遵义医科大学办公室文件

遵医校办发〔2021〕10号

遵义医科大学办公室
关于印发遵义医科大学信息系统
管理制度的通知

各院系、各部门：

《遵义医科大学信息系统管理制度》已经学校2020年12月26日第二十次校长办公会审议通过，现印发给你们，请遵照执行。

遵义医科大学办公室

2021年1月7日

遵义医科大学信息系统管理制度

第一章　总　则

第一条　为明确岗位职责，规范操作流程，保障学校信息系统安全、有效运行，根据有关法律、法规和政府有关规定，结合学校实际，制定本制度。

第二条　计算机信息系统是指由学校及各二级部门利用计算机通信技术，对内部控制进行集成、转化和提升所形成的信息化管理平台。

第三条　利用信息系统实施内部控制，需注意下列风险：

（一）信息系统缺乏或规划不合理，可能造成信息孤岛或重复建设，导致学校管理效率低下；

（二）系统开发不符合内部控制要求，授权管理不当，可能导致无法利用信息技术实施有效控制；

（三）系统运行维护和安全措施不到位，可能导致信息泄漏或毁损，系统无法正常运行。

第四条　重视信息系统在内部控制中的作用，根据内部控制要求，结合组织架构、业务范围、地域分布、技术能力等因素，制定信息系统建设整体规划，加大投入力度，有序组织信息系统开发、运行与维护，优化管理流程，防范经营风险，全面提升现代化管理水平。

第五条　计算机网络管理中心负责学校范围内的计算机信息系统安全管理工作。

第二章 信息系统的开发

第六条 计算机网络管理中心根据信息系统建设整体规划提出项目建设方案，明确建设目标、人员配备、职责分工、经费保障和进度安排等相关内容，按照规定的流程报批通过后实施。

计算机网络管理中心组织各二级单位提出开发需求和关键控制点，规范开发流程，明确系统设计、编程、安装调试、验收、上线等要求，严格按照建设方案、开发流程和相关要求组织开发工作。

计算机网络管理中心根据项目建设方案、需求、关键控制点等选择可采取外购调试或业务外包两种方式进行。采取外购调试的，应当采用公开招标等形式择优确定供应商或开发单位。

第七条 针对不同数据的输入方式，考虑对进入系统数据的检查和校验功能。对于必需的后台操作，应当加强管理，建立规范的流程制度，对操作情况进行监控或审计。

应当在信息系统中设置操作日志功能，确保操作的可审计性；对异常的或违背内部控制要求的交易和数据，应当设计系统自动报告并设置跟踪处理机制。

第八条 外包开发须加强信息系统开发全过程的跟踪管理，组织开发单位或开发人员与各部门的进行沟通和协调，督促开发单位或开发人员按照建设方案、计划进度和质量要求完成编程工作。

第九条 计算机网络管理中心应根据配备的硬件设备和系统软件的具体情况，组织安排相应的硬件厂家或软件开发商的技术人员入场调试。对于关键的软硬件设备，应安排专人负责

跟踪、记录整个安装调试过程；在完成软硬件设备的安装调试后，应注意做好有关文档的验收及归档保存工作。

第十条 外购调试或业务外包的信息系统上线前，计算机网络管理中心须切实做好各项准备工作。查验设备厂商、软件开发商或开发人员提交的有关运行维护资料，包括技术手册、操作手册等，并负责监督对相关岗位人员的技术培训工作。制定科学的上线计划和新旧系统转换方案，考虑应急预案，确保新旧系统顺利切换和平稳衔接。系统上线涉及数据迁移的，还应制定详细的数据迁移计划。

第十一条 对于信息技术软件，应注意母盘或源代码的保存登记工作，并由专人管理。日常工作中应尽量使用母盘复制品，避免造成对母盘或源代码的破坏。

第三章 信息系统的运行与维护

第十二条 信息系统投运前，计算机网络管理中心要掌握有关设备所提供的各种系统监控、维护工具，并检查其安全性和完整性。

第十三条 信息系统投运前，计算机网络管理中心应与软件开发商和设备的供应商共同制定系统投运实施方案以及应急处理方案，并尽可能在测试环境中测试通过后，再在实际运行环境中实施。

第十四条 信息系统变更应当严格遵照管理流程进行操作。信息系统操作人员不得擅自进行系统软件的删除、修改等操作；不得擅自升级、改变系统软件版本；不得擅自改变软件系统环境配置。

对学校重大信息系统配置的更改，应先形成方案文件，经计算机网络管理中心讨论确认可行，报学校领导批准后执行。方案中应包括系统备份方式、调试运行期限、更改和操作记录、应急措施等相关内容。

第十五条 根据业务性质、重要性程度、涉密情况等确定信息系统的安全等级，建立不同等级信息的授权使用制度。

（一）各信息管理部门建立用户管理制度，根据工作岗位需求严格控制重要业务系统的访问权限；根据数据的保密规定和用途，确定拥有系统权限人员的存取权限、存取方式和审批手续。合理分配用户权限，对不同岗位用户、不同信息等级分别设定口令。定期审查系统账号，避免授权不当或存在非授权账号，禁止不相容岗位用户账号交叉操作。

（二）对于通过网络传输的涉密或关键数据，应当采取加密措施，确保信息传递的保密性、准确性和完整性。

（三）计算机终端用户计算机应当安装安全软件，防范信息系统受到病毒等恶意软件的感染和破坏。

（四）计算机终端用户计算机内的资料涉及学校秘密的，应设定开机密码或将文件加密；凡涉及学校机密的数据或文件，非工作需要不得以任何形式转移，更不得透露给他人。离开原工作岗位的员工由所在部门负责人将所有相关资料收回并保存。

（五）计算机终端用户务必将重要数据存放在计算机硬盘中除系统盘分区(操作系统所在的硬盘分区，一般是 C 盘)外的硬盘分区。计算机信息系统发生故障，应及时与计算机网络管理中心联系并采取数据安全保护措施。

（六）严禁安装与工作无关的程序与软件，严禁使用计算机进行与工作无关的操作，以免浪费资源，传播病毒。每日下班后及时关机，并切断电源。

（七）每周备份业务数据并刻制光盘保存，确保信息系统一旦发生故障能够快速恢复。备份数据库数据不得更改，数据备份光盘应异地存放，保存期限为 3 年。

（八）计算机终端用户未做好备份前不得删除硬盘中的重要数据。对重要的数据应双份备份，并异地存放；对采用磁性介质或光盘保存的数据，应做好防磁、防火、防潮和防尘工作，定期进行检查、复制，防止由于磁性介质损坏导致数据丢失。

（九）严禁试图获得非法权限、破解密码、攻击系统的行为，严禁未经授权的使用和操作；对于学校网络，普通用户只有浏览查看权利，严禁非法篡改、故意攻击或躲避防火墙的行为。

第十六条 计算机网络管理中心人员必须熟练掌握局域网络使用的基本知识。熟悉工作范围内工作软件及其使用方法。严格遵守信息传递操作流程，严禁外泄网络用户密码及共享权限密码；严禁擅改他人文件。

第十七条 学校全体人员均有权制止违反规定、可能损害网络的行为，并有义务及时向计算机网络管理中心汇报。存在违反规定的可疑情况，应立即向计算机网络管理中心通报。

第十八条 信息系统设备完成安装调试后，未经计算机网络管理中心同意，任何个人或部门不得擅自移动或拆除。如因工作需要，确需对有关设备进行移动或拆除，需报计算机网络管理中心审批同意后，由计算机网络管理中心组织有关技术人

员实施，并做好相应的登记变更工作。关键硬件设备完成安装后，运行地点要相对固定，移动或拆除要在完成审批程序后，方可实施。

第十九条 硬件设备的报废应由使用部门提出书面申请，计算机网络管理中心根据设备使用情况进行审核，出具设备报废清单，按固定资产报废程序办理。

第四章 信息系统的设备采购与维护

第二十条 各二级部门IT设备或配件的采购与管理参照学校设备处相关制度执行，由计算机网络管理中心督导落实。综合管理部设置专门的软硬件设备台帐，并由专人保管，做到登记明晰，设备的进出库、安装有账可查。计算机网络管理中心应每年对各部门的计算机设备资产进行核查，要求做到与有关固定资产资料相对应。

第二十一条 设备进入使用部门后，使用部门应保证运行设备的安全及完整，防止出现设备的人为损坏或丢失。

第五章 禁止行为及处罚措施

第二十二条 学校教职员工应遵守《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）及国家、省、市有关规定，严格遵守学校有关规章制度，严格执行安全保密制度，有利用学校网络进行下述行为之一者，视情节严重程度给予警告、记过等处分，并有权解除劳动合同；给学校造成损失的，应予赔偿；构成犯罪的，移交司法机关处理。

（一）发布反动、非法和虚假的消息，或制作、浏览、复制、传播反动信息；

（二）宣扬封建迷信、邪教、黄色淫秽制品、违反社会公德、以及赌博和教唆犯罪等；

（三）漫骂攻击他人，散布谣言、扰乱社会秩序、鼓动聚众滋事；

（四）泄露他人隐私、攻击他人及损害他人合法权益；

（五）制造或者故意输入、传播计算机病毒和其他有害数据，进行任何黑客活动和性质类似的破坏活动；

（六）泄露、外借和转移学校专业数据信息。利用非法手段复制、截收、篡改学校计算机信息系统中的数据；

（七）利用扫描、监听、伪装等工具对学校网络和服务器进行恶意攻击，或非法侵入他人网络和服务器系统；

（八）利用计算机和网络干扰他人正常工作；

（九）工作时间严禁使用计算机玩游戏，播放MP3、CD、DVD、在线视频等；

（十）法律和法规禁止的其他有害信息。

第二十三条 严格机房管理。有违反以下情况行为之一者，情节轻微的，给予警告处分；情节严重，给学校造成重大损失的，需赔偿相应损失。

（一）严禁携带易燃易爆、强磁物品及其它与机房工作无关的物品进入机房；禁止在机房内吃食物、抽烟、随地吐痰；未经机房管理人员同意严禁无关人员进入机房；

（二）未经学校授权且机房管理人员在场监督，任何人不得自行配置、更换或挪用机房内的路由器、交换机、服务器以

及其他通信设备等；不得在机房服务器上安装与系统应用无关的软件；

（三）机房设备未发生故障或无故障隐患时机房管理人员不得私自对光纤、路由器、交换机、硬件防火墙、UPS 系统、服务器和网线等网络设备进行任何调试；

（四）严禁撕毁、涂画或遮盖 IT 设备标签，或未经计算机网络管理中心备案擅自调整学校计算机信息系统的配置；严禁使用假冒伪劣产品、擅自外接电源开关和插座、擅自移动和装拆各类设备及其他辅助设备、擅自请人维修；

（五）禁止未授权用户接入学校计算机网络及访问网络中的资源；

第二十四条 计算机终端用户因主观操作不当导致设备、设施损坏，应承担相应修复费用；不能修复的按所损坏设备、设施市场价值的 20%—80%予以赔偿；蓄意破坏设备、设施的，除照价赔偿外，视情节严重给予行政处罚。

第六章 附 则

第二十五条 珠海校区参照本规定执行。

第二十六条 本制度自公布之日起施行；由学校网络安全和信息化领导小组负责解释。

遵义医科大学办公室 2021 年 1 月 7 日印发

共印 3 份