息系统安全管理进行指导和监督；负责维护和审查有关安全审计记录，及时发现存在问题，提出安全风险防范对策；定期对单位信息基础设施进行巡检；开展网络安全知识的培训和宣传工作；监控本单位网络安全总体状况，保管信息设备资产台账，制定网络安全工作方案和应急预案；及时向学校网络安全和信息化办公室报告网络安全事件，协助调查取证和落实整改措施。网络安全员在行使安全防控职责时，如确因工作需要，经批准，可了解涉及单位运作与管理有关的信息系统的重要信息。网络安全员发现本单位重大网络安全隐患，有责任向学校网络安全和信息化办公室报告；发现信息系统关键岗位人员使用不当，应及时建议单位进行调整。

第十四条 信息系统关键岗位人员须严格遵守保密法规和有关网络安全管理规定，按“分权和授权”原则，明确岗位权责，允许兼任，但避免权责过于集中。其中系统管理人员、网络管理人员、数据库管理员、系统开发人员、系统维护人员行使各自职权，相互监督，但不宜兼任系统业务操作员。

第十五条 对信息系统关键岗位人员应实行人员备份管理，保证至少有两个合适的人员可处理系统问题。关键岗位人员应定期接受安全相关业务培训与学习，加强自身安全意识和风险防范意识。关键岗位人员离岗后，必须即刻更换其操作密码或注销用户。

第十六条 系统管理员负责系统的运行管理，实施系统安全运行细则；严格用户权限管理，维护系统安全正常运行；认真记录系统安全事件，及时向网络安全员报告安全事件；对系统操作的其他人员予以安全监督。

第十七条 网络管理员负责网络的运行管理，实施网络安全策略和安全运行细则；安全配置网络参数，严格控制网络用户访问权限，维护网络安全正常运行；监控网络关键设备、网络端口、网络物理线路，防范网络入侵与破坏，及时向网络安全员报告安全事件；对操作网络管理功能的其他人员进行安全监督。

第十八条 数据库管理员负责系统数据库的运行维护，确保安全运行，数据有备份、可恢复。严格控制数据库用户访问权限。

第十九条 系统开发人员在系统开发建设中，应严格执行系统安全策略，保证系统功能的安全准确实现。

第二十条 系统维护人员负责系统维护，及时排除系统故障，做好维护记录，确保系统正常运行；不得擅自改变系统功能；不得安装与系统无关的其他计算机程序；维护过程中，发现安全漏洞应及时报告网络安全员。

第二十一条 系统业务操作员应严格执行系统操作规程和运行安全管理制度；不得向他人提供自己的操作密码；及时向系

统管理员报告系统各种异常事件。

第四章　校园网安全

第二十二条　校园网既是用户使用互联网的基础条件，又是依托网络运行的信息系统的基础条件。校园网安全管理，是指由校园网络运维管理和网络资源与服务管理所构成的安全管理。

第二十三条　网络与信息化管理处负责校园网络规划建设和安全管理工作，保障校园网核心网络系统和信息系统等的安全。

第二十四条　校园网络出口由网络与信息化管理处统一建设和进行安全管理，任何单位或个人不得私自另建互联网出口。

第二十五条　校园网核心网由网络与信息化管理处统一管理及维护，对校园网用户进行安全审查和监督。接入校园网的各部门、各学院，以及教室、实验室、机房、宿舍和个人使用者必须严格使用由网络与信息化管理处分配的 IP 地址。任何人不得随意变更 IP 地址及网络设置，不得盗用 IP 地址及相关用户帐号。

第二十六条　设备安全管理。接入校园网的计算机、服务器、交换机等网络设备应当符合国家有关技术标准和使用规定。各种网络接入设备要切实做好防病毒技术措施，主机操作系统及时更新系统补丁。禁止私拉乱接网络布线及私自安装、更换和拆除网络设备。如有特殊需要，须经过网络与信息化管理处审批后方可实施。所有服务器、主干交换机及其他系统主要设备配置更新变化时及时进行备份。网络设备、安全设备、应用系统、操作系统、数据库均应设置登录密码安全管理，密码应符合规定的长度及复杂度，并定期进行更新。设备安全运行日志至少保存 180 天。

第二十七条 校园网帐号安全管理。在校园网开设的用户账户和口令，网络与信息化管理处将严格信息管理，不向任何单位和个人提供相关信息，记录帐号使用情况、帐号对应 IP 地址情况。

第二十八条 用户安全管理。所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度和实名上网制度，并对所提供的信息负责。还应及时更改个人初始密码，并妥善保存，不向任何人泄露或转借账号等信息。任何单位和个人不得利用联网计算机从事危害校园网服务器、工作站、终端设备甚至校外服务设施的活动。

第二十九条 域名安全管理。四川师范大学注册域名为：sicnu.edu.cn 和 sicnu.cn，网络与信息化管理处负责管理，校内用户可按相关规定申请使用二级以下各级域名，暂不提供其他域名解析服务。各部门、各学院域名须有专人管理，定期进行安全和使用情况检查，防止出现违法或无效链接。

第三十条 电子邮件安全管理。校园网电子邮件系统为校园用户提供电子邮件收发服务，严禁利用电子邮件散发垃圾邮件、传播计算机病毒等。任何用户不得利用校园网制作、复制、查阅和传播违反法律法规、破坏学校和社会和谐稳定的信息。

第三十一条 电子信息系统机房安全管理。电子信息系统机房由相关主管部门安排专人负责日常安全管理，按照机房管理制度定期对机房进行日常检查，详细记录机房 UPS 供配电、制冷通风、防雷接地、消防设施、防盗或视频监控、防水防潮、设备线缆标识标记等物理设施情况，对不满足机房设计标准的及时进行

整改，做好相关设备的专业维保工作。机房负责人还应加强机房出入控制，建立机房进出审批制度和流程，详细记录机房进出人员及操作事项。对于机房火灾、盗窃及破坏相关情况应及时上报学校及上级主管部门。

第三十二条 校园内的弱电管网、交接箱及光缆由后勤集团通讯中心统一进行日常维护和安全管理。单独使用校内管道及光缆或光纤资源的需进行申请，未经批准擅自使用的一经发现，将采用物理阻断和强行整改措施，由违规方支付相关费用；经批准的需由建设方自行维护该光缆或光纤链路，并负责其安全管理。

第三十三条 无线网络安全。校园无线网络为学校资源，四川师范大学校园内的无线网络覆盖工作由学校统一规划部署、科学利用。未经网络与信息化管理处审核许可，任何单位和个人不得擅自进行校内（含楼宇内）无线网络（单个房间覆盖的除外）的建设和服务，也不得擅自同意校外无线网络服务提供商在校园内（包含对外经营场所）从事无线网络安装、经营业务。校内单位及个人架设的自用小型无线网络，不得干扰校园网络的正常运行，一旦发现与学校无线网络发生冲突或干扰，网络与信息化管理处有权采取断网整改措施。按照“谁安装谁负责”的原则，架设无线路由设备的单位及个人，需要加强对所设无线网络的接入安全管理，落实安全管理责任人。

第五章 信息系统运行安全

第三十四条 信息系统是由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。信息系统

运行安全依照“谁主管，谁负责；谁主办，谁负责”的原则，各级系统管理员是相关系统安全运行管理的直接责任人。

第三十五条 各类信息系统运行期间须依据学校安排做好信息系统安全等级保护工作，包括安全等级变更备案与安全测评，不符合要求的须在指定期间内完成整改建设工作，使之持续具备与其安全等级相适应的网络安全防范能力。

第三十六条 信息系统日常运行维护须从网络安全、主机安全、应用安全、数据安全与备份恢复及安全管理措施等方面加强安全管理。

第三十七条 网络安全应保障系统运行的网络结构安全合理。保证关键网络设备的业务处理能力满足系统运行需要，保证接入网络和核心网络的带宽满足系统运行需要。确保系统具有合理的访问控制措施。在网络边界部署访问控制设备，启用访问控制功能。通过访问控制列表对系统资源实现允许或拒绝用户访问。保证系统所用网络设备得到有效防护。对登录网络设备的用户进行身份鉴别，登录密码符合安全要求的长度和复杂程度。当需要对网络设备进行远程管理时，应采取必要措施防止信息在网络传输过程中被截取。

第三十八条 主机安全应对登录主机操作系统和数据库系统的用户进行身份标识和鉴别。主机访问控制。应启用访问控制功能，依据安全策略控制用户对资源的访问。应限制默认帐户的访问权限，重命名系统默认帐户，修改默认口令。应及时删除多余的、过期的帐户，避免共享帐户的存在。入侵和计算机病毒防范。操作系统应遵循最小安装的原则，按需安装组件和应用程序，

并保持系统补丁及时得到更新。主机应安装防计算机病毒软件，并及时更新软件版本和病毒特征库。根据安全要求设置登录终端的操作超时锁定策略，限制单个用户对系统资源的最大或最小使用限度。

第三十九条 应用安全应则提供系统身份鉴别机制。信息系统应提供专用的登录控制模块对登录用户进行身份标识和鉴别；提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；启用身份鉴别和登录失败处理功能，并根据安全策略配置相关参数。访问控制机制。信息系统应提供访问控制功能，控制用户组、用户对系统功能和用户数据的访问；应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。软件容错机制。信息系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式符合系统设定要求。在系统发生故障时，应确保部份基本功能可用。

第四十条 数据安全与备份恢复应采用加密技术确保信息系统重要数据在传输过程中的完整性、在系统中的可用性以及符合特定要求的保密性。应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据传输方法。信息系统应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。应根据信息系统的备份技术要求，制定相应的应急预案与灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效

性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新。

第四十一条 安全管理措施应包括信息系统运行期间应根据本办法第三章内容配备信息系统安全运维所需的管理人员并加强人员管理。信息系统投入运行、网络系统接入和重要资源的访问等关键活动应进行审批、记录。应对网络设备、主机系统和信息系统进行定期安全漏洞检测评估，及时修补漏洞，整改加固安全防护措施。应定期对信息系统运行日志和审计数据进行分析，以便及时发现异常情况，采取措施调整纠正。信息系统应使用符合国家密码管理规定的密码技术和产品。信息系统重大变更，应制定相应的变更方案，报主管部门审批后方可实施变更，并在实施后向相关业务人员通告。信息系统运行期间如发生网络安全事件，应按照《四川师范大学网络安全事件应急处置预案》规定进行报告处置。

第六章 网络安全事件管理

第四十二条 网络安全事件是指由于自然或人为的原因对校园网、各类信息系统或信息内容造成危害，对学校或社会造成负面影响的事件。

第四十三条 学校网络安全和信息化办公室负责制定学校网络安全事件应急预案并组织演练。

第四十四条 校园网络安全事件的报告和处置由《四川师范大学网络安全事件应急处置预案》另行规定。

第七章 考核与奖惩

第四十五条 学校网络安全和信息化领导小组根据学校网

络安全情况并结合上级部门安排不定期开展学校网络安全检查工作，并对网络安全工作成绩突出的单位和个人给予表彰奖励。

第四十六条 网络安全工作是学校及各单位的重要工作之一，网络安全工作情况作为学校对各单位年度工作考核、先进集体评选的一项重要依据，出现重大安全事件的单位不得评为先进集体。

第四十七条 对于玩忽职守或故意危害学校网络安全而造成网络安全事件的，学校将根据损失情况和不良影响的程度给予当事者以通报批评直至处分，构成犯罪的移交司法部门处理。

第八章 附 则

第四十八条 未尽事宜依照上级机关有关政策法规之规定办理。

第四十九条 本办法由学校网络安全与信息化领导小组授权网络安全和信息化办公室负责解释。

第五十条 本办法自印发之日起执行。