



西南交通大学

5 月主题党日

学
习
材
料

党委组织部编

2026 年

习近平给四所交通大学全体师生的回信

上海交通大学、西安交通大学、西南交通大学、北京交通大学全体师生：

来信收悉。你们四所高校根脉相连，今年共同迎来建校 130 周年，在此向全体师生员工、广大校友表示祝贺。

希望你们坚持以新时代中国特色社会主义思想为指导，秉持“求实学、务实业”办学宗旨，传承弘扬西迁精神，聚焦国家重大战略需求，加强科技自主创新和人才自主培养，在促进产学研深度融合上实现更多突破，为建设教育强国、科技强国、人才强国作出新贡献。

习近平

2026 年 4 月 7 日

“十五五”时期经济社会发展的指导思想、重大原则和根本保证

<https://www.12371.cn/2026/01/13/VIDE1768297442093987.shtml>

西南交通大学“1896”跨越式发展五年计划

<https://mp.weixin.qq.com/s/sMmFait0a953Pw5WbrGZrQ>

个人电脑（终端）安全管理相关法律法规

一、《中华人民共和国网络安全法》（2025 年修订）

第十三条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第二十九条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第四十八条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，

不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第五十条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

二、《中华人民共和国数据安全法》（2021 年）

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五十万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

三、网络安全技术规范中的有关规定

在《终端计算机通用安全技术规范(GB/T 29240-2024)》中规定：若采用账户口令方式作为操作系统用户身份标识与

鉴别，口令应至少包含数字、小写字母、大写字母、特殊字符 4 类中的 3 类，口令长度至少 8 位。

在《政务计算机终端核心配置规范(GB/T 30278-2024)》中对操作系统入侵防范配置的要求为：1)应禁止移动存储介质中的可执行程序、脚本等自动运行；2)应启用对系统组件数据的自我保护功能；3)应启用登录账户超时锁定功能，并设置唤醒口令；4)应关闭不必要的服务和端口；5)应配置最小安装原则，仅安装必要的系统组件和程序；6)应开启操作系统安全补丁在线自动更新功能。

四、《西南交通大学网络安全管理办法》（西交校信网〔2025〕4号）

（经学校 2025-2026 学年第一学期第 8 次校长办公会审议及第十五届党委第 88 次常委会（扩大）会议审定通过）

第八条 任何单位或个人不得利用校园网危害国家安全、泄露国家秘密，不得侵犯国家、社会、集体利益和个人的合法权益，不得从事违法犯罪活动。

第九条 校园网接入访问实行实名认证制度。校园网用户必须严格遵守国家相关法律法规，对入网终端做好安全防护，不得利用网络制作、复制、查阅和传播有害信息，不得从事危害网络安全的活动，并对上网行为负责。对危害网络安全的用户，信网处有权对其进行断网处理。

第三十二条 二级单位应按照网络安全事件报告与处置流程及时、如实报告和妥善处置网络安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位责任人进

行约谈或通报；对于造成严重后果的，依纪依法追究相关人员的责任。

第三十四条 对于其他违反本管理办法的个人行为，学生由学生工作部、研究生工作部按《西南交通大学学生纪律处分规定》的相关规定进行处理；教职工由人力资源部按学校相关规定进行处理。

西南交通大学师生个人终端安全防护规范

（内部资料，严禁通过 QQ 群、微信群等方式传播）

为维护学校校园网络整体安全，根据国家网络安全相关法律法规和技术规范，依据《西南交通大学网络安全管理办法》（西交校信网〔2025〕4号）有关规定，对学校师生个人电脑、平板、手机等电子设备（以下统称“个人终端”）的安全防护做出如下规范：

1.个人终端接入校园网须使用实名办理的上网账号或交大 ID 进行实名认证，一人一账号，严禁冒用、转借、共享账号。

2.个人终端开机密码、系统账号密码长度应不少于 8 位且至少包含数字、大写字母、小写字母、特殊字符 4 类中的 3 类，不在多平台使用同一密码。个人在学校各业务系统的账号密码不得保存在浏览器中。

3.个人终端须安装并使用正版操作系统及软件。须安装杀毒软件并定期更新病毒库，每月至少进行一次全盘病毒扫描，及时安装操作系统和应用软件的安全补丁。

4.个人终端应关闭非必要的远程桌面、文件共享等服务端口，不随意点击来源不明的邮件附件、短信链接，不安装来历不明的软件，接入公共网络时避免操作敏感业务，不接入陌生、无连接密码的 WIFI 网络。

5.个人终端应定期进行文件备份，重要文件应设置访问密码或加密存储，严防数据泄露。

6.严禁利用个人终端制作、复制、查阅、发布或传播危害国家安全、淫秽色情、暴力恐怖等法律法规所禁止的内容，不得参与网络赌博、刷单、网络诈骗等各类违法活动。

7.禁止使用非涉密个人终端处理、存储、传输涉密信息及学校内部敏感数据，不得通过个人终端拍摄、传播涉密科研项目相关内容。

8.使用生成式 AI 工具时，不得向第三方平台输入涉密信息、个人隐私数据、未公开的科研资料。AI 生成内容用于学术成果时需明确标注使用情况。禁止在保存有重要工作信息、个人信息的终端上部署 Openclaw。

9.因学术研究确需访问境外学术资源的，需向学校信网处申请使用合规通道，严禁在个人终端使用翻墙工具进行“翻墙”。

10.个人终端安全责任由使用者本人自负，因终端管理不善引发信息泄露、网络攻击、病毒传播等安全事件的，使用者需承担相应的责任。