

保密宣传教育

保卫部应急救援大队
2026年3月

01

保密宣传教育的重要意义



维护国家安全利益



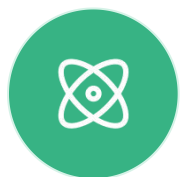
防范军事机密泄露

某国曾因军工单位人员违规携带涉密文件出境，导致新型武器参数泄露，危害国防安全，此类事件需通过保密教育杜绝。



保障经济信息安全

2023年某企业核心技术资料被境外间谍窃取，造成超10亿元经济损失，保密教育可提升员工信息防护意识。



维护社会稳定秩序

某地发生涉密工程信息泄露事件，引发民众恐慌，保密宣传能增强公民对敏感信息的保护责任感。



防范信息泄露风险

强化办公设备管理

某企业员工将涉密文件拷贝至私人U盘带回家处理，导致文件被病毒窃取，造成核心技术泄露，此类案例占信息泄露事件的38%。

规范网络使用行为

2023年某科研机构因工作人员在公共WiFi环境下传输涉密数据，被黑客拦截，导致重要研究成果提前泄露，造成重大损失。

加强纸质文件管控

某政府部门工作人员将废弃涉密文件随意丢弃在垃圾桶，被不法分子捡拾后倒卖，引发敏感信息外泄事件，涉事人员被严肃追责。

强化全民保密意识

开展多场景宣传教育

社区通过宣传栏、讲座等形式，如某街道举办“保密知识进万家”活动，向居民普及保密法规和日常防范技巧。



企业组织专项培训

某科技公司定期开展保密培训，模拟文件泄露场景，让员工掌握涉密信息的正确处理流程和应急措施。

02

保密宣传教育基础知识





保密工作基本概念

保密定义与范围

保密是指保护国家、企业或个人的涉密信息不被泄露，如军事机密、商业数据等，需明确界定保密对象和密级。

保密工作原则

遵循“最小化”原则，如某科技公司仅允许核心研发人员接触核心技术资料，严格控制信息传播范围。

保密法律依据

《中华人民共和国保守国家秘密法》规定，泄露国家秘密将承担法律责任，如某单位员工因过失泄露机密被处罚。

保密相关法律法规



《中华人民共和国保守国家秘密法》

该法明确国家秘密范围与密级，2010年修订后加大对泄密行为惩处，如某科研人员泄露机密被判有期徒刑。

《中华人民共和国刑法》相关条款

刑法第398条规定故意泄露国家秘密罪，最高可判七年，某国企员工因向境外传递秘密文件获刑。

行业保密规章

金融行业有《银行业金融机构保密管理办法》，要求对客户信息加密存储，某银行因泄露客户数据被处罚。

涉密信息分类标准

国家秘密分类

按《中华人民共和国保守国家秘密法》，国家秘密分绝密、机密、秘密三级，如军事部署文件多为绝密级。

工作秘密界定

某央企规定，未公开的客户信息、项目进度等属工作秘密，需通过内部权限系统管理，严禁外泄。

商业秘密保护

华为公司将5G核心算法列为商业秘密，与员工签订保密协议，违者需承担高额违约金和法律责任。



03

当前保密工作整体形势



信息化带来的新挑战



数据传输安全风险

某科研机构通过邮件传输涉密数据时，因未加密被黑客截获，导致核心技术资料泄露，造成重大损失。



移动办公泄密隐患

员工使用个人手机处理工作，在公共WiFi环境下接收涉密文件，被恶意软件窃取，引发泄密事件。



社交媒体信息扩散

某企业员工在微信群误发内部保密方案，信息迅速扩散至外部，竞争对手据此调整策略，企业遭受经济损失。

常见泄密隐患分析



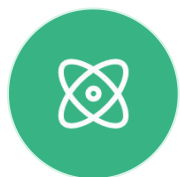
社交平台信息泄露

某企业员工在微信朋友圈发布含项目数据的工作照，被竞争对手获取，导致核心技术方案提前曝光，造成百万级经济损失。



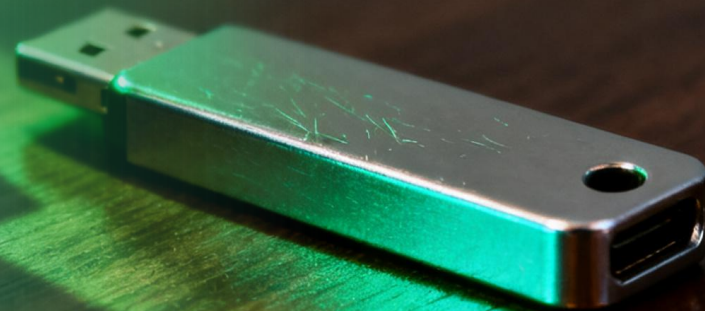
办公设备使用不当

某单位人员将涉密U盘接入个人电脑，被病毒窃取文件，其中包含未公开的招投标信息，被不法分子用于围标串标。



纸质文件管理疏漏

某研究所档案室人员未及时销毁废弃涉密图纸，被保洁人员当作废纸变卖，图纸涉及新型材料配方，造成技术秘密外泄。



04

保密宣传教育重点对象



党政机关涉密工作人员



涉密文件管理规范

需严格执行"专人保管、专柜存放"制度，如某省办公厅曾发生涉密U盘违规带出办公区导致泄密事件，被通报批评。



涉密会议保密要求

参加涉及国家秘密的会议需关闭手机信号，某部委重要会议因未落实此规定，导致会议内容被窃听泄露。



网络保密操作准则

严禁使用非涉密计算机处理涉密信息，某市政府工作人员用私人邮箱传输涉密文件，被依法追究刑事责任。

企业核心涉密岗位人员



技术研发岗位保密要点

某科技公司工程师因在咖啡厅讨论芯片设计方案，导致核心代码被竞争对手窃听，造成超5000万元经济损失。



财务数据管理规范

某上市公司财务总监通过微信传输未加密的季度财报，被黑客截获并提前泄露，引发股价异常波动。



高管决策信息保护

某国企总经理在私人邮件中谈及并购计划，被境外情报机构获取，导致项目谈判陷入被动局面。

互联网平台从业人员

数据处理环节保密规范

某电商平台曾因员工违规导出用户消费数据获利被查处，需严格执行数据脱敏与权限分级管理，禁止私存敏感信息。

用户隐私信息保护要点

社交平台需加强私信内容审核，2023年某短视频平台因员工泄露明星隐私聊天记录引发法律纠纷，凸显监管漏洞。

平台系统安全操作要求

某云服务企业发生运维人员误删客户加密文件事件，需落实操作日志留痕与双人复核机制，定期开展安全演练。



高校科研工作人员

涉密项目研发环节管理

某高校在芯片研发中，要求工作人员在专用设备上处理数据，纸质资料需存入密码柜，严禁私自带出实验室。

对外学术交流保密规范

参加国际学术会议前，需经学校保密办审核PPT内容，2023年某教授因未审核泄露技术参数被通报批评。

科研成果转化保密要求

与企业合作时，需签订保密协议，某研究所曾因未明确保密期限导致专利技术提前公开。

社会普通公众



日常信息保护意识培养

生活中接收快递时，应去除面单上的姓名、电话等信息再丢弃，避免被不法分子利用，2023年某快递信息泄露案涉5万余人。

社交媒体信息发布规范

在朋友圈晒照片时，勿泄露军事基地、政府机关等敏感区域背景，曾有人因晒军营定位被依法处理。

网络信息辨别能力提升

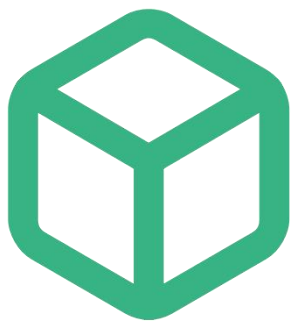
收到不明链接或文件时，如“中奖通知”等，切勿随意点击，2024年某钓鱼链接导致2000余人信息被盗。

05

保密宣传教育的核心内容



涉密文件管理规范



文件定密与标识

某科研单位对涉密图纸采用"绝密-★-2025"格式标识，明确密级、保密期限，粘贴于文件首页左上角。



流转与借阅登记

某国企规定涉密文件借阅需经部门负责人签字，使用"涉密文件借阅登记表"记录借阅人、用途及归还时间。



存储与销毁要求

涉密U盘需单独存放于密码柜，销毁时使用专业碎纸机粉碎，某机关曾因未按此操作导致文件泄露被通报。

网络信息保密要求

01

涉密信息传输规范

严禁使用微信、QQ等非涉密即时通讯工具传输工作秘密，某单位曾因员工用微信发送涉密文件被通报批评。

02

办公设备使用管理

工作电脑禁止连接外部网络和私人存储设备，某企业员工插入私人U盘导致核心数据泄露，造成重大损失。

03

网络行为安全准则

不得在非涉密网络发布敏感信息，某科研人员在论坛讨论工作进展时泄露项目信息，被依法追责。

对外交往保密守则

涉外会议保密管理

召开涉外技术交流会时，需提前报备保密部门，会场禁用无线麦克风，涉密资料会后由专人回收销毁。

境外通讯安全规范

在境外使用加密通讯设备，禁止通过非授权邮箱传输工作文件，某企业曾因境外邮件泄密遭重大损失。

涉外礼品往来准则

对外赠送礼品需经审批，不得包含涉密信息载体，如某单位曾因赠送含内部数据的纪念品被通报。

泄密事件处置流程



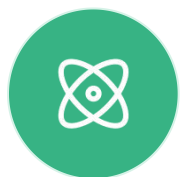
事件初步研判与上报

发现疑似泄密后，立即核查信息涉及范围，如某企业员工误发涉密文件至外部群，需1小时内上报保密管理部门。



证据固定与现场控制

封存涉事设备（如电脑、U盘），禁止无关人员接触，参考某科研单位泄密案中对服务器日志的即时备份措施。



应急响应与止损措施

启动应急预案，通知相关单位屏蔽信息扩散，如某政府部门泄密后联系平台删除敏感帖文，24小时内完成初步处置。



06

保密宣传教育的开展方式



线下专题培训宣讲

保密法规政策解读

某军工企业开展《保密法》专题培训，结合“某研究所泄密案”案例，详解涉密载体管理要求，参训人员达200余人。

涉密场景模拟演练

组织学员进行办公室文件分类、会议保密场景模拟，设置“假意咨询涉密信息”等突发情境，提升应急处置能力。

典型泄密案例剖析

通过“某科技公司核心数据泄露事件”，分析邮件传输、U盘使用等环节漏洞，强调“涉密不上网”基本原则。



线上新媒体科普推广



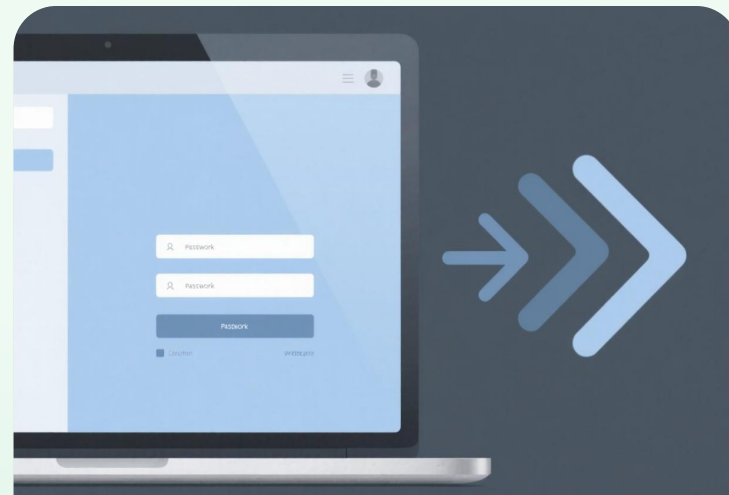
短视频平台系列科普

某央企在抖音推出“保密小贴士”系列，用情景剧演示文件加密操作，单条视频播放量超500万，互动量达30万+。



微信公众号专题推送

国家保密局公众号定期发布《典型泄密案例警示》，图文结合剖析某科技公司员工邮箱泄密事件，订阅用户超800万。



H5互动小游戏传播

某省保密局开发“保密卫士”H5游戏，设置密码破解、文件传输等关卡，上线3天参与人数突破10万，分享率达45%。



涉密场景实战演练

办公设备泄密模拟

模拟员工将涉密文件误发至外部邮箱场景，某科技公司曾因此泄露核心代码，演练中设置邮件拦截与应急上报环节。

会议信息泄露处置

模拟涉密会议中手机录音导致信息外泄，参考某军工单位案例，演练现场设备管控、信息溯源及违规人员处理流程。

物理载体丢失应对

模拟涉密U盘遗失场景，参照某政府部门处置经验，演练定位追踪、数据擦除及内部通报等应急响应步骤。

主题警示案例展览



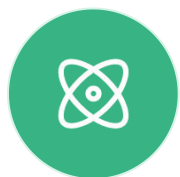
典型泄密事件图文展

展示如某科研单位员工因违规传输机密文件被追责案例，配文件传输记录截图及法律文书照片，直观呈现后果。



行业领域专题案例展

聚焦军工领域，如某军工企业图纸外泄导致核心技术泄露，通过时间线还原泄密过程及造成的1.2亿元经济损失。



新兴媒介泄密案例展

呈现某公务员在微信工作群发送涉密信息事件，展示聊天记录截图，说明此类行为违反《保密法》第26条规定。

警示传输

RAG 55.35 (monitored)

法律书

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

1913.10.10/10

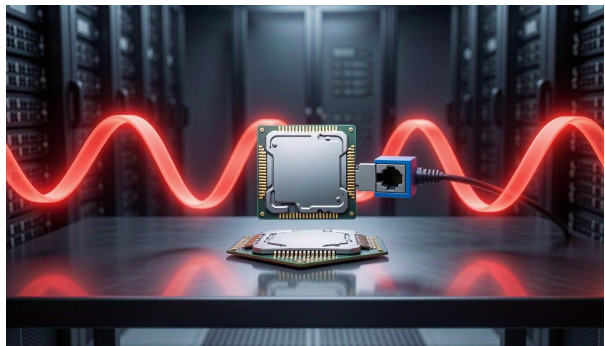
密密密密后果

07

保密宣传教育常见问题

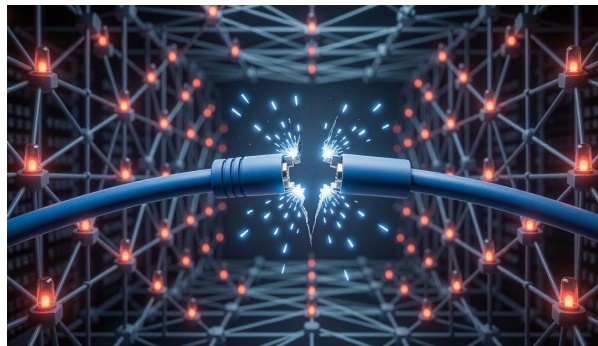


保密意识淡薄问题



日常文件随意处置

某科研单位员工将含机密数据的U盘随意插在公共电脑，被外部人员拷贝，导致核心技术泄露，造成重大损失。



网络传输不设防

某公司职员通过微信发送保密合同给客户，未加密且被无关人员看到，引发商业信息泄露纠纷。



口头泄密风险

某涉密会议结束后，参会人员在餐厅闲聊时提及会议内容，被竞争对手人员窃听，导致项目计划提前暴露。

保密技能不足问题



文件加密操作不规范

某企业员工未设置复杂密码，仅用生日作为文档密码，导致商业合同被竞争对手轻易破解，造成重大经济损失。

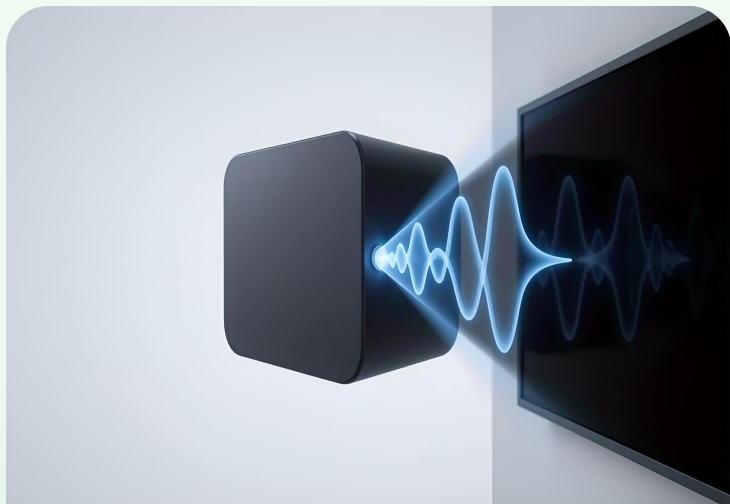


涉密信息传输方式不当

某单位人员通过普通微信发送涉密文件，被网络爬虫抓取，涉及国家机密的项目数据泄露，相关责任人被严肃处理。



宣传形式僵化问题



单向灌输式宣讲普遍

某单位保密培训仅播放30分钟旧版警示教育片，员工低头玩手机，互动提问环节无人回应，信息接收率不足40%。



宣传载体陈旧单一

某国企保密宣传仍以张贴纸质通知为主，全年仅更新2次内容，年轻员工表示“从未主动关注过公告栏信息”。



缺乏分层分类教育

某科研院所对新入职实习生与核心技术人员采用相同保密课件，实习生觉得太深奥，老员工认为内容重复枯燥。

考核评估缺失问题

评估标准模糊

某央企保密教育仅以“签到率”为考核指标，未设定涉密信息泄露风险模拟测试等量化标准，导致员工保密意识薄弱。

结果应用不足

某事业单位保密考核后未将结果与晋升挂钩，员工参与培训积极性低，出现连续三年考核成绩无改善的情况。

反馈机制缺失

某互联网公司保密培训后未收集员工对教育内容的反馈，导致涉密文件管理模块讲解模糊的问题长期未被发现。



08

优化保密宣传教育建议



创新宣传教育形式

开发互动式保密知识游戏

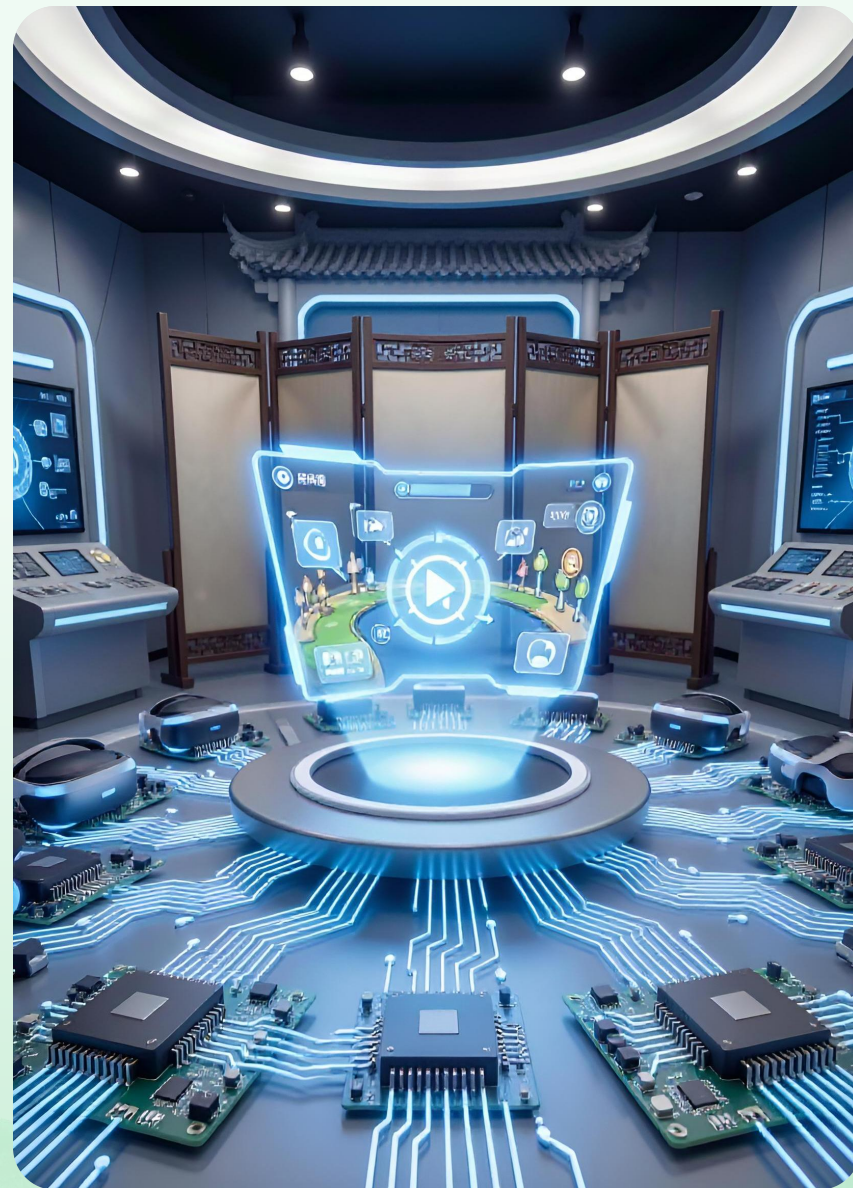
某军工企业开发“保密防线”线上游戏，员工通过破解虚拟泄密场景积累积分兑换奖励，参与率提升40%。

制作沉浸式VR保密实训课程

某政府部门搭建VR保密实训系统，模拟会议室文件泄露、U盘使用不当等场景，让学员在虚拟环境中实操应对。

开展保密主题情景剧巡演

某央企组织员工编排《保密红线》情景剧，通过办公室泄密、网络传输风险等真实案例，在各分公司巡演20余场。



完善长效工作机制



建立保密责任制

某科技公司明确各部门负责人
为保密第一责任人，签订责任书，
将保密工作纳入绩效考核，
季度检查落实情况。



制定年度保密计划

某机关单位每年初制定保密教
育计划，明确每月培训主题，
如“涉密文件管理”“网络保
密”等，确保教育常态化。



完善监督检查机制

某国企设立保密监督岗，每周
抽查涉密电脑使用情况，发现
违规外联行为立即通报，全年
整改隐患30余起。

强化宣传成效考核



建立量化评估指标体系

参考某央企做法，设置保密知识测试通过率（目标 $\geq 95\%$ ）、宣传活动参与率（要求 $\geq 80\%$ ）等可量化指标，定期统计分析。



开展多维度考核方式

结合季度保密检查，通过现场提问员工保密要点、抽查涉密文件管理记录等方式，评估宣传教育实际效果。



实施考核结果应用机制

将考核结果与部门绩效挂钩，某单位对考核优秀部门给予年度评优加分，对未达标部门要求限期整改并重新培训。



THE END
谢谢

