郑州轻工业大学网络安全和信息化领导小组办公室文件

郑轻大网信〔2022〕2号

# 郑州轻工业大学校园网接入终端使用规范

## 一、主机（接入设备）安全

（一）了解熟悉自己使用的接入终端的硬件配置及驱动软件，设备安装的应用软件类型、用途以及对摄像头、麦克风、通信录、记事本等访问的权限设置。

（二）使用原生内核的主流浏览器(IE Edge,谷歌Google Chrome，火狐FireFox，Safari等)，定期清理浏览器访问历史记录。

（三）安装杀毒软件(360安全卫士等)，及时更新病毒库，并定期查杀病毒、木马，进行终端安全性检测和修复。

（四）注销（报废、更换）的接入设备要及时进行数据迁移并销毁原有数据。

## 二、操作系统安全

（一）安装正版操作系统并及时更新系统，安装补丁。

（二）开启操作系统防火墙，了解其配置及安全防护策略设置。

（三）设置系统密码并符合强密码设置规范（字母、数字和特殊符号组合），并定期更新。

（四）定期清理系统垃圾，重装操作系统。

**三、应用软件安全**

（一）安装正版应用软件，不安装使用破解、盗版、第三方外挂以及非法应用软件。

（二）通过主流途径（官方、应用市场等）推送，下载应用软件。

（三）定期更新应用软件，不用的应用软件要及时卸载并清理使用痕迹。

（四）对所使用的即时通信（微信、QQ 等）、文件传输下载平台（网盘）等应用的临时文件要定期清理。

**四、数据安全**

（一）了解所用设备对个人隐私数据、办公业务数据的风险隐患，加强数据保护意识。

（二）使用主流输入法工具，熟悉所用设备的摄像头、麦克风等权限设置，打印机、扫描仪的共享权限范围。

（三）定期清理浏览器登录记录、访问记录、搜索引擎搜索记录、收藏夹记录等。

（四）对存留的重要数据进行备份，过程性数据用完及时清理。

**五、内容安全**

（一）浏览访问主流（官方）网站及平台的内容，有信息鉴别的

基本能力，不信谣、不传谣、不随意转发浏览到的内容，不随意扫描二维码。

（二）管理好自己（有权）使用的邮件系统账号及邮件内容，定期修改密码及清理内容。核实检查发件人，不打开可疑邮件及邮件附件。

（三）对自己在网络空间生产的内容负责，确保内容交互安全。

（四）工作内容信息和数据共享发送，要坚持字段“最小够用”“最短周期”“最小必要”“用而不存”等原则，设置共享密码加密保护和水印溯源。

**六、外接设备安全**

（一）管理好所用设备的USB等接口的接入安全。不随意使用陌生U盘、移动硬盘等外接设备。

（二）管好所用优盘等外接设备及安全，重要数据要加密存储。

（三）了解熟悉自己（有权）管理使用的打印机（扫描仪）及相关权限设置，对所打印（扫描）的文档及内容负责。

（四）不随意设置使用外接网卡、蓝牙等设备。

**七、网络接入安全**

（一）不私架WIFI，给他人共享网络接入与上网认证账号。不使用免费开放式WIFI。

（二）不私自更改网络（包括私网、专网等）接入与配置。

（三）重要业务传输尽量使用有线网络方式，减少无线传输风险。

（四）不使用未经许可的非法VPN，进行跨业务域、跨区域、跨

境访问与数据传输。

**八、管理规范**

（一）划清专用设备和个人设备的使用边界，网络接入边界，数据传输边界。

（二）管理好所用信息系统的账号及密码，定期更新且不随意与他人共享。

郑州轻工业大学网络安全和信息化领导小组办公室

2022 年 3 月 30 日

郑州轻工业大学网信办　　2022 年 3 月 31 日印发