

涉密人员一言一行，不仅关乎个人职业操守，更直接关系到单位保密甚至国家安全。八小时之外，看似离开了单位，实则仍处于保密防线延伸地带，一旦思想上滋生麻痹侥幸心理、放松自我约束，就会模糊公私边界，导致行为失范、底线失守，需要引起涉密人员高度重视。



资料照片

藏在“八小时外”的失泄密隐患

随着生活场景不断拓展，涉密人员面临的失泄密风险愈发隐蔽多元，一些日常交流、社交娱乐等场景下的失泄密隐患极易被忽视。

闲谈失度。亲友相聚、邻里闲聊等社交场景是泄密的高发区。宽松氛围中，若未绷紧保密弦，易出现炫耀式分享、随意应答泄露涉密信息等问题。例如，某涉密单位工作人员田某，在赴同事家做客闲聊时，随意谈论自己参与的某重大涉密项目进展情况，相关内容被他人听到并发布至网络，造成了国家秘密泄露。最终，田某被依法追究责任。

下班携密。部分涉密人员心存侥幸，违规将涉密文件、涉密载体带回家中。例如，某涉密单位工作人员张某，将3份涉密文件违规带回家中，并允许好友李某浏览，殊不知李某早已被境外间谍情报机关策反。李某趁机偷拍文件并传输至境外，造成了国家秘密泄露。最

终，张某、李某均被依法追究责任。

网络传密。网络沟通便捷，但暗藏多重失泄密风险。例如，某机关单位工作人员刘某，节日值班期间，为图一时之便将涉密电报内容拍摄并发送至工作群，后经多次传播扩散，造成失泄密，相关人员被依法追究责任。

“八小时外”安全保密手册

涉密人员需牢记保密工作不是“八小时内”的专属命题，而是贯穿涉密人员工作与生活的“终身课题”，需将保密意识融入生活点滴。

闲聊不“漏嘴”。不向亲友、同学、朋友闲聊透露任何涉密敏感信息，不在公共场所谈论敏感工作内容，不炫耀涉密工作身份、业务细节，坚决杜绝酒后失言、闲谈泄密。

载体不“乱跑”。下班前将涉密文件资料锁入保密柜，关闭涉密设备。不私自将涉密文件、U盘、笔记本电脑等涉密载体带出办公场

下班能『下线』吗？

关键处不能“掉链子”

资源的开发、技术的进步、数据的流动，无不深嵌于产业链供应链这张无形的网络中。近年来，境外间谍情报机关针对我国产业链供应链的渗透、破坏与窃密行为日益隐蔽化、专业化、体系化，对我国经济安全、科技安全与数据安全构成严重威胁。

产业链供应链上谍影重重

半导体技术的“内鬼泄密”。核心技术是产业链的“命门”，也是不法分子觊觎的重点目标。公开案例显示，国内某半导体企业前工程师张某，离职后违反保密义务，向境外组织非法提供核心生产工艺等商业秘密。核心技术的工艺参数、设计图纸外流，不仅会使企业数年研发投入付诸东流，还可能削弱我国在全球半导体产业链中的话语权。最终，张某受到了法律的严惩。

数据资源的“寄生窃取”。公开案例显示，国内某公司通过技术手段寄生在某电商平台系统内，日均盗取超百万条经营数据，非法牟利数千万元。这种行为并非简单的商业侵权，而是有组织、产业化的数据窃取，企图掏空平台核心商业资源、破坏健康的数据生态。最终，相关涉案人员均受到法律的严惩。

关键矿产信息的“机密套取”。稀土是关乎高端制造、国防军工的战略资源，境外长期高度关注相关收储情况，千方百计获取我内部数据。公开案例显示，境外某有色金属公司通过其中方雇员叶某某，以金钱利诱国内某稀土公司副总经理成某。成某为谋私利违反规定，将其掌握的我国稀土收储品类、数量、价格等7项机密级国家秘密非法提供给境外。最终，叶某某、成某均受到法律的严惩。

产业链供应链“防护对策”

面对严峻复杂的产业链供应链安全形势，单一环节的修补或被动响应已无法应对，应构建科学高效的防护体系。

严格硬件管理。严控芯片、服务器、工控设备等关键硬件准入，实施供应商安全审查与溯源管理；全面排查禁用存在安全风险的设备，建立供应商准入与动态管理机制，防范别有用心之人在硬件中植入窃密装置、预置间谍固件。

严格软件管理。强化软件、开源组件、云服务安全管控，开展代码审计与漏洞排查，防范恶意代码、后门植入。严格涉密敏感数据、核心技术、商业秘密全生命周期管理，执行最小权限、端到端加密、跨境数据安全评估，严防数据窃取、篡改或非法出境。

严格人员管理。落实反间谍安全防范责任，对关键岗位人员开展背景审查与保密培训，严禁在非涉密设备上处理涉密信息。规范涉外合作、外包、外协管理，防范境外间谍情报机关通过拉拢策反、利益诱惑等方式窃取涉密敏感信息。

所。不私存、不翻拍、不私印涉密文件资料，废弃涉密文件资料应按规定销毁，不随意丢弃或当作废品售卖。

上网不“踩雷”。不在社交媒体上发布、转发涉密图文、内部工作信息，不用私人手机、私人邮箱存储传输涉密敏感数据，守住网络防线。

国家安全机关提示

国家安全无小事，保密责任无盲区。“八小时外”不是保密纪律的“法外之地”，更不是国家安全的“空白地带”。涉密人员必须摒弃侥幸心理，严守工作纪律，切实落实保密责任，守护好国家秘密。如发现可能危害国家安全的线索，请及时通过12339国家安全机关举报受理电话、网络举报受理平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

口无遮拦，害人害己

慎言，是中华民族千年传承的文化智慧，更是涉密人员应时刻铭记于心的安全守则。近年来，境外势力始终将我国涉密群体作为重点渗透目标，以个别涉密人员保密意识淡薄、口无遮拦、言语失度为突破口，伺机套取涉密信息，危害我国家安全。

古人对慎言的重视由来已久，将“慎言”与安身立命相关联，久而久之演化成了贤能之人的处世哲学。《周易》中“言行，君子之枢机……可不慎乎”，指出言行是事关成败的关键。《论语》中“敏于

事而慎于言”，成为后来历代官箴的核心表述。《道德经》中“知者不言，言者不知”，强调真正掌握核心信息的人，往往保持沉默，是对“言不尽意”的一种清醒认知。《韩非子》中“事以密成，语以泄败”，道尽了保守秘密对事业成败的决定性影响，堪称最凝练的“保密条例”。儒家、道家、法家虽思想路径不同，但在“慎言”这件事上，罕见地指向了相同的结论。胜负之分，守密与否是关键变量。越王勾践卧薪尝胆二十年，复国大计深藏心底，谋划之事从不外泄，忍

辱负重，反败为胜。秦孝公与商鞅密谋新法数月，变法内容严格保密，公布后让反对者措手不及，为变法顺利推行赢得了宝贵时间。保密是成事的铠甲，而泄密则是败局的诱因。明朝萨尔浒之战，明将杨镐在出兵前竟向后金发出“告知书”，公示进军的时间与路线，美其名曰“示威”，实则将全部作战部署拱手相告，终致军事行动失败。这些历史故事，清晰地勾勒出古人保密智慧的内涵：守密者成事，泄密者败身。

(均转自国家安全部微信公众号)