

防灾科技学院信息化管理中心

信息中心〔2021〕29号

关于印发《防灾科技学院核心机房安全管理制度》的通知

学校各部门、各单位：

为保证学校信息系统机房内设备处于最佳状态，使其运行服务质量能够满足业务使用的需求，并保证信息资产不被非法物理访问。特制定《防灾科技学院核心机房安全管理制度》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021年12月3日

防灾科技学院核心机房安全管理制度

第一章 总则

第一条 为保证学校信息系统机房内设备处于最佳状态，使其运行服务质量能够满足业务使用的需求，并保证信息资产不被非法物理访问，特制定本规定。

第二条 信息化管理中心完成对机房维护和管理并负责此规定执行，由系统管理员负责对核心机房的日常管理。

第二章 机房环境管理

第三条 加强机房的日常防火管理，具体管理要求如下：

1. 机房防火要求应符合现行国家标准《建筑设计防火规范》（GB50016）的有关规定。
2. 信息系统机房的耐火等级不应低于二级。
3. 主机房的顶棚、壁板（包括夹芯材料）和隔断应为不燃烧体，且不得采用有机复合材料。
4. 禁止将易燃、易爆、有毒物品、强磁物品带入机房。

第四条 机房空调应指定专人负责，使机房温、湿度应符合机房维护技术指标要求：

1. 夏季：正常温度范围：22℃+2℃
正常湿度范围：45%~65%
2. 冬季：正常温度范围：20℃+2℃
正常湿度范围：45%~65%

第五条 机房应有良好的防静电措施，机房内配置防静电手环，地面铺设防静电地板。

第六条 机房照明设备安全可靠，应配备应急灯，各种照明设备应有机房专人负责，定期检修。

第七条 机房门窗要密闭，环境保持卫生清洁，机房内设备摆放整齐。

第八条 信息系统机房应具备单独的 UPS 不间断电源或逆变器，并有专人负责维护，针对机房内电力系统，还有如下要求：

1. 应配备不间断电源系统和电池，电池容量至少保证在停电期间能够完成正常关机时间。

2. 电子信息设备正常工作时输入电压波形失真度 $\leq 5\%$ ，零地电压 $< 2V$ 。

第九条 机房内设备必须按照设计及相关规定布置，机房内预留位置不能随意占用。

第三章 机房设备进出管理

第十条 设备的维护必须有专人负责，机房管理人员应定期检查相关设备运行情况，他人不可随意操作。设备需要停机检查时，应经办公室批准后，方可进行。关闭设备时，应经办公室领导同意。

第十一条 未经办公室授权，机房内的任何设备不得搬出机房，外来设备也不得擅自进入机房，机房设备的进出由系统管理员负责。

第十二条 设备进出机房的流程：

1. 由登记申请人提交设备进出机房申请流程，明确申请事由及设备相关信息，负责人审核通过后，XX 全程陪同设备方可进入机房。
2. 相关工作人员组织设备和系统安装，机房管理员进行配合。
3. 设备和系统安装完毕后，机房值班员进行登记并在设备上贴签，更新机柜部署图；如果是网络或安全设备，还需更新网络拓扑图。

第十三条 设备进入机房，应接入由 UPS 供电的插座。每个插座接入设备的数量，应符合插座的容量要求。

第十四条 非电子信息设备禁止接入 UPS 供电的电源插座。空调机吸尘器等应接市电。

第十五条 设备安放合理，布线整齐，强电与通信电缆走线分离，避免交叉，禁止随意改动布线。

第四章 机房人员进出管理

第十六条 机房是服务器及网络主设备放置和运行的区域，机房管理员负责机房的进出管理。

第十七条 在机房的入口处加注标识，如“机房重地，闲人免进”等，并且将《机房安全管理制度》张贴在入口处，对来访者起到标识与警示作用。

第十八条 外来人员不得擅自进入机房。因公原因进入机房，

应由运维接待人员提交带外部人员出入机房申请单，明确访问事由并得到负责人批准后，由运维人员全程陪同才能进入机房，仅授权人员进出机房必须及时锁门，杜绝其他非授权人员以任何理由私自进入机房。

第十九条 办公室内部人员在机房有突发事件（如火灾等）时，可以不经过请示直接进入机房，协助系统管理员处理突发事件，其他人员未经许可不得擅自进入机房。

第五章 日常巡检管理

第二十条 机房管理员和网络管理员需对人员及设备进出机房严格把关，维护更新设备资料表。

第二十一条 系统管理员和网络管理员定时巡检中心机房设备状态、各网络设备以及各业务系统运行状况，填写日常巡检表，出现异常情况时，及时上报办公室并组织力量排查处置。

第二十二条 系统管理员应检查机房内 UPS、空调、监控系统、门禁、配电线路的可靠运行情况，发现故障或安全隐患及时排除。

第二十三条 安全管理员负责每日对机房安全设备进行安全巡检，并进行分析记录。

第二十四条 建立严格的联络机制，办公室人员在外出服务或休班时，要保持 24h 通信联络的畅通。

第二十五条 单位不定期组织消防安全学习，开展多种形式的消防安全宣传教育。

第二十六条 消防通道禁止员工随意出入,消防门不得上锁。各楼层张贴逃生路线线图供员工参考。

第二十七条 对消防设备设施的性能情况经常进行检查,确保消防栓、灭火器具等完好、有效,消防通道畅通,消防标识清晰、准确。

第二十八条 办公区域严禁存放易燃易爆物品。

第二十九条 发生火情应立即采取相应措施。

第六章 机房突发事件应急预案

第三十条 火警。值班人员要随时提高警惕,如发现机房内有异常气味,应仔细、认真地巡视机房各处,直到查清原因,确定无危险情况为止。如发现机房内有烟雾,甚至火焰。首先切断电源(每个值班人员均应清楚电源开关位置并确保其畅通无阻)。对烟雾产生处,应检查原因,尽力扑灭,尤其应注意活动地板下的情况。对火情,一方面要尽快报警,同时要采取一切措施控制并扑灭火焰。

第三十一条 水警。机房内如有水管破裂等严重水情时,要切断电源,然后设法排水,保护机房内各种设备的安全。对无法控制的严重水情,要立即报警。机房顶部漏水时,应设法用容器及塑料布保护机房各种设备不被淋湿。情况严重时切断电源,并通知维修部门采取必要的措施。

第三十二条 停电。网络系统因停电而启动暂停和恢复程序

统一由系统管理员负责，如遇紧急情况需要由其他人启动，应得到系统管理员或信息安全应急指挥小组授权；接到停电通知后，系统管理员应提前一天通过有效方式发布通知公告，通知内容应包括网络暂停原因、暂停时间及恢复时间等事项；如遇重大故障或系统受到攻击，需停机进行维护时，系统管理员应及时通知业务主管部门。为保证系统暂停程序有足够的时间，系统暂停应在停电前一小时开始操作；系统恢复应在确认来电后半小时内启动；发现意外停电应及时通知安全保密管理员和系统管理员，并通知单位领导。询问机电厂商，确定停电原因和初步恢复时间，如无法及时恢复系统，系统管理员应及时正常地关闭重要的网络设备、服务器、UPS 和主电源。通知部门领导和重要部门，报告采取的措施及恢复供电和系统运行时间。确认供电恢复后，启动网络设备和服务器恢复系统运行。

第七章 附则

第三十三条 本规定的解释权归信息化管理中心。

第三十四条 本制度自发布之日起施行，《防灾科技学院核心机房管理规定》（信息中心〔2021〕03号）文件同时废止。

