

南昌技师学院

洪技政〔2025〕19号

关于印发《南昌技师学院网络安全管理制度》 等2个制度的通知

各科室、分院：

《南昌技师学院网络安全管理制度》《南昌技师学院校园网网络设施管理规定》已经2025年第4次院党委会研究通过，现印发给你们，请遵照执行。



南昌技师学院网络安全管理制度

第一章 网络安全管理职责

第一条 信息中心负责全院网络及信息安全日常工作，及时解决突发事件和问题，编制网络安全事故报告。校园网络发生信息案件以及遭到黑客攻击后，信息中心必须及时备案并向公安机关报告。

第二条 信息中心对师生用户上网进行安全教育指导和监督：

（一）学院各信息终端用户必须接受信息中心监督管理，教室和个人使用者必须严格使用由信息中心分配的 IP 地址。

（二）信息中心负责对校园网用户进行监督和检查，对入网计算机和使用者进行登记管理。

第二章 用户网络安全管理

第三条 任何部门和个人不得利用联网计算机从事下列活动：

（一）未经允许访问校园网络服务器、工作站、交换机、路由器及其它相关设备；未经允许对校园网设备所具有的功能、程序、数据进行删除、修改和增加；

（二）未经允许擅自提供与教育无关的网络服务；

（三）故意制作、传播计算机病毒与破坏性程序；

（四）其他危害网络安全的行为。

第四条 用户增强自我保护意识，经常更换口令，保护好用

用户名，不得更改 IP 及网络设置，不得盗用用户账号，同时有责任保障自身账号安全，严禁用各种手段破解他人口令、盗用他人用户名。不得利用各种网络设备或软件技术从事用户账户及口令的侦听、盗用活动。

第五条 装有涉密资料、重要数据、财务数据的电脑要以专线形式接入，与日常工作网络实行物理隔离。

第六条 校园网各类服务器中开设的账户和口令为个人用户所拥有的，信息中心对用户口令保密，不得向任何单位和个人提供这些信息。

第七条 校园网的系统软件、应用软件及信息数据由信息中心实施保护措施。任何人不得擅自将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

第八条 各部门需严格执行国家相关法律法规，防止发生窃密、泄密事件。未经允许，任何人不得让外来人员使用学院的网络系统。

第九条 未经批准，连结在学院网络上的所有用户不得再通过其它入口上因特网或外单位网络。

第三章 网络病毒的防治

第十条 每台终端计算机上须安装防病毒软件，各科室、分院要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向信息中心报告陌生、可疑邮件和计算机非正常运行等情况。

第十一条 信息中心负责给校园网中各服务器安装防病毒软件，定期进行病毒检查及清理，做好各服务器的防病毒和防篡改工作，及时下载并安装系统漏洞补丁，采取各种有效措施防止黑客攻击和破坏。

第十二条 所有 U 盘须检查确认无病毒后，方能上机使用。严格控制外来 U 盘的使用，各部门使用外来 U 盘须经检验认可，私自使用造成病毒侵害要追究当事人责任。

第四章 网络安全人员工作职责

第十三条 信息中心网络安全人员必须定期检查学院官网信息，发现有关泄漏机密及不健康信息第一时间删除、记录、上报主管领导。认真执行技术规范，监控、封堵、清除网上有害信息。

第十四条 信息中心网络安全人员对校园网络的系统及环境进行安全维护，充分利用现有的安全设备设施、软件，使用合理的技术手段对网络运行安全进行有效监控，最大限度防止计算机病毒入侵和黑客攻击。随时检查防火墙、网络病毒检测等网络安全技术措施的配置，对学院网络进行有效的网络安全配置以防止网络安全漏洞造成的后果扩散。

第十五条 信息中心网络安全人员要定期检查有关网络和服务器系统的运行日志，定期和不定期地对全院网络进行网络安全检查，重要网络设备必须保持日志记录，记录留存时间不少于 180 天。

第十六条 信息中心网络安全人员要注意保护网络数据信息

的安全,对于存储在数据库中的关键数据以及关键的应用系统及时进行数据备份,及时更新数据库和防病毒软件病毒库,定期对所有数据库进行漏洞扫描、补丁修复,保证重要数据的安全。

南昌技师学院办公室

2025年4月1日印发
