提升安全保密意识，快来看看这些文件泄密的案例

4 月 15 日是全民国家安全教育日，是为了增强全民国家安全意识，维护国家安全而设立的节日。下面两篇“保密观”关于文件保密的文章推荐给大家，共同提升安全保密意识。

文章一：案例告诉你，文件经手，当心泄密！

机关单位日常工作中，涉密文件保密管理可谓“老生常谈”。但我们往往容易忽视，涉密文件保密管理并非个体所能独立完成，在整个文件运转过程中，存在多名经手人，一人发生疏忽，则整个安全屏障即被打破。

1.密件″入手″环节

密件“入手”环节的失泄密隐患，可以表现为私自委托不属于涉密文件知悉范围人员去收取密件导致泄密；收取密件时心存旁骛，忙于其他工作，如放假、下班等，对密件随手处置泄密等。

2018 年 4 月，某市机要部门通知原市检验检疫局服务中心文件专管员周某紧急去取一套涉密文件，但周某忙于手头其他工作，难以走开。周某认为，取文件而已，反正谁去都一样，便未向分管领导报告，私自委托新入职尚未接受保密培训的驾驶员赵某帮其代领。赵某领取文件后，出于炫耀心理，在返回途中于车内私自用手机将其中 3

份机密级文件首页进行拍照，并实时在微信群“相亲相爱一家人”中发布，造成泄密。

2.密件“倒手”环节

从对象上看，密件“倒手”可分为“倒”给别人和“倒”给自己。可以表现为对自己传阅的文件不认真审阅，未能及时发现文件密级、保密期限、发放范围等核心要素，导致其通过互联网违规传递；贪图便利，明知不符合保密规定，仍然违规复印、扫描、摘录、汇编；为参考学习，私自拍照上传至互联网计算机中等。

2019 年 2 月，夜已深，某市政府业务部门工作人员望某在办公室加班整理文件时，发现一份传阅的机密级会议纪要对业务工作具有很强的指导和借鉴意义，便产生了全文留存以便学习参考的想法。望某知道，按规定若想留存密件需履行报批手续并使用涉密复印机进行复印，但涉密复印机由单位文印室统一管理，已经锁门。此时的望某已十分疲惫，实在不想第二天再“折腾”了，便关了办公室的门，偷偷用手机对该文件进行了拍照，并使用手机软件对拍摄的涉密文件进行文字识别后发送至自己的办公用互联网计算机上，转化为 Word 文档进行编辑。目前，此案正在进一步查处中。

3.密件“出手”环节

密件“出手”环节的失泄密风险，可以表现为该移交不移交，私自留存备份，后续或自用、或贩卖，进而造成泄密或泄密隐患；“一

揽子”移交，不按规定将密件、非密件分类移交，不详细告知接手人注意事项，甚至“单方”移交，不与接手人发生接触，自顾自办理完毕等。

2016 年 12 月，有关部门在工作中发现，某参公事业单位研究室主任蒋某在连接互联网的计算机中违规存储、处理大量涉密材料，其中绝密级国家秘密 1 份、机密级国家秘密 12 份、秘密级国家秘密 59 份，涉及国家秘密数量多、时间跨度大。经查，蒋某为转业干部，曾辗转部队多个部门工作，业务经验丰富。该计算机中存储、处理的涉密文件为其 2008 年转业时私自留存。据蒋某称，其日常有收集资料的习惯，认为这种做法对新岗位熟悉工作帮助很大。

2015 年 5 月，有关部门在工作中发现，某县县委宣传部一台连接互联网计算机违规存储、处理国家秘密信息。经查，该计算机使用人为工作人员易某。同年 3 月，工作人员陈某在交接工作过程中，贪图省事，未按规定履行工作交接手续，在未告知相关领导及同事的情况下，私自将移动硬盘中的部分涉密文件与非涉密文件一并拷贝至易某使用的非涉密计算机上（内含 3 份秘密级文件）。易某接手工作后，工作量激增，未能及时对陈某交接的电子文件一一过目，导致对该情况未能及时发现并作出正确处理。

案情分析

与故意卖密牟利、对外提供等极端恶劣情形不同，机关工作中涉密文件的丢失、泄露多是过失或对相关后果预料不足所致，因此各级领导干部首先要摆正自己的保密态度，树正“三观”：

一是树正“利益观”。将国家利益时刻放在首位，严禁将密件作为实现个人目的的工具和手段，绝不能将个人利益凌驾于国家秘密安全之上。

二是树正“业绩观”。不能因时间紧、任务重就放松了工作标准和要求，坚决杜绝各种图便利、走捷径的行为。

三是树正“大局观”。真正确立“文件保密一盘棋”的思想，从自身做起，严格遵守保密纪律。

而对于各单位保密部门来说，还必须加强相关管理，强化制度落实：

一是合理配置人力资源和办公资源，在涉及核心、紧急、重大工作且文件经手数量巨大时，抽调专人帮助工作或灵活机动设置岗位替补，及时配备涉密设备，为便利工作创造条件。

二是组织签订专项保密承诺书，明晰工作标准和要求，让干部职工工作有参考、有抓手。

三是组织定期检查，及时发现隐患，认真整改补漏洞。

文章二：保密！涉密会议文件材料应当这样管理

涉密会议文件材料管理是一个普遍性的问题。在各机关、单位，通过召开会议传达学习相关文件材料，是贯彻落实党和国家方针政策、法令、决议以及上级指示的重要途径。而当会议议题、内容或者文件涉及国家秘密时，对文件材料的管理尤其需要提高警惕、严防泄密。

然而，在实际工作中，涉密会议文件材料管理不当的问题时有发生。不仅有涉密会议组织者图省事让参会人员自带涉密文件，还有参会人员私自留存涉密会议文件；既涉及涉密会议组织者与参会单位会议文件收发衔接的问题，还有参会单位对参会人员带回的会议文件查收和监督管理的问题。

案例 1:2005 年，某涉密单位干部孙某参加涉密会议，会议要求涉密会议材料“会后收回”。孙某未按要求交回涉密会议材料，将涉密会议材料带入宾馆，存放在更衣柜中。孙某外出时，涉密会议材料和个人财物被盗，经多方查找未果。事件发生后，孙某受到党纪政纪严肃处理。

案例 2：2013 年 3 月，某部委工作人员娄某丢失 1 份机密级文件。经查，娄某外出参加会议返程途中，不慎将涉密文件遗失在公交车上。发现情况后，娄某立即向单位报告，并通过积极联系公交公司、向公安部门报案等方式进行查找，但未能找到。经评估，文件内容已在有

关报告中对外公开，文件丢失不会带来实质性损害，有关部门给予娄某行政警告处分。

案例 3：某开发区信访办主任刘某在参加完市涉密会议后，将 1 份机密级会议文件带回单位，不仅未按规定及时交保密室查收，而且在文件使用后疏于保管，随意放置在办公桌上，被一上访人员趁办公室无人拿走，在开发区服务中心复印后将原件送回，并将复印件交给一名个体职业者通过互联网向境外发送。有关部门发现后，随即对两人实施了刑事拘留。刘某也因此受到行政警告处分。

个人私自留存涉密会议文件的现象屡禁不止，究其原因，一方面是参会人员的保密意识淡漠，另一方面是涉密会议组织者的保密工作不到位，没有做好会议文件材料的管理。

涉密文件的管理，关系到国家安全和利益，各单位应当充分认识到涉密会议活动的严肃性以及保护涉密会议文件的重要性，采取切实有效措施，加强管理，并提高工作人员的责任心和保密意识。

保密法第三十一条规定：举办会议或者其他活动涉及国家秘密的，主办单位应当采取保密措施，并对参加人员进行保密教育，提出具体保密要求。

保密法实施条例第二十七条第三款规定：举办会议涉及国家秘密的，主办单位应当按照国家保密规定管理国家秘密载体。

1、会议布好“保密网”

有关机关单位应当根据“谁主办，谁负责”的原则进行管理，明确涉密会议管理职责。主办单位应当制订保密工作方案，根据会议主题、内容或文件、资料涉及国家秘密的最高密级，及时确定会议的密级，对参加人员提出保密要求，开展保密常识和保密防范知识教育，提出具体保密管理要求，并明确专人负责督促落实。

承办单位要按照主办单位要求，提供安全保密的环境、设施和设备，并对工作人员进行保密教育，明确工作人员的保密责任，要求其做好保密工作。

保密行政管理部门应当对重大涉密会议的保密工作进行监督和指导，并提供必要的安全保密技术服务保障。

2、管理念好“保密诀”

对涉密会议文件的管理，应当严格按照国家秘密载体保密管理有关规定执行。涉密会议组织者会前应加强办公设备和场所保密技术检查和防护，对会议驻地采取保密管理措施。会议期间应做好会场保密保障和会场外可疑无线信号监测，跟踪会议文件、资料发放情况，对会议驻地进行保密巡查。会后应督促做好文件、资料的清退、回收、销毁和保密设备回收等工作，落实保密管理措施。

涉密会议特别注明要“会后收回”的或由会议代表带回单位交保密室保管的文件资料，参加人员应在会议结束时主动交回会议管理人员或退回单位保密室并办理退回签收手续，不得私自留存涉密文件资

料，不得擅自记录、录音、摄像、拍照和摘抄，不得擅自复印涉密文件、资料等。

3、报道绷紧“保密弦”

近年来，由于信息公开保密审查不严导致涉密文件泄密的案例时有发生。对此有关机关单位还要在会议后严格信息上网审查，控制信息来源、落实审查制度、规范审查程序，从源头上防止涉密会议文件材料泄密事件的发生。

涉密会议有关方面接受采访或者公开报道应当经过批准，对是否涉密界定不清的，应当逐级报有权确定该事项密级的上级机关或保密部门审查确定，严防在宣传报道中造成失泄密事件。