集美大学文件

集大综〔2023〕18号

关于印发《集美大学网络安全管理办法（试行）》的通知

校内各单位：

《集美大学网络安全管理办法（试行）》已经2023年第12次党委常委会审议通过，现印发给你们，请结合实际，认真贯彻执行。

集美大学

2023年9月30日

集美大学网络安全管理办法（试行）

第一章　总则

第一条 为保证学校网络安全与信息化建设工作的健康有序发展，规范网络安全建设管理工作，确保网络安全，根据《中华人民共和国网络安全法》等相关法律法规要求以及《集美大学章程》，结合学校实际情况，制定本办法。

第二条 本办法所称网络安全工作是指为保障学校网络安全和信息化建设相关基础设施、信息系统及数据的完整性、可用性及保密性，而采取的网络安全检测、防护、处置等技术措施，以及相关标准规范、管理制度的制定、执行等。

涉密信息安全管理等不在本办法范畴内，由学校相关单位根据相关规定进行管理。

第三条 学校按照国家有关网络安全和信息化政策法规，建立健全网络安全管理体系、防护体系和保障体系，全面实行网络安全等级保护制度。

第四条 网络安全工作是学校信息化建设的关键工作，信息化项目年度预算中须包含网络安全专项费用，切实保障网络安全建设和常规工作顺利开展。

第二章　组织机构与职责

第五条 党委宣传部负责指导、督查二级党委落实网络意识

形态责任制工作，统筹学校网上舆论引导、网络信息监测、网络文化建设等工作。

第六条 网络安全与信息化办公室（以下简称“网信办”）是学校网络安全工作的归口管理机构，负责组织协调全校网络安全保障体系建设和日常网络安全管理、保障。

第七条 党委保卫部（保卫处）作为与公安机关的对口部门，负责协助公安机关开展网络安全案件的处理。

第八条 校内各单位按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，分别负责本单位主管、运维、使用的各信息系统及内部网络的安全工作，同时负责本单位人员网络安全教育工作。

第九条 校内广大师生作为校园网和信息化系统的使用者，同样也是网络安全工作的参与者，有责任和义务遵守学校网络安全的相关规定，积极参与网络安全的建设和管理。

第三章　基础设施安全管理

第十条 校园网及相关基础设施由网信办统一规划、建设、管理，并提供统一网络出口和统一安全防护，校内各单位及个人不得擅自建设、更改、损毁、挪用校园网及相关基础设施，不得私接外网出口。

第十一条 校园网主要服务于学校教学、科研及校务管理等，用户不得将校园网用于其他用途，严禁利用校园网开展各类未经许可的活动。

第十二条 校园网实行实名认证制度。网信办根据要求配合公安等有关部门对违法违规行为进行查处，用户必须接受并配合相关监督检查。

第十三条 联网实验室在提供上网服务时实行实名认证。因故无法实行上网实名认证的实验室，可以申请免认证。免认证的实验室必须按要求做好上网实名登记。

第十四条 用户要妥善保管自己的上网账号和密码，并对自己的账号在网上的行为负责，不得将账号借给他人使用，不得盗用他人账号，不得使用路由器共享上网。

第十五条 校园网用户应文明上网，规范网络行为，上网行为不得危害到学校网络安全和正常秩序，严禁利用校园网从事任何无授权的探测、破坏、信息窃取等互联网攻击活动。

第十六条 接入校园网的主机未经许可不得对校园网以外提供互联网服务，如在教学、科研上确有特殊需求，需要直接对外开放服务（限于非WEB 信息发布类服务），经网信办审批并安全检测通过后可开放，由申请人员和所在单位承担相关全部网络安全责任。

第四章　信息系统安全管理

第十七条 学校信息系统建设和服务实行网络安全审核制。不符合网络安全要求的信息系统必须进行整改，整改完成后方可继续建设或提供服务。

第十八条 学校信息系统建设应遵循校内网络安全相关制

度、技术规范、标准流程。信息系统上线前以及系统代码变更必须通过必要的网络安全检测，未通过检测擅自上线或变更代码的，一切网络安全责任由相关责任人和项目主管单位承担。

第十九条 学校各单位的信息系统原则上应依托于学校服务器平台建设，并进行登记备案。涉及学校核心数据、师生员工个人信息等敏感信息的信息系统，不得部署在校外。

第二十条 对于没有校内替代方案，确实必须部署在校外的信息系统，经网信办审批同意后，可以部署到符合安全要求的校外公共云计算平台，由系统承建方负责网络安全和等级保护备案，由申请人员和校内项目主管单位承担网络安全相关责任。

未按上述要求建设的信息化系统，不属于学校官方行为，不得使用学校资金建设，不得使用校名、校徽、域名等学校标识，一切网络安全责任由相关单位（包括建设使用单位、资金提供单位、宣传推广单位等）及参与人员承担。

第二十一条 为保证学校信息化建设项目的建设质量，确保网络安全建设工作及安全运维工作正常开展，应采用安全规范、质量和售后服务优良的软、硬件产品或服务厂商，不得由自然人或没有相应资质的企业承担信息化项目建设任务。

第二十二条 为确保信息系统的安全性，面向师生或跨部门使用的系统，必须接入学校统一建设的信息化基础平台，实现统一身份认证、统一应用入口、统一消息推送和数据共享交换，不得单独建立用户认证系统、消息推送系统和数据交换系统，不得

单独建立移动APP、各类小程序、公众号等聚合应用入口。

第二十三条 校内各信息系统应按照学校信息化数据相关管理规定，采取必要的安全措施，确保数据安全。

第二十四条 信息化建设中所涉及到的个人信息，必须按照国家相关法律法规及学校个人信息保护相关规定进行严格保护，任何单位及个人不得违法违规采集、存储、使用和处理校内各类个人信息。

第五章　内容安全管理

第二十五条 任何单位和个人必须遵守国家有关法律法规和学校的有关管理规定，严格执行信息安全保密制度，并对所提供和发布的信息负责。

第二十六条 禁止使用互联网（包括但不限于邮箱、即时通信工具、社交网络工具等）处理、传递、转发涉密、工作敏感信息及涉及个人隐私信息。

第二十七条 学校各单位通过网络信息系统向网络发布信息时，应确保信息的真实有效，并采取身份鉴别、访问控制等防护技术措施，加强信息安全监控，防止出现内容篡改等安全事件。

第二十八条 学校各单位的网络信息发布工作需严格遵循国家有关规定，建立内容审核机制，规范信息发布审批流程，应由该单位主管领导分管，专人负责执行，并做到先审查后发布。

第二十九条 全校师生员工应当遵守各种相关法律法规，不得制作、复制、发布和传播违反相关法律法规的内容。

第三十条 网上公开发布信息必须符合国家法律法规。党委宣传部负责对学校网站等内容进行监管及合规处置，各单位负责本单位所开办的信息系统内容安全，网信办提供技术支持。相关单位须相互配合，及时处理有害信息。

第六章　终端安全管理

第三十一条 终端设备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、移动设备及其他物联网接入终端。

第三十二条 终端设备使用人按照“谁使用，谁负责”的原则，对其终端设备负有保管和安全使用的责任。网信办对终端设备的安全管理提供技术支持和指导。

第三十三条 学校提供常用正版软件下载，终端设备上安装、运行的软件须为正版软件。在终端设备上使用盗版软件带来的安全和法律责任由终端设备使用人承担。

第三十四条 终端设备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。

第三十五条 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。

第三十六条 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，应立即断网后进行处置。

第三十七条 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。

第三十八条 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。

第七章　人员安全管理

第三十九条 学校各单位应建立健全本单位的网络安全岗位责任制度，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信息安全与保密协议，明确网络安全与保密要求和责任。

第四十条 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，收回各类身份证件、钥匙以及学校提供的软硬件设备，重要、敏感岗位人员应签署离岗或离职安全保密承诺书。

第四十一条 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。

第四十二条 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。

第八章　服务外包安全管理

第四十三条 学校网络信息技术外包服务包括：咨询服务、运行维护服务、驻场服务以及技术培训，外包服务过程中，服务提供商应遵循国家和学校的相关安全规定，确保学校信息系统运行环境的稳定。

第四十四条 各单位应与外包服务方签订安全保密协议或合同，明确外包服务方其服务所对应的设施设备、软件系统、信息数据相关安全责任要求，并对服务人员进行安全保密教育。

第四十五条 各单位网络信息员负责对服务方提供的服务进行安全性监督与评估，采取安全措施对访问实施控制，出现问题应遵照合同规定及时处理和报告，确保其提供的服务符合单位的内部控制要求。

第四十六条 对外包服务的信息系统的安全状况应定期评估，当出现重大安全问题或隐患时应进行重新评估，提出改进意见，直至停止外包服务。

第四十七条 在重要安全区域，对外部服务方的每次访问进行风险控制，必要时应对外部服务方的访问进行限制、审计及监督。

第九章　安全预警与应急处置

第四十八条 网信办按照规定通报网络安全监测预警信息。各单位应当根据国家、地方网络安全部门、网信办发布的预警信息及时做好相应防范工作，做好相应处置工作。

第四十九条 网信办负责制定网络安全事件应急预案，按照应急预案对安全事件进行分级、分类处理。安全事件相关单位及人员应积极配合，认真落实网络安全事件处置相关工作。为避免安全事件不良影响扩大，网信办有权直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。

第五十条 各单位网络安全管理人员必须熟悉本单位网络安全事件应急处置措施。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。

第五十一条 校内各单位应根据本单位网络安全和信息化建设情况制定相应的监控与值守制度，重要敏感时期按照要求做好网络安全值班值守工作。

第五十二条 校园网内发生网络安全事件，应当立即启动网络安全事件应急预案，各单位和相关人员须按照应急预案规定进行处置。

学校各单位或师生员工均有义务及时向网信办报告网络安全事件，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。

第五十三条 网信办负责组织校内网络安全事件处置应急演练，相关单位应积极参与，通过演练提高校内网络安全事件处置能力。

第十章　附则

第五十四条 本办法为校内网络安全工作的基本规定，校内其他涉及网络安全的相关规定应以本办法为依据，若有不同之处以本办法为准。

第五十五条 本办法由网信办负责解释。

第五十六条 本办法自印发之日起施行。

集美大学学校办公室　　2023 年 9 月 30 日印发