

防灾科技学院信息化管理中心

信息中心〔2021〕08号

关于印发《防灾科技学院网络信息安全日常管理操作规定》的通知

学校各部门、各单位：

为规范学校网络信息安全日常操作，提高网络安全活动执行效率，降低可能由人员误操作等导致的一系列网络安全事件，特制定《防灾科技学院网络信息安全日常管理操作规定》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021年10月7日

防灾科技学院网络信息安全日常管理操作规定

第一章 总则

第一条 为规范防灾科技学院（以下简称“学院”）网络信息安全日常操作，提高网络安全活动执行效率，降低可能由人员误操作等导致的一系列网络安全事件，特制定本规定。

第二条 本规定所指网络安全相关活动是指机房物理设施日常维护、网络及安全设备软硬件日常管理、服务器设施日常管理等。

第二章 网络、安全、服务器软硬件管理

第三条 学院各单位使用人员必须熟悉系统和设备的技术结构、主要功能、主要性能指标和使用方法，严格遵守系统和设备的操作规程。

第四条 各类设备在开机前，必须检查环境条件，电源电压和连接线缆等，符合要求后方可开机。开机必须按规定的顺序和操作规程进行，并待设备稳定后方能进行工作。

第五条 设备如需关机，每次关机前，必须先保存当前运行日志，检查设备的运行状态，按要求顺序关机，并填写操作记录。

第六条 当设备在运行中发生故障时，必须报告相关领导，认真记录故障现象，保护故障现场，由专业维护人员检查维修。

第七条 所有设备必须定期进行维护保养，长期不用的库存设备应定期加电检查。

第三章 机房物理设施日常维护管理

第八条 机房物理设施日常维护管理是指门禁、电源、防火、防水、防静电、温湿度控制等设施日常维护保养，需采用合理的维护方式，降低维护过程风险。

第九条 机房物理设施日常维护管理的主要内容包括：

（一）加强机房温湿度管理，确保机房环境处于合理的温湿度范围。定期检查机房内的防火，防水，防盗等设施和安全警报装置。

（二）定期检查 UPS 系统和电源供电设备。

（三）建立完整的设备维护档案，定期调阅维护记录并进行分析比较，捕捉故障苗头，及时采取措施。

（四）从设备启动、停止的现象，正常运行时的噪声，设备上指示灯的状态，以及设备发热程度等方面感知预发现象。

（五）做好设施安全保障，制定设备故障的处理方案。

（六）按时更换或调整某些元器件或零部件。

（七）认真作好日常的例行性维护和测试。

（八）定期清除机房灰尘，保证机房卫生。

（九）每年定期清除机房地板下和走槽里的灰尘，检查线缆的完好性和隔离性，更换老化、变质和绝缘不好的线缆。

第四章 关键设备操作流程

第十条 针对网络关键设备如防火墙、核心交换机等设备操作，如设备需要断电或重启，需告知并通过信息化管理中心审批，

审批通过后在网络空闲时进行，如午休以及休息日。

第十一条 核心交换机、汇聚交换机，楼层交换机等网络设备的操作，需制定相应方案，方案通过领导审批之后，才能进行相关操作。操作过程中如有修改必须做好相应记录。

第十二条 设备配置变更后需进行专项测试，如查看网络是否有异常等，网络设备操作完成之后最短测试周期为一天。

第十三条 如网络设备需要断电，按照以下流程执行：

（一）首先 save 配置，然后导出配置。

（二）输入 shutdown -h now 关机命令，等待设备关机。

（三）在指示灯熄灭之后，切断电源。开机则反之。

第十四条 安全设备由信息化管理中心集中管理，网络安全设备维护方式及登录密码使用必须符合要求。

第十五条 如果机房发生大面积停电，将不必要的服务器以及不必要的网络设备做断电处理，以延长重要网络设备和主机的工作时间，如 UPS 报警只剩 5-15 分钟则做好配置及数据备份后关闭全部服务器与网络设备。

第十六条 服务器远程维护后需手动退出登录，服务器如需断电，需手动进行操作系统关机，等待系统关闭之后再行断电，严禁直接断电操作。

第五章 附则

第十七条 本规定由信息化管理中心负责解释。

第十八条 本规定自颁布之日起施行。

