沈阳城市建设学院文件

城建院发〔2019〕140 号　　签发人：张蕾

关于印发《沈阳城市建设学院核心机房管理办法（试行）》的通知

各单位、部门：

现将《沈阳城市建设学院核心机房管理办法（试行）》印发给你们，请认真学习并遵照执行。

沈阳城市建设学院

2019 年 12 月 31 日

沈阳城市建设学院核心机房管理办法（试行）

学校核心机房是学校网络的神经系统，承载校区内各类网上系统业务的后台运行。为进一步加强对学校核心机房的管理，确保核心机房的各项安全，结合学校实际，特制定本办法。

第一章　日常行为准则

第一条 注意保持环境卫生。严禁在核心机房用餐、抽烟、随地吐痰；对于意外或工作过程中弄污核心机房地板和其它物品的，必须及时采取措施清理干净，保持核心机房无尘洁净。

第二条 注意检查核心机房的防晒、防水、防潮情况，维持核心机房环境通爽，注意天气对核心机房的影响，阴雨天气应及时主动检查去水通风等设施运转情况。

第三条 技术人员有义务维护核心机房安全、平稳的设备工作环境，一切有可能危及核心机房设备的行为，技术人员有权立即禁止。

第二章　核心机房安保

第四条 出入核心机房应注意锁好防盗门。对于教学参观进出核心机房的教师及学生，核心机房相应的工作人员应负责教师及学生的安全防范工作。最后离开核心机房的工作人员必须自觉检查和关闭所有核心机房的门窗、锁定防盗装置。拒绝陌生人进出核心机房。

第五条 工作人员离开工作区域前，应保证工作区域内保存

的重要文件、资料、设备、数据处于安全保护状态。锁定服务器并将重要调试设备妥善保存等。

第六条 核心机房的工作人员负责到访人员的出入登记。

第七条 到访人员进入必须有专门的工作人员全面负责其行为安全。

第八条 未经主管领导批准，禁止将核心机房相关的钥匙、保安密码等重要信息透漏给其他人员，同时有责任对安防信息保密。对于遗失钥匙、泄露安防信息的情况要及时上报，并积极主动采取措施保证核心机房安全。

第九条 禁止带领与核心机房工作无关的人员进出核心机房。

第十条 绝不允许与核心机房无关的工作人员直接或间接操纵核心机房任何设备。

第十一条 出现核心机房盗窃、破门、火警、水浸、110 报警等严重事件时，核心机房工作人员有义务以最快的速度和最短的时间到达现场，协助处理相关的事件。

第三章　消防安全

第十二条 核心机房工作人员应熟悉核心机房内部消防安全操作和规则，了解消防设备操作原理，掌握消防应急处理步骤、措施和要领。

第十三条 任何人不能随意更改消防系统工作状态及设备位置。

第十四条 如发现消防安全隐患，应及时采取措施解决，不

能解决的应及时通知相关负责人，并跟踪处理进展直至问题彻底解决。

第四章　核心机房硬件设备安全使用

第十五条 核心机房人员必须熟知核心机房内设备的基本安全操作和规则。

第十六条 应定期检查、整理硬件物理连接线路，定期检查硬件运作状态如设备指示灯、仪表，定期查阅硬件运行自检报告，从而及时了解硬件运行状态。

第十七条 禁止随意搬动设备、随意在设备上进行安装、拆卸硬件随意更改设备连线、禁止随意进行硬件复位。

第十八条 对会影响到全局的硬件设备的更改、调试等操作应预先发布通知，并且应有充分的时间、方案、人员准备，才能进行硬件设备的更改。

第十九条 不允许任何人在服务器、交换设备等核心设备上进行与工作范围无关的任何操作。

第二十条 要注意和落实硬件设备的维护保养措施。

第五章　软件安全使用

第二十一条 禁止在服务器上进行试验性质的软件调试，禁止在服务器随意安装软件。需要对服务器进行配置，必须在其它可进行试验的机器上调试通过并确认可行后，才能对服务器进行准确的配置。

第二十二条 对会影响到全局的软件更改、调试等操作应先

发布通知，并且应有充分的时间、方案、人员准备，才能进行软件配置的更改。

第二十三条 不允许任何人员在服务器等核心设备上进行与工作范围无关的软件调试和操作。

第六章　核心机房资料、文档和数据安全规定

第二十四条 禁止任何人员将核心机房内的资料、文档、数据、配置参数等信息擅自以任何形式提供给无关人员或向外随意传播。

第二十五条 对于牵涉到网络安全、数据安全的重要信息、密码、资料、文档等必须妥善存放。外来工作人员的确需要翻阅文档、资料或者查询相关数据的，应由核心机房相关负责人代为查阅，并只能向其提供与其当前工作内容相关的数据或资料。

第七章　核心机房财产登记和保护规定

第二十六条 核心机房的设备、线路、资源等必须有清晰的数量、型号记录。

第二十七条 核心机房工作人员应安全和谨慎使用核心机房的任何设备、仪器等，在使用完毕后，应将物品归还并存放于原处，杜绝随意摆放。

第二十八条 对于使用过程中损坏、非正常消耗、遗失的物品应汇报登记，并对责任人追究相关责任。

第二十九条 未经主管领导同意，不允许向他人外借或提供核心机房设备和物品。

第八章　火灾应急预案

第三十条 火灾一旦发生，在消防队员未赶到前，中心技术人员必须保持头脑清醒，迅速开展报警、开启应急通道、疏散核心机房内滞留人员、切断电源等工作。

第三十一条 第一时间向领导小组汇报，有条件记录下具体时间、硬件毁坏程度、网络毁坏程度等第一手资料。

第三十二条 禁止无关人员进出核心机房。

第三十三条 根据硬件毁坏程度确定处理方案。

第三十四条 根据实际情况恢复异地数据库备份，启动异地服务器设备。

第三十五条 进一步检查网络连接确保各楼之间的网络安全。

第三十六条 快速设计最佳处理方案。

第三十七条 组织相关人员进行网络重建。

第九章　停电应急预案

第三十八条 核心机房意外停电后，首先确定停电的范围以及受影响的设备范围。

第三十九条 确定停电的范围为本校后，工作人员马上打电话给后勤集团，并汇报网络应急预案领导小组。

第四十条 如果停电范围小，只限核心核心机房，在 UPS 正常供电的情况下不会影响系统的正常工作；如果停电时间超过 UPS 的供电时间，需及时通知各单位部门。

第四十一条 如果停电的时间在 1 个小时之内，可以在 UPS

的正常供电范围内等待电力恢复。此期间 UPS 只能供应核心服务器的供电，如果不能确认在 2 个小时内恢复供电，核心机房技术人员在 UPS 供电 1.5 小时后，按照核心机房设备断电关机启动规程关掉其他的设备和服务器，最后停掉核心交换机和路由器电源。供电恢复后按顺序启动服务器、数据库及相关设备。

主　送：各单位、部门

党政办公室　　2019 年 12 月 31 日印发