武夷学院文件

武院综〔2020〕59号

关于印发《武夷学院网络安全管理办法》的通知

各部门、各二级学院:

为加强对学校网络安全工作的统筹领导，保证信息化建设的健康有序发展，规范校内网络安全管理，根据法律法规以及学校相关规定，对《武夷学院校园网管理办法》，《武夷学院网络信息服务管理规范》等管理文件进行修订，合编为《武夷学院网络安全管理办法》，现将《武夷学院网络安全管理办法》印发给你们，请按照责任分工认真贯彻落实。

武夷学院

2020年11月6日

武夷学院网络安全管理办法

为加强对学校网络安全工作的统筹领导，保证信息化建设的健康有序发展，规范校内网络安全管理，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》（中华人民共和国国务院令第 147 号发布）、《互联网信息服务管理办法》（中华人民共和国国务院令第 292 号公布）、《教育部关于加强教育行业网络与网络安全工作的指导意见》（教 技〔2014〕4 号）、《教育部关于进一步加强直属高校直属单位网络安全工作的通知》（教技〔2015〕1 号）、《教育部公安部关于全面推进教育行业网络安全等级保护工作的通知》（教技〔2015〕2 号）、《2019 年教育信息化和网络安全工作要点》、《教育移动互联网应用程序备案管理办法》（教技〔2019〕3 号）、《高等院校管理服务类教育移动互联网应用专项治理行动方案》（教技〔2019〕265 号）和其他法律法规以及学校相关规定，对“武夷学院校园网管理办法”“武夷学院网络信息服务管理规范”等管理文件进行修订，合编为“武夷学院网络安全管理办法”，具体内容如下。

第一章 总 则

第一条 本办法所称网络安全管理工作是指为学校的信

息化建设的基础设施、数据和信息系统等保障其完整性、可用性及保密性的相关管理和技术工作，以及相关技术标准规范、管理制度的制定工作等。本办法所指学校各单位包括各机关部、处、室，学院，直属单位以及有关科研机构。

第二条 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落实网络安全管理的义务和责任。

第三条 涉及国家秘密的有关信息内容管理工作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 组织机构与职责

第四条 网络安全与信息化工作领导小组（以下简称领导小组）为学校网络安全的领导机构，负责学校网络安全建设的战略规划、实施监督及重大网络安全事件处理的决策指导，并组织协调各成员，督促学校各单位落实网络安全的管理规定，不断提高学校网络安全发展水平。

第五条 网络安全与信息化工作领导小组组成如下：

（一）组长： 武夷学院党委书记

武夷学院党委副书记、校长

常务副组长： 武夷学院网络信息安全主管副校长

副组长：　　武夷学院党委副书记、副校长

（四）成员：宣传部、办公室、学工部、团委、教务处、人事处、科研处、财务处、保卫处、发展规划处、信息技术与实验室管理中心主要负责人及各二级党委主要负责人。

领导小组下设办公室，挂靠信息技术与实验室管理中心，负责日常网络安全和信息化工作，主任由信息技术与实验室管理中心负责人兼任。

第六条 网络安全和信息化工作领导小组办公室（以下简称领导小组办公室）具体负责网络安全及信息化建设、规划、开发及校园网运行和维护工作。其主要职责是：

（一）拟定网络安全及信息化建设规划，并组织实施；

（二）拟定网络安全及信息化管理规章制度；

（三）组织开展网络安全等级保护工作；

（四）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；

（五）学校网络安全的其他工作；

（六）负责校园骨干网的日常运行和维护；对校园网的用户进行管理，提供技术咨询、指导及支持；配合宣传部和保卫处对有害信息监控、封堵、取证等工作；

（七）负责 IP 地址、域名管理、电子邮件、教育移动

互联网应用程序的管理等工作;

（八）对校内各单位网络安全及信息化管理员开展培训，提供技术咨询、指导；。

（九）完成领导小组交办的其他工作。

第七条 宣传部主要负责学校新闻和专题教育网站建设、网络舆情收集等，并建立相应的网络舆情分析和引导机制。发现有违法违规行为的，应当保留有关原始记录，及时对相关信息进行处理。具体职责包括:

（一）组织网络安全宣传和教育培训工作;

（二）开展网络思想政治工作和网络精神文件建设;

（三）学校网站、微博和微信内容审核;

（四）网站设立管理，微博、微信和 APP 的设立审批;

（五）完成领导小组交办的其他工作。

第八条 保卫处（武装部）主要配合校园网的安全监督、检查，以及对散布有害信息事件进行调查，并向领导小组提出处理意见。

第九条 后勤处（基建办）负责信息化所需的地下管网规划、建设和运行维护工作。负责将校园网线路建设纳入学校所有基建、修缮工程设计、实施和竣工验收范畴。

第十条 学校各处（部、室）、各学院、各单位、各上网

服务场所，作为校园网络使用部门，均属于校园网二级管理部门，须切实增强政治意识，按照“谁主管，谁负责；谁主办，谁负责” 的要求，负责建设和管理好所属二级网站，各单位须确定一位分管网络安全与信息相关工作的领导及一名网络安全及信息化管理员，切实履行守土之责，主动协助有关部门管理好校园网络。网络安全及信息化管理员职责是:

（一）负责对本单位网络设备、入网计算机与线路等设施的管理;

（二）负责本单位入网计算机的信息登记工作;

（三）制作及维护本单位网页，负责本单位信息资源的管理，及时更新本单位主页，并对本单位发布的信息内容负责;

（四）负责本单位计算机系统安装、使用与维护工作，帮助本单位用户解决使用网络的疑难问题;

（五）负责本单位因教学科研需要的云计算资源的申请、分配、使用与系统维护;

（六）管理员应主动到现场配合技术人员处理相关技术故障;

（七）完成领导小组交办的其他工作。

第十一条 关键岗位的管理人员和技术人员应按学校规定与领导小组办公室签订网络安全保密协议，明确相关要求

和责任。

第三章　校园网管理

第十二条 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、无线网络和各种虚拟专网。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、网络接入与运维等内容。

第十三条 校园网与互联网及其他公共信息网络实行隔离，学校统一出口、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。

第十四条 校园网和信息系统接入互联网必须按照相关法定规范采取访问控制、安全审计、访问日志记录、完整性检查、入侵防范、恶意代码防范等措施加强技术防护。

第十五条 校园网入网实行“实名注册、认证上网、一人一号”制度。用户必须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，严禁盗用其他用户上网信息使用校园网。

第十六条 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。

第十七条 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、解决网络布线和设备安装所需空间、安

防和消防安全管理。

第十八条 校园网主要服务于学校教学、科研及管理等，各单位不得将校园网资源挪作他用或擅自向校外提供校园网的任何资源。

第四章 数据中心管理

第十九条 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。

第二十条 数据中心的使用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安全的活动。

第二十一条 根据信息系统安全等级的不同，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 学校统一中心数据库、数据共享交换平台的建设和安全管理。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，并对本单位业务数据库及所申请的共享数据的安全负责。

第二十三条 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、审计及标准接口。学校各单位建设面向师生服务的应用系统时，应使用统一身份认证平台进行身份认证。

第二十四条 学校各单位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，须报领导小组办公室审批。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，原则上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。

第二十五条 学校对数据中心的使用实施统一准入管理，符合技术规范标准并检测通过的系统方可上线运行。

第二十六条 机房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纵机房任何设备。

第二十七条 严格遵守安全用电相关规范，严禁在数据中心机房中私拉电线，滥用电器，严禁超负荷用电；严禁私自拆卸机器设备，不得擅自将任何设备携带进出；机房内严禁存放易燃、易爆、易腐蚀物品及堆放杂物；严禁饮食、吸烟、聊天。

第二十八条 机房管理员应熟练掌握使用方法，在危险性高的位置应张贴相应的安全操作方法、警示以及指引。

第五章　信息系统建设、运行和维护管理

第二十九条 信息系统是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统。这里信息系统包含教育移动互联网应用程序。

第三十条 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、管理网络安全设施，建立健全网络安全防护体系，全面实施信息系统安全等级保护制度。

第三十一条 领导小组办公室负责统筹学校信息系统安全等级保护工作，组织学校各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。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。

第三十二条　为确保项目质量，信息系统建设单位在立项阶段应确定安全保护等级，由领导小组办公室对建设方案进行单独的安全论证和等级评审。对于安全等级第二级以上（含第二级）的信息系统，由领导小组办公室统一办理系统备案。

第三十三条 学校鼓励建设单位优先采购安全可靠、技术

成熟和服务优质的成品软件用于信息系统建设。对于教育移动应用程序应优先采用在公共服务体系中已完成提供者备案的应用。对教育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，所有教育移动应用程序须按要求完成备案。

第三十四条 信息系统开发环境、测试环境和运行环境应严格隔离。

第三十五条 信息系统在建设阶段应按已确定安全保护等级，同步落实安全保护措施。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，并向领导小组办公室提供备份制度、软硬件及账号信息。对于安全等级第二级以上（含第二级）的信息系统，由领导小组办公室会同使用部门组织等级测评。信息系统通过初步验收和网络安全保护等级测评后，由领导小组办公室组织竣工验收。

第三十六条 信息系统建设单位可自行或委托校内其他部门维护信息系统。亦可根据实际需要，委托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，应由使用部门制定维护制度，并报领导小组办公室审批。

第三十七条 学校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）进行安全审计，通过记录、检查系统和用户活动信息，检测系统漏洞，处置异常访问和操作。

第三十八条 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，规范信系统使用者和维护者的操作行为。

第三十九条 对于安全等级二级以上（含二级）的信息系统，学校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，原则上第三级系统每年进行一次测评，第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

第四十条 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、设备配置、网络课程、图书资源、日志记录等。

第四十一条 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。

第四十二条 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服务无关的个人信息。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。

第四十三条 学校统一核心信息系统的备份与恢复管理，制订备份与恢复计划，定期测试备份与恢复计划，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

第四十四条 学校各单位开办互联网网站，应上报宣传部审批，使用学校互联网域名和互联网 IP 地址，并遵守相关规章制度。

第四十五条 学校统一建设学校网站集群平台并负责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。

第四十六条 学校各单位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管理。网站投入试运行后，通过安全检查方可正式上线。

第四十七条 互联网网站运行维护单位应建立网站值守制度，制订应急处置流程，组织专人对网站进行监测，发现网站运行异常及时处置。

第四十八条 互联网网站的内容安全由网站开办单位负责。互联网网站开办单位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、审核、发布的人员，明确审核与发布程序，保存相关操作记录。

第四十九条 学校各单位不得提供电子公告服务。确有需要，经批准备案后方能提供电子公告服务。提供电子公告服务的互联网网站开办单位承担电子公告服务内容管理的主体责任，并按国家有关规定落实专项安全管理和技术措施。

第五十条 对于使用频度不大、阶段性使用的网站，互联网网站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、长期不更新的网站，互联网网站开办单位应关闭网站以降低安全风险。

第八章 电子邮件安全管理

第五十一条 学校统一为各单位和师生员工提供电子邮件服务及安全管理。各单位和师生员工使用学校电子邮箱应遵守学校电子邮箱管理等相关规章制度。

第五十二条 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，应立即上报处理。

第九章　终端计算机安全管理

第五十三条 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。

第五十四条 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。

第五十五条 终端计算机设备上安装、运行的软件须为正版软件。在终端计算机上使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第五十六条 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。

第五十七条 终端计算机使用人应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。

第五十八条 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，应立即断网后进行处置。

第五十九条 终端计算机使用人应对终端计算机妥善保管。若发生损坏丢失，按学校仪器设备相关管理规定处理。

第十章　存储介质安全管理

第六十条 存储介质是指存储数据的载体，主要包括硬盘、存储阵列等不可移动存储介质，以及移动硬盘、U盘等可移动存储介质。

第六十一条 存储阵列等大容量介质应托管在学校数据中心统一运行、维护和管理。采取必要技术措施防范数据泄漏风险，确保存储数据安全。

第六十二条 学校各单位应建立移动介质管理制度，记录介质领用、交回、维修、报废、损毁等情况。介质使用人按照“谁使用，谁负责”的原则，对其移动介质负有保管和安全使用的责任。

第六十三条 非涉密移动存储介质不得用于存储涉密信息，不得在涉密计算机上使用。

第六十四条 移动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。

第六十五条 介质使用人应注意移动存储介质的内容管理，对送出维修或销毁的介质应事先清除敏感信息。

第六十六条 办公室保密科应配备必要的电子信息消除和销毁设备。存储介质履行必要的审批程序后，可由保密科集中销毁。

第十一章　人员安全管理

第六十七条 学校各单位应建立健全本单位的岗位网络安全责任制度，明确岗位及人员的网络安全责任。关键岗位的计算机使用和管理人员应签订网络安全与保密协议，明确网络安全与保密要求和责任。

第六十八条 学校各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、以及学校提供的软硬件设备，并签署安全保密承诺书。

第六十九条 学校各单位应定期对网络安全岗位的人员进行安全知识和技能的考核，并对考核结果进行记录和保存。

第七十条 学校各单位应建立外部人员访问机房等重要区域的审批制度，外部人员须经审批后方可进入，并安排工作人员现场陪同，对访问活动进行记录和保存。

第十二章 外包服务管理

第七十一条 信息技术外包服务是指信息系统的开发和运维的外包。

第七十二条 外包服务需求单位应与信息技术外包服务提供商签订服务合同和网络安全与保密协议，明确网络安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程

中产生的任何信息资产，不得以服务为由强制要求委托方购买、使用指定产品。信息技术外包服务合同和网络安全与保密协议应按学校合同管理办法的有关要求，报领导小组办公室审核。

第七十三条 信息技术现场服务过程中，外包服务需求单位应安排专人陪同，并详细记录服务过程。

第七十四条 外包开发的系统、软件上线应用前，外包服务需求单位应组织安全检查，要求开发方及时提供系统、软件的升级、漏洞等信息和相应服务。

第七十五条 远程在线运维管理设备由学校统一购置、运维和管理。信息系统运维如需采用远程方式进行，必须通过远程在线运维管理设备统一进行管理。

第十三章　网络安全应急管理

第七十六条 学校对网络安全应急工作统筹管理，领导小组办公室负责网络安全应急工作的技术支撑和保障。

第七十七条 学校制定网络安全应急预案、处置流程、事件报告；若学校网络安全应急预案不能满足需求，相关单位可制订本单位网络安全应急预案，并报领导小组办公室备案。

第七十八条 领导小组办公室定期组织网络安全应急演练，评估并适时组织网络安全应急预案修订。学校各单位应

组织开展网络安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第七十九条 领导小组办公室负责组建学校网络安全应急技术支援队伍，完善24小时应急值守制度，提高网络安全事件的预防、预警和应对能力，预防和减轻网络安全事件造成的损失和危害。

第八十条 学校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。做到安全事件早发现、早报告、早控制、早解决。

第八十一条 学校各单位或师生员工均有义务及时向领导小组办公室报告网络安全事件，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。

第十四章 网络安全教育培训

第八十二条 学校组织网络安全宣传和教育培训工作，建立健全相关制度。

第八十三条 宣传部牵头各单位定期组织开展针对师生员工的网络安全教育，提高师生员工的安全和防范意识。

第八十四条 领导小组办公室定期开展针对网络安全管理人员和技术人员的专业技能培训，提高网络安全工作能力

和水平。

第八十五条 教师发展中心牵头各单位定期组织开展针对教师信息化技能培训，提高教师信息素养。

第十五章　网络安全检查监督

第八十六条 学校各单位定期对本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，并配合有关部门的网络安全检查、信息内容检查、保密检查与审批等工作。

第八十七条 学校对各单位的网络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。

第八十八条 领导小组办公室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安全主管部门。

第十六章　网络安全责任追究

第八十九条 学校建立网络安全责任追究和倒查机制。

第九十条 有关单位在收到网络与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。

第九十一条 学校各单位应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，学校将对相关单位责任人进行约谈或通报。

第九十二条 教师员工违反本办法规定的，由领导小组办公室责令改正，并通报批评；拒不改正或者导致危害网络安全等严重后果的，根据学校有关规定给予处分。学生构成违反本办法规定的，构成违纪违规的，根据《武夷学院学生违纪处分管理办法》处理。触犯刑律的，移交司法机关处理。

第十七章 附 则

第九十三条 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，由学校办公室保密科监督指导。

第九十四条 本办法自发布之日起实施，由领导小组办公室负责解释。学校原有相关规定与本办法不一致的，按本办法执行。

武夷学院办公室　　2020年11月6日印发