中山大学文件

中大信息〔2017〕1号

中山大学关于印发《中山大学信息技术安全管理办法》的通知

校机关各部、处、室，各学院、直属系，各直属单位，各有关科研机构:

为加强学校信息技术安全管理、推进学校信息系统（含互联网网站）安全等级保护工作、提高信息技术安全防护能力和水平、保障学校各项事业健康有序发展，根据有关规定，结合我校实际，学校研究制定了《中山大学信息技术安全管理办法》。该办法已经中山大学2016年第27次党委常委会审议通过，现予以印发，请遵照执行。

特此通知。

中山大学

2017年1月11日

中山大学信息技术安全管理办法

第一章　总　则

第一条 为加强学校信息技术安全管理，推进学校信息系统（含互联网网站）安全等级保护工作，提高信息技术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《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）、《教育部关于进一步加强直属高校直属单位信息技术安全工作的通知》（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，结合我校实际，特制定本办法。

第二条 本办法所称信息技术安全工作，是指为使由学校建设、运行、维护或管理并支撑学校教学、科研和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、可用性等得到保持、不被破坏所开展的相关管理和技术工作。

本办法所指学校各单位包括各机关部、处、室，学院、直属系，直属单位以及有关科研机构。

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，建立健全信息技术安全责任体系，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履行信息技术安全的义务和责任。

第二章　组织机构与职责

第四条 学校主要负责人是学校信息技术安全的第一责任人，分管信息化工作的校领导协助主要负责人履行学校信息技术安全责任。

第五条 信息化管理办公室是学校信息技术安全归口管理部门，负责统筹学校网络安全与信息化建设工作。具体职责包括:

（一）制定信息技术安全总体规划，并组织实施;

（二）拟定信息技术安全管理规章制度，制定信息技术安全标准规范;

（三）组织开展信息系统安全等级保护工作;

（四）负责信息安全应急管理，协调处理与政府信息安全管理部门的关系;

（五）组织信息安全宣传和教育培训工作;

（六）负责信息技术安全监督检查工作;

（七）学校信息技术安全的其他工作。

第六条 网络与信息技术中心是信息安全技术支撑单位，负责学校信息技术安全防护体系的建设、运行维护、技术指导和服务支持。

第七条 学校各单位是本单位网络安全和信息化工作的责任主体，各单位主要负责人是本单位网络安全和信息化工作第一责任人，负责按本办法落实信息技术安全工作。

第三章　校园网络管理

第八条 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。

第九条 校园网络规划由信息化管理办公室制定。涉及光缆布线、网络机房、网络设备、网管系统、域名管理、安全防护、认证计费、网络接入与运维等方面，由网络与信息技术中心负责建设、运行、维护和管理。校园规划管理部门和建设部门负责在学校地下管网统一管理的原则下，进行规划、建设和运行维护。学校所有基建、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，由网络与信息技术中心统一出口、统一管理和统一防护。未经批准，学校各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 网络与信息技术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 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与信息技术中心负责实施。涉密信息系统不得接入校园网络。

第十三条 校园网络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。

第十四条 严禁任何单位和个人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

第十五条 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。网络与信息技术中心负责数据中心的建设、运行、维护和管理。

第十六条 网络与信息技术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。

第十七条 网络与信息技术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单位业务数据库之间完成数据交换和共享。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。

第十八条 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。网络与信息技术中心负责统一身份认证平台的安全，学校各

单位负责本单位应用系统的权限管理及安全。

第十九条 原则上，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，须报信息化管理办公室审批。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，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。

第二十条 网络与信息技术中心对学校数据中心的使用实施准入管理，负责制定使用数据中心的技术规范和标准，在系统上线前进行安全检测。符合技术规范标准并检测通过的系统方可上线运行。

第二十一条 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信息技术安全的活动。

第五章 信息系统建设、运行和维护管理

第二十二条 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，建立健全信息技术安全防护体系，全面实施信息系统安全等级保护制度。

第二十三条 信息化管理办公室负责制定学校信息系统项目规划和顶层设计。学校各单位根据本单位业务需求，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获学校信息化建设经费的优先支持。

第二十四条 信息化管理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。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。网络与信息技术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，并协助学校各单位进行系统定级、建设整改。

第二十五条 为确保项目质量，信息化管理办公室在立项阶段组织需求、技术、预算等方面的专家论证。信息系统建设单位在立项阶段应确定安全保护等级，由信息化管理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，由信息化管理办公室统一办理系统备案。

第二十六条 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。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。

第二十七条 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。对于安全等级第二级以上（含第二级）的信息系统，由信息化管理办公室会同网络与信息技术中心组织等级测评。信息系统通过初步验收和信息安全保护等级

测评后，由信息化管理办公室组织竣工验收。

第二十八条 信息系统开发环境、测试环境和运行环境应严格隔离，网络与信息技术中心负责上述环境的建设、运行、维护和管理。

第二十九条 信息系统建设单位可自行或委托网络与信息技术中心维护信息系统。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，原则上应由网络与信息技术中心维护。

第三十条 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）进行安全审计，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。

第三十一条 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。

第三十二条 对于安全等级第二级以上（含第二级）的信息系统，信息化管理办公室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，四级系统应每年进行两次测评，三级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

第三十三条 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。

第三十四条 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。

第三十五条 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。

第三十六条 网络与信息技术中心负责学校核心信息系统的备份与恢复管理，制订备份与恢复计划，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计划，并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

第三十七条 学校各单位开办互联网网站，应使用学校互联网域名和互联网 IP 地址，并遵守《中山大学互联网网站管理办法》及相关规章制度。

第三十八条 网络与信息技术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。

第三十九条 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，通过网络与信息技术中心组织的安全检查方可正式上线。

第四十条 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。

第四十一条 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、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。

第四十二条 原则上，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。

第四十三条 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

第四十四条 网络与信息技术中心为学校各单位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。

第四十五条 网络与信息技术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。

第四十六条 师生员工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，应立即通知网络与信息技术中心处理。

第九章 终端计算机安全管理

第四十七条 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。

第四十八条 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。网络与信息技术中心对终端计算机的安全管理提供技术支持和指导。

第四十九条 网络与信息技术中心建立终端计算机统一管理平台，实现常用正版软件下载分发、系统补丁安装、病毒软件安装升级及漏洞管理等功能。

第五十条 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并定期更改。

第五十二条 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。

第五十三条 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。

第五十四条 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

第五十五条 存储介质是指存储数据的载体，主要包括硬盘、存储阵列、磁带库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。

第五十六条 原则上，存储阵列、磁带库等大容量介质应托管在学校数据中心，并由网络与信息技术中心统一运行、维护和管理。网络与信息技术中心应采取必要技术措施防范数据泄漏风险，确保存储数据安全。

第五十七条 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。

第五十八条 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。

第五十九条 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。

第六十一条 网络与信息技术中心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，可由网络与信息技术中心集中销毁。

第十一章 人员安全管理

第六十二条 学校各单位应建立健全本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。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。

第六十三条 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、徽章以及学校提供的软硬件设备，并签署安全保密承诺书。

第六十四条 学校各单位应定期对信息技术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。

第六十五条 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 外包服务安全管理

第六十六条 信息技术外包服务是指信息系统的开发和运维的外包。

第六十七条 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信息安全与保密协议，明确信息安全与保密责任，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信息安全与保密协议应按学校合同管理办法的有关要求，报信息化管理办公室审核。

第六十八条 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。

第六十九条 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。

第七十条 网络与信息技术中心负责远程在线运维管理设备的统一购置、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 信息安全应急管理

第七十一条 信息化管理办公室负责学校信息安全应急工作的统筹管理，网络与信息技术中心负责信息安全应急工作的技术支撑和保障。

第七十二条 信息化管理办公室负责制定学校信息技术安

全事件报告与处置流程，网络与信息技术中心负责制订学校信息技术安全应急预案;若学校信息技术安全应急预案不能满足需求，相关单位可制订本单位信息技术安全应急预案。信息技术安全应急预案制修订后应及时报信息化管理办公室备案。

第七十三条 信息化管理办公室定期组织信息技术安全应急演练，评估并适时组织信息技术安全应急预案修订。学校各单位应组织开展信息技术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。

第七十四条 网络与信息技术中心负责组建学校信息安全应急技术支援队伍，完善24小时应急值守制度，提高信息安全事件的预防、预警和应对能力，预防和减轻信息安全事件造成的损失和危害。

第七十五条 学校各单位应按照学校信息技术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。

第七十六条 学校各单位或师生员工均有义务及时向网络与信息技术中心报告信息安全事件，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。

第十四章 信息安全教育培训

第七十七条 信息化管理办公室负责组织学校信息安全宣传和教育培训工作，建立健全相关制度。

第七十八条 信息化管理办公室定期组织开展针对师生员工的信息安全教育，提高师生员工的安全和防范意识。

第七十九条 信息化管理办公室定期开展针对信息安全管理人员和技术人员的专业技能培训，提高信息安全工作能力和水平。

第十五章 信息安全检查监督

第八十条 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，并配合有关部门的信息安全检查、信息内容检查、保密检查与审批等工作。

第八十一条 信息化管理办公室联合网络与信息技术中心对学校各单位的信息技术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。

第八十二条 信息化管理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信息安全主管部门。

第十六章 信息安全责任追究

第八十三条 学校建立信息安全责任追究和倒查机制。

第八十四条 有关单位在收到网络与信息技术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。

第八十五条 学校各单位应按照信息技术安全事件报告与处置流程及时、如实地报告和妥善处置信息技术安全事件。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。

第八十六条 师生员工违反本办法规定的，由信息化管理办公室责令改正，并通报批评；拒不改正或者导致危害信息技术安全等严重后果的，根据学校有关规定给予以纪律处分。触犯刑律的，移交司法机关处理。

第十七章 附则

第八十七条 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，由学校保密办公室监督指导。

第八十八条 学校各单位可参照本办法制订本单位的实施细则。

第八十九条 本办法自 2017 年 3 月 1 日起实施，由信息化管理办公室负责解释。学校原有相关规定 理 月