保密工作文萃

BAO MI GONG ZUO WEN CUI

2017年7月
总第4期
4

中共山西师范大学保密委员会办公室　整理

案例警示：

某单位干部张某随意将存有涉密文件、资料的移动硬盘交由同事王某使用。王某擅自将该硬盘中的涉密文件、资料拷贝到自己的计算机和移动硬盘中，后因其计算机接入互联网，造成严重泄密。张某、王某因此受到开除党籍、开除公职处分。

复制涉密载体必知的保密要求！

1　复制本机关、本单位产生的机密级、秘密级涉密载体，应当经主管领导批准；复制其他机关、单位产生的涉密载体，应当经制发机关、单位批准，未经批准不得复制。

2　复制涉密载体不得改变其密级、保密期限或删除国家秘密标志。

3　复制涉密载体应当履行登记手续，加盖复制机关、单位的戳记。复制件要采取与原件相同的保密措施。

4复制涉密载体应尽量在本机关、本单位内部进行，需要送外单位复制的，应当委托具有涉密载体印刷资质的单位复制。

5严禁复制绝密级涉密载体。确因工作需要复制的，属于本机关、本单位产生的，必须经本机关、本单位主要领导批准；非本机关、本单位产生的，须经原密级确定机关、单位或者其上级机关批准。

（选自《保密科学技术》）

CONTENTS 目录

保密知识简明读本

什么是国家秘密？

国家秘密是指关系国家安全和利益，依照法定程序确定，在一年时间内只限一定范围的人员知悉的事项。

国家秘密必须具备以下三个要素：

1、“关系国家安全和利益”，是构成国家秘密的实质要素，是指某一事项一旦泄露会使国家安全和利益受到损害。这是国家秘密的本质属性。

2、“依照法定程序确定”，是构成国家秘密的程序要素，是指根据定密权限，按照国家秘密及其密级具体范围的规定，确定国家秘密的密级、保密期限、知悉范围，并做出国家秘密标志，做到权限法定、依据法定、内容法定、标志法定。一项关系国家安全和利益的事项，只有依照法定程序确定为国家秘密，才具有国家秘密的法律地位，受到法律保护。

3、“在一定时间内只限一定范围的人员知悉”，是构成国家秘密的时空要素，是指关系国家安全和利益的秘密事项，在依照法定程序确定为国家秘密后，应当限定在一定的时间和空间范围内，即在保密期限内，不能超出限定的知悉范围。

【知识链接】

各国关于国家秘密概念的提法不完全相同，大多数国家称之为国家秘密，有的国家称为“政府秘密”。

国家秘密与工作秘密和商业秘密不同。工作秘密，是指各级党政机关在其公务活动和内部管理中产生的不属于国家秘密而又不宜对外公开的事项。商业秘密，是指不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。

国家秘密的基本范围是什么？

根据保密法规定，下列涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密：

（1）国家事务重大决策中的秘密事项；

（2）国防建设和武装力量活动中的秘密事项；

（3）外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项；

（4）国民经济和社会发展中的秘密事项；

（5）科学技术中的秘密事项；

（6）维护国家安全活动和追查刑事犯罪中的秘密事项；

（7）经国家保密行政管理部门确定的其他秘密事项。

政党的秘密事项中符合上述规定的，属于国家秘密。

知识链接

以列举方式规定国家秘密基本范围，是许多国家立法的通例。有的国家规定，国家秘密包括：军事计划、武器系统或军事行动；外国政府信息；情报活动(包括特殊行动)，情报源或方法，或者密码；外交关系或本国的外交活动，包括秘密渠道；与国家安全（包括打击跨国恐怖活动）有关的科学、技术或经济事项；保护核材料与核设施的本国政府项目；与国家安全（包括打击跨国恐怖活动)有关的系统、装置、基础设施、项目、方案或者保护工作的缺陷或效能；大规模杀伤性武器。

有的国家规定，涉及国家安全和情报的信息、国防信息、国际关系信息、刑事调查信息属于涉密信息而受到保护。

还有的国家规定，国家秘密范围包括：军事情报；经济、科技信息；外交和对外经济领域的信息；情报、反间谍和侦缉领域的信息等。

国家秘密分哪几个等级？

国家秘密的密级，是按照国家秘密事项与国家安全和利益的关联程度，以泄露后可能造成的损害程度为标准，对国家秘密作出的等级划分。

国家秘密的密级分为绝密、机密、秘密三级。

绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害；

机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害；

秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害。

为准确界定国家秘密，使“关系国家安全和利益”的事项具体化、标准化，更便于操作，国家保密行政管理部门将有关“关系国家安全和利益”事项泄露会造成的后果分类归纳为7大类，共40个小类，统称“关系国家安全和利益的定义群”，作为制定或调整保密事项范围的依据。7大类分别是：危害国家防御能力；危害国家政权的巩固和使国家机关依法行使职权失去保障；影响国家统一、民族团结和社会安定；妨碍国家外交、外事活动正常进行；损害国家经济利益和科技优势；妨碍国家重要保卫对象和保卫目标安全；妨碍国家秘密情报的获取和削弱保密措施有效性。

知识链接

有的国家将国家秘密的密级分为最高机密、机密、秘密、限制级信息和保护级信息。最高机密是指能够加剧国际紧张局势；能够严重破坏与友邦国家的关系；对生命安全有直接影响，或对公共秩序、个人安全和自由有严重影响；对本国及盟国国家安全能够造成重大损失，或对国家安全和情报工作的开展有重要的影响；能够导致对国家金融和商业利益产生实质性破坏的信息。

除了上述五种密级，相关人还可以追加其他保密条件来保障特殊信息的适当处理。这些追加的保密条件可以是：只可现场阅读，口述传递，代码传递或隔离处理等。在很多情况下，这些追加的保密条件只适用于高度敏感的信息，通常是秘密级以上。

国家秘密确定依据是什么？

国家秘密及其密级的具体范围，简称保密事项范围，是确定、变更和解除国家秘密事项的具体标准和依据。

保密事项范围由国家保密行政管理部门分别会同外交、公安、国家安全和其他中央有关机关规定。军事方面的国家秘密及其密级的具体范围，由中央军事委员会规定。

保密事项范围规定不同行业、领域的国家秘密事项和密级，是对国家秘密基本范围的具体化，是机关、单位确定国家秘密的重要依据，由国家秘密范围和国家秘密目录两部分构成。保密事项范围应当根据情况变化及时调整。

知识链接

目前国家保密行政管理部门会同中央有关机关已制定了94个保密事项范围。

许多国家有类似我国的保密事项范围，如定密指南、《属于国家秘密的情报目录》等。

有的国家规定，定密指南由原始定密官员发布，用于确定某具体信息中必须保密的要素，并确定每一部分秘密信息的密级及保密期限。定密指南至少每5年修订一次。

有的国家《属于国家秘密的情报目录》经总统令批准颁布，详细列举军事、外交、经济和科技、侦察和反侦察工作等领域中属于国家秘密的信息，以及掌握该信息的国家行政机关及其他单位的名称。

国家秘密的保密期限是如何规定的？

国家秘密的保密期限，应当根据事项的性质和特点，按照维护国家安全和利益的需要，限定在必要的期限内；不能确定期限的，应当确定解密的条件。

国家秘密的保密期限，除另有规定外，绝密级不超过30年，机密级不超过20年，秘密级不超过10年。

机关、单位应当根据工作需要，确定具体的保密期限、解密时间或者解密条件。

知识链接

保密期限可以用3种方式来表现，分别是保密期限、解密时间和解密条件。

保密期限为具体的保密时限，如规定保密期限为5年，则从制发之日起满5年，该秘密事项即自行解密；

解密时间为具体日期或时刻，如规定某一秘密事项的解密时间为2020年5月1日，则到2020年5月1日该秘密事项保密期限到期，自行解密；

解密条件主要用于具体明确便于判断的事件或情形，如规定某一秘密事项以执行完毕作为解密条件的，则该事项实施完成后，自行解密。

国家秘密的知悉范围是如何规定的？

准确、适当地确定国家秘密的知悉范围，是确保国家秘密处于可控范围之内并采取相应保密防护措施的重要前提。

确定知悉范围有两个基本原则。一是工作需要原则。确定国家秘密知悉范围，首先应当根据工作需要确定，不应简单地把知悉国家秘密视作一种政治待遇，或者把行政级别作为确定国家秘密知悉范围的依据。将工作需要作为知悉国家秘密的前提条件，也是国际通行做法。二是最小化原则。在可能的情况下，应当把知悉范围尽量限定到最小。能够限定到具体人员的，限定到具体人员；不能限定到具体人员的，限定到机关、单位，由机关、单位限定到具体人员。

国家秘密知悉范围以外的人员，因工作需要知悉国家秘密的，应当经过机关、单位负责人批准。

知识链接

有的国家规定，符合下列条件的人员，可以接触定密信息：(1)获得部门首长或者其指派的人的批准；(2)签署保密协议书；(3)确需知悉该信息；(4)接受保密培训。

典型案例

2006年1月，有关部门在互联网检查时发现，某网站刊登1份机密级工作简报，造成泄密。经查，2005年1月，某机关编印了该机密级工作简报，因简报包含有关学习教育资料，临时决定把发文范围由原来只发特定单位的35份扩大到包括农业县区、城市社区基层单位在内的600份。由于发放范围广泛，基层环节较多，造成简报流失。事件发生后，该部门对涉密工作简报使用、发放不当的责任人员给予了相应处分。

哪些机关、单位有定密权?

确定国家秘密的密级,应当遵守定密权限。

中央国家机关、省级机关及其授权的机关、单位可以确定绝密级、机密级和秘密级国家秘密;设区的市、自治州一级的机关及其授权的机关、单位可以确定机密级和秘密级国家秘密。具体的定密权限、授权范围由国家保密行政管理部门规定。

公安、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。

上级机关、单位对某一事项已经定密的,机关、单位在执行时应按该事项已定密级确定。如中央下发拘国家秘密文件,各地区各部门在贯彻过程中,就该事项再产生的涉密文件、资料,应当按中央文件的密吸确定同等密级,不得擅自改变密级。

知识链接

机关、单位产生保密事项范围有明确规定而无权确定相应密级的国家秘密事项时,应当先行采取保密措施,同时立即报请具有相应定密权的上级机关、单位确定;没有上级机关、单位的,则根据该事项所涉及的业务范围,报请具有相应定密权限的业务主管部门或者保密行政管理部门确定。接到定密报告的机关、单位或者保密行政管理部门,应当及时作出批复。

经常产生国家秘密事项的无定密权的机关、单位,应当向业务主管部门或者保密行政管理部门申清定密权限。

定密责任人的主要职责是什么?

定密责任人包括两类人员,一是机关、单位的负责人;二是特别指定的人员。机关、单位主要负责人对定密工作负总责。分管业务工作涉及国家秘密的负责人,应当确定为定密责任人。机关、单位负责人一经任命,即是本机关、本单位的定密责任人,不需履行确定程序。

机关、单位可以根据工作需要,指定若干其他人员为定密责任人。需要指定定密责任人的,主要有两种情况,一是定密工作量大的机关、单位,如中央国家机关、省级党政领导机关和重要涉密单位;二是业务工作具有特殊保密要求的机关、单位,如公安、国家安全、纪检监察机关和武器装备科研生产单位等。

定密责任人职责既包括按照保密事项范围确定国家秘密,也包括根据情况变化变更和解除国家秘密。

具体职责有:

1、审核批准本机关、本单位产生的国家秘密的密级、保密期限和知悉范围;

2、对本机关、本单位产生的尚在保密期限内的国家秘密进行年度审核,作出维持、变更或者解除的央定;

3、对是否属于国家秘密和属于何种密级不明确拘事项先行拟定密级,并按照规定的程序报有关保密厅政管理部门确定。

知识链接

授权专门人员行使定密权,是许多国家的通行做法。有的国家实行定密官制度,强调定密工作的个人责任制。定密官分为原始定密官和派生定密官。原始定密官由总统行政命令直接确定或授权确定。享有原始定密权的有总统、履行行政职责的副总统、部长以及由总统任命并公布的官员。上述官员可以对定密权进行委托授权,'委托授权的同时要明确被委托人享有的原始定密权级别,不得越权定密。派生定密不需要授权,但要根据原始定密官所制定的定密指南进行。

国家秘密如何标志?

国家秘密标志是一种法定的文字与符号标识,用以表明所标识的物品(载体以及设备、产品等)承载内容属于国家秘密,并提示其密级和保密期限。机关、单位对其制作的国家秘密载体必须标注密级、保密期限,这是法定的强制性要求,目的在于提示并要求知悉范围内的机关、单位和人员采取保护措施,承担相应的保密义务,同时也提示知悉范围外偶然获得国家秘密载体的人员,有责任对其履行保密义务,对国家秘密进行妥善保护。做出国家秘密标志,对于有效保护国家秘密的安全,具有十分重要的作用。

国家秘密标志,可以根据不同的载体形式采用不同的标注方式,但应当易于识别。

书面形式的载体应在封面或首页做出国家秘密标志;地图、图纸、图表则在其标题之后或者下方适当位置做出国家秘密标志。

非书面形式的载体,要以能够明显识别的方式予以标注;凡有包装(套、盒、袋等)的载体,应以恰当方式在载体包装上标注。

汇编涉密文件、资料,应对各独立文件、资料做出标志,并在封面或者首页以其中最高密级和最长保密期限做出标志。

摘录、引用属于国家秘密内容的,应按照其中最高密级和最长保密期限做出标志。

电子文档中含有国家秘密内容的,应做出国家秘密标志,且国家秘密标志应与文档正文不可分离。

对不能或不宜做出国家秘密标志的,包括一些特殊的属于国家秘密的设备、产品,产生或制作机关、单位应作出文字记载,并将其密级和保密期限及时通知知悉范围内的机关、单位或人员。

国家秘密标志专用于标注各类国家秘密载体和属于国家秘密的设备、产品,商业秘密、工作秘密、个人隐私及其他不属于国家秘密的不得使用国家秘密标志。

知识链接

有的国家规定,对定密信息使用统一的保密标志。如果不能在特定的秘密信息或者定密材料上做出保密标志,产生该信息的人员应当向信息接收人或者持有人发出书面保护指令。保密标志应当统一、清晰地标注在信息上,以清楚地表明信息的保密状况、密级和保密期限。

国家秘密如何确定?

确定国家秘密应当严格依照法定程序进行。依照法定程序,是指根据定密权限,按照保密事项范围的规定,确定国家秘密的密级、保密期限、知悉范围,并做出国家秘密标志,做到权限法定、依据法定、内容法定、标志法定。

定密工作的基本程序是,先由承办人对照保密事项范围提出定密的具体意见,再由定密责任人审核批准。

在定密的同时,还要对国家秘密载体以及属于国家秘密的设备、产品做出国家秘密标志。

国家秘密与工作秘密和商业秘密的区别是什么？

国家秘密与工作秘密的区别在于：

1、法律性质不同。国家秘密是事关国家安全和利益的重要事项，工作秘密则是仅与党政机关的公务活动有关的不宜公开的内部情况、资料、信息，泄露工作秘密一般不会直接危害国家的安全和利益，而仅对党政机关的管理秩序构成一定的损害；

2、确定程序不同。国家秘密必须依照法定程序确定，而工作秘密则由党政机关根据公务活动的需要自行确定；

3、等级不同。国家秘密根据法律规定划分为绝密、机密和秘密三个等级，而工作秘密则无等级划分；

4、产生领域不同。国家秘密既可能产生于党政机关的公务活动，也可能产生于其他组织、团体的活动，而工作秘密则只能产生于党政机关的公务活动；

5、法律责任不同。国家秘密受《中华人民共和国保守国家秘密法》保护，泄露国家秘密的法律责任形式是刑事责任和行政责任，工作秘密受《中华人民共和国公务员法》保护，泄露工作秘密的法律责任形式是行政责任。

国家秘密与商业秘密的区别在于：

1、法律性质不同。国家秘密体现公权力，其权利主体是国家，而商业秘密体现私权利，其权利主体是技术、经营信息的发明人或者其他合法所有人、使用人；

2、确定程序不同。国家秘密必须依照法定程序确定，而商业秘密的确定视权利人的意志而定；

3、国家秘密不能自由转让，而商业秘密则可以进入市场自由转让；

4、法律保护水平不同。对国家秘密，有专门的保密法及其配套法规予以保护，而商业秘密受《中华人民共和国反不正当竞争法》保护，主要由权利人自行管理。泄露国家秘密的法律责任主要是刑事责任和行政责任，而侵犯商业秘密承担的法律责任主要是民事责任，只有当侵犯商业秘密行为造成权利人重大经济损失或者有其他严重后果的，才能追究刑事责任。

知识链接

国外基本没有与工作秘密完全对应的概念，一般把工作秘密作为政府信息公开时不宜公开的事项。也有一些国家把工作秘密放在国家秘密范畴里进行保护，如有的国家规定内部资料是国家秘密的等级之一。有的国家将可能对特定的公共利益造成损害，因而不能被泄露的信息称为敏感信息。

国家秘密与商业秘密在一定条件下可以互相转化。国家秘密中涉及科技和经济发展的事项，随着时间的推移，对国家安全和利益的影响可能会明显减弱，从而丧失国家秘密的特性而予以解密。但对于实际产生或使用该秘密的企业来说，该秘密事项可能对维护其经济利益、保持其竞争优势仍具重要价值，此时，企业就可以在国家秘密解密后将其转化为商业秘密。反之，企业的商业秘密如果与国家安全和利益有重大关系，具备了国家秘密的基本属性，应当依照法定程序确定为国家秘密。

国家秘密如何变更？

国家秘密变更的内容，包括密级的降低或提高、保密期限的缩短或延长、知悉范围的缩小或扩大。三者既可以单独变更，也可以同时变更。国家秘密的密级如有下列情形之一的，应当及时变更：一是国家秘密确定时所依据的保密事项范围已作调整；二是该事项泄露后对国家安全和利益的损害程度发生明显变化。

国家秘密变更，由原定密机关、单位决定，也可以由其上级机关决定。变更后，应及时书面通知知悉范围内的机关、单位和人员。接到通知的有关机关、单位和人员，应当在原涉密载体上做出国家秘密变更后的标志。

非本机关、本单位确定的国家秘密事项，需要变更的，可以向原定密机关、单位或其上级机关或有关保密行政管理部门提出建议，不得自行变更。

“不明确”和“有争议”事项的密级如何确定?

机关、单位对是否属于国家秘密或者属于何种密级不明确或者有争议的,由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门确定。

对是否属于国家秘密或者属于何种密级不明确的,机关、单位应当先行拟定密级并采取保密措施,逐级报至有权确定该事项密级的保密行政管理部门确定,保密行政管理部门应当及时作出决定。

合法知悉国家秘密事项的机关、单位对某一事项是否属于国家秘密或者属于何种密级持有不同意见,向原定密机关、单位提出异议未被接受的,争议各方均可向有相应密级确定权的保密行政管理部门提出。在定密争议解决前,争议双方应当按照原定密级对有关事项继续采取相应的保密措施。国家秘密知悉范围内的人员对所知悉的已确定密级的事项认为定密不当的,可以通过其所在机关、单位向原定密机关、单位提出。

知识链接

有的国家规定,当获得授权的信息持有人善意地认为该信息的定密状况不合适时,鼓励并期待该持有人按照规定的程序对信息的定密状况提出异议。

定密异议必须以书面形式提出,但只需要对为什么定密或者不定密,以及为什么定为某个密级提出质疑,无需阐述更具体的理由。

所有政府机关应当建立一个系统来处理、追踪和记载信息授权持有人所提出的正式的定密异议。

政府机关应当在60日内对异议作出书面答复。

国家秘密如何解除?

国家秘密的解除,是定密工作的重要组成部分。对不需要保密的事项及时解密,有利于节约保密资源,集中人力、物力和财力做好国家秘密的保护工作,有利于信息资源的合理利用。

解密主要有两种方式:

一是自行解密,即保密期限已满的国家秘密事项自行解密。机关、单位对于保管、使用的国家秘密保密期限已满而未收到有关机关、单位延长保密期限通知的,可以认定该项国家秘密已经自行解密,不需要继续履行相应的保密义务。

二是审查解密。机关、单位应当定期审核所确定的国家秘密事项,特别是保密期限即将届满的国家秘密事项。对在保密期限内的因保密事项范围调整不再作为国家秘密事项,或者公开后不会损害国家安全和利益,不需要继续保密的,应当及时解密,并通知原知悉范围内的机关、单位和人员。

解密的国家秘密事项并不意味着可以公开。有的国家秘密事项解密后,可能需要作为工作秘密或内部事项进行管理。需要公开的,应当由解密的机关、单位经过审查后作出决定。

知识链接:

世界各国都对国家秘密的解除进行了明确规定。

有的国家解密制度由自动解密、系统解密和强制解密组成。符合解密条件的秘密信息到期自动解密;对未满保密期限不能自动解密的信息,产生秘密的部门要定期系统审查,以决定是否降密或解密;任何个人或机构均有权向特定的行政机关提出对特定的国家安全信息予以强制解密的请求,接受强制解密请求的部门均应对该信息进行审查,以决定是否解密。

如何收发、传递涉密载体

涉密载体的运转过程，主要包括密件的收发、传递、传输、签收、送阅等环节。

密件收发的保密要求。接收密件时，应当严格按照收发密件的基本程序办理，严格履行清点、签收手续，并检查签收单上的登记与密件实物是否相符。分发密件时，应当严格按照限定的接触范围分发，不能擅自扩大范围。限定范围以外的机关、单位因工作需要要求增发的，应当经过单位主管领导批准。分发时，应当认真填写密件分发表。

传递密件的保密要求。绝密级密件在市区内投递，应当派专车双人进行或者交由机要交通部门投递。其他密级的密件，也要专车专人投递，或者通过机要文件交换站进行交换，或者交由机要通信部门投递。发往市区外的密件，要通过机要交通或者机要通信部门投递。携带密件不得进入与工作无关的场所。未经批准，禁止携带密件参加外事活动和进入境外机构。携带密件外出途中安全受到威胁时，应当立即就近请示保密、公安、国家安全部门或请求其他国家机关、单位予以帮助，并尽快与本机关、本单位取得联系，如实报告情况。

因公出境一般不得携带密件。确因工作需要携带的必须按照国家保密局、海关总署《关于禁止邮寄或非法携运国家秘密文件、资料和其他物品出境的规定》办理。在出境时，海关凭许可证查验后放行。这些规定也适用于机关、单位在对外交往与合作中合法向外方提供国家秘密，并由外方人员携带国家秘密出境的情况。

守好 [无形密]

涉密人员除了要管好这些看得见的涉密载体外，更需要管好自己以及“无形密”。“有形密”失泄露尚可追查，或许能有所补救，而“无形密”失泄露则难以察觉，无法补救，所造成的损失和危害也无法估量。有以下几点值得注意：首先，要守住脑。涉密人员一定要有敏感的保密神经和牢而又牢的保密意识，只有从思想上绷紧保密弦，行动上才不会失去底线，才能从根子上减少失泄密事件的发生。其次，要管住嘴。“酒后吐真言”告诉我们，喝酒会使人乱了方寸，所以涉密人员一定要做到“不该说的不说”、“不该喝的不喝”，只有管好自己的嘴，才能保住心中的密。最后，要藏住心。自己喜欢什么，不喜欢什么，哪方面强，哪方面弱，不要轻易示人，以免他人投其所好，慢慢用各种诱惑引诱，最后被引上不归路。

办公场所泄密警示录

近年来，机关单位普遍加强了针对计算机网络的保密管理，涉密人员网络信息安全意识和保密技术常识明显增强。然而，与此同时，一些涉密人员却忽略了办公室的安全保密工作，认为办公室环境相对封闭，存放涉密文件资料相对安全，放松了警惕。殊不知，正是这种错误认识的存在，导致了窃密泄密案件的发生。

信访信中的涉密文件从何而来？

2014年1月，有关部门接到通报，在群众信访来信中发现1份与其信访事项相关的秘密级文件复印件，虽然文件编号有被涂抹的痕迹，但仍然可辨。经核实，该文件系发放至某市属单位信访部门的涉密文件。

文件从何而来？调查后，办案人员厘清了事件的来龙去脉。

1月3日，某市属单位信访部门工作人员取回上述涉密文件后，经办公室主任孙某签批，报局长张某审阅。1月6日，办公室文秘佟某将文件送给张某，由于张某的办公室总是有很多上访人员进出，佟某未能及时将文件送达，就拿回放在了自己的办公桌上。期间，佟某多次离开办公室维持信访秩序，都未锁门。上访人员杜某趁佟某办公室无人之际将上述文件拿出，阅读并复印3份，随后将原件放回原位。

此后，杜某将复印件交给上访人员谷某，委托他邮寄给相关部门。谷某称，在邮寄称重过程中信件散落在地上，他看到了复印件，觉得好奇就又复印了1份。另外，上访人员孙某也复印了1份。案件发生后，有关部门将上访人员手中持有的涉密文件进行了回收销毁，给予负有直接责任的佟某行政警告处分并调离工作岗位，给予负有领导责任的张某行政警告处分，对主管副局长白某通报批评，对办公室主任孙某通报批评并调离该单位信访部门。

办公室不是保险柜

诚然，办公室相对于其他外部区域，尤其是单位以外的区域而言，封闭性和安全性更强。但这种安全性和封闭性并不是绝对的，尤其是那些与外部人员经常接触的部门。一些机关单位工作人员放松了保密弦，没有对涉密文件资料按照保密管理要求进行严格管理，使之处于失控状态。分析近年来发生在办公室内的窃密泄密案件，主要有以下两个方面的原因：

一是部分涉密人员保密意识不强且存在不良工作习惯。一些机关单位工作人员想当然地将办公室当做绝对安全的场所，视为涉密载体的“保险柜”，不采取任何防范措施，随意摆放涉密载体，导致涉密文件事实上处于失控状态。本案中，佟某离开办公室没有锁门，给上访人员窃取涉密文件以可乘之机。此后，涉密文件已经被杜某、谷某多次复印，泄密结果已经发生，但由于杜某复制后又将涉密文件放回了原处，佟某始终没有察觉，导致文件泄露后未能及时采取补救措施，知悉范围进一步扩大。此案并非个案。2011年5月至6月间，某县人大常委会办公室文件管理员刀某先后从县委办、县政府领取多份涉密文件，因单位领导外出，刀某便将文件摆放在办公桌上。待刀某准备将文件送领导签阅时，发现涉密文件已下落不明。后经多方查找，仍未找到。又如，2005年，某县信访部门收到市信访部门密传的1份机密级文件，当文件传阅至朱某时，正遇有人上访，朱某便随手将文件放在接待室的桌子上，离开接待室接访，造成了国家秘密的泄露。

二是办公室环境安全隐患突出。存放、保管涉密载体的办公场所，其安全性、封闭性必须满足一定的标准，能够防止盗窃、窥视和破坏行为的发生。以保密要害部门部位为例，不仅应当满足“三铁一器”的基本要求，还应当限制非涉密人员的进出。以本案为例，信访部门长期面对大量群众来访，接触人员复杂，极易出现场面混乱的情况。因此，非办公人员进入办公场所，拿走涉密文件、损坏涉

密载体等情况在此类部门时有发生，更要高度防范，绝不能有一丝马虎。此外，还要适时对存放、保管涉密载体办公室的安全情况进行检查，一旦出现问题，应及时采取补救措施，减少损失。

杜绝办公室失泄密的“蝴蝶效应”

如何有效防止办公室发生失泄密事件，可以从以下三方面入手。

第一，强化涉密人员保密意识和保密常识，加强保密教育培训。要对本单位本部门尤其是办公室日常工作中的保密薄弱环节进行梳理，明确保密工作的风险点和防控重点。对已经出现的办公室泄密问题要积极反思、查漏补缺；对可能出现的办公室泄密问题要进行前瞻判断，并制订相应的处置预案。要加强保密教育培训，督促涉密人员培养良好的保密习惯：将涉密载体按照不同密级存放在专门的保险柜内；离开办公室时做到“关门、闭窗、锁柜”；对可能接触到涉密载体的人员仔细观察、细致询问，出现异常立即报告。

第二，要加强办公室保密环境建设，提高办公安全指数。要加强办公室“硬件”建设，严格按照保密要求进行办公场所建设，配备相关涉密载体保管、登记、销毁设备，并在保密要害部门部位管理上坚决落实“三铁一器”等措施。同时，加强办公室管理和安全常规检查，防止无关人员进入，适时对保密防护设施设备的使用、涉密人员变动、涉密载体流转及销毁等情况进行检查，并适时改进调整。

发生在办公室里的泄密总是静悄悄的，就像“蝴蝶效应”中那只扇动翅膀的蝴蝶，初始时我们难以察觉，但正是这翅膀的微微扇动，却引发了一系列连锁反应，并最终导致“美国德克萨斯州的龙卷风”。办公室的泄密也是如此，也许只是薄薄的一页纸被违规带走，但其中包含的涉密信息或许会使一个行业发生巨变。在以往发生的案件中，就有因办公室的涉密文件违规流出而影响整个股市行情的情况。在此提醒大家，尤其是政府职能部门，一定要加强办公室保密管理，防止失泄密事件的发生。

涉密人员在岗有哪些保密要求

涉密人员上岗后，应接受在岗教育培训、出境及从业限制，遇有重大事项应报告，并接受监督。

1、涉密人员应接受在岗教育培训。用人机关、单位应对涉密人员开展经常性的保密形势、保密工作政策法规和保密知识技能更新教育，使涉密人员切实增强保密意识、养成保密习惯、提高保密技能。

2、涉密人员出境要进行审批。主管部门要严格涉密人员出境审批，必要时应征求公安机关和国家安全机关的意见。公安机关和国家安全机关认为涉密人员出境可能对国家安全造成危害或者对国家利益造成重大损失的，有关部门不得批准。未经机关、单位及主管部门同意，涉密人员不得私自办理出境手续；严禁弄虚作假，以其他身份骗取办理出境手续。

3、涉密人员从业有严格限制。严禁涉密人员私自到境外机构、组织或者外商独资企业工作，私自为境外机构、组织或者人员提供劳务、咨询或者其他服务。涉密人员所在机关、单位发现其有上述行为，必须予以制止，并取消其涉密资格。

4、涉密人员对下列事项应当及时报告：发生泄密或者造成重大泄密隐患的；发现敌对势力和境外情报机构针对本人有渗透、策反行为的；接受境外机构、组织及非亲属人员资助的；与境外人员结婚的；配偶、子女获得境外永久居留资格或者取得外国国籍的；其他可能影响国家秘密安全的个人情况。

5、涉密人员要接受在岗监督。机关、单位应及时了解掌握涉密人员思想状况和工作表现，制止和纠正涉密人员违反保密法规的行为。对不适合在涉密岗位工作的，应当及时调离。对在党和国家保密工作方针政策贯彻落实、保密法律法规制度贯彻执行、保密工作开展、泄密隐患发现处理等方面有突出成绩的，应予以表彰奖励。

保密干部的培训教育

保密干部的培训教育工作，主要由保密行政管理部门和所在机关、单位负责，要突出重点，着眼长远，注重针对性，既要考虑阶段性工作需要，又要着眼于保密干部队伍整体素质的提升。培训教育的内容主要包括：党的保密工作方针政策、保密形势任务、保密专业知识、保密工作技能等。其中，保密专业知识教育，要突出保密法律、保密管理、保密科技知识的培训。从保密工作的内容看，要着重抓好定密、涉密人员、涉密载体、涉密信息系统、涉密活动、涉密场所、保密审查、保密监督检查、违规行为管控和泄密案件查处等专业知识的教育。

教育培训的方式，既包括组织集中培训，又包括督促干部自学，还包括督促干部养成在实践中学习的习惯，通过总结保密工作实践经验，把握保密工作的基本规律，丰富保密知识，提高工作能力和水平，提升自身的素质修养。同时，还应充分发挥国家保密教育培训基地的作用，有计划地组织保密干部到培训基地接受全面系统的保密科学知识和相关理论知识的培训。

保密干部的概念

保密干部，是依照保密法律规定，履行保密管理职责，组织开展保密工作的人员，包括各级保密委员会组成人员和各级保密行政管理部门、保密工作机构的专兼职工作人员。保密干部是开展保密工作的主体，是做好保密工作的组织保证。

专职保密干部，是指根据机关、单位职责分工，专职从事保密行政管理工作的人员，如机关、单位保密工作机构的工作人员。有的机关、单位虽未设立专门保密工作机构，但配备有专职负责保密管理工作的人员，这些人员也属于专职保密干部；兼职保密干部，是指机关、单位未设立专门保密工作机构，但指定其他岗位的干部兼职负责保密工作管理，这类工作人员即为兼职保密干部。根据保密工作管理的需要和有关规定，中央和国家机关，省级领导机关，军工科研生产单位，高等院校及重要涉密科研单位，保密资质单位，军队师级以上机关、单位和其他保密工作任务较重的机关、单位，应当配置一定数量的专职保密干部。机关、单位保密干部数量配置，一般根据保密工作任务决定，以能够满足保密管理需求为标准。

保密，从销毁开始

销毁涉密载体应当符合国家保密规定和标准，确保销毁的涉密信息无法还原。

1、决定销毁的涉密载体，应当进行清点登记造册，经本机关、本单位主管领导审查批准后销毁。

2、送销毁机构销毁的涉密载体，应严密分装，由专人押送到保密行政管理部门建立的销毁机构或定点承销单位销毁。

3、机关、单位自行销毁少量涉密载体的，应当使用符合国家保密标准的销毁设备和方法。

4、严格禁止将拟销毁的涉密载体作为废品出售或转送他人。

保存涉密载体有哪些保密要求？

1、涉密载体必须在符合国家保密标准的场所和文件保密柜内保存。绝密级涉密载体应当专柜保存。

2、离开办公室时，应当将涉密载体存放在保密设备里，并严密关锁门窗。

3、个人因公持有的涉密载体，使用完毕后应当及时清退。严禁个人持有和私自保存涉密载体。

案例警示：

2011年7月，某测绘队办公室被盗，室内存放的两台笔记本电脑丢失。经核实，其中一台为涉密笔记本电脑，内存多份涉密地图和涉密地理信息数据。经警方核实，此次事件是因该办公室人员李某下班忘记锁门所致。事件发生后，李某及该测绘队相关负责同志受到严肃处理。

保密干部的工作内容

单个保密干部的工作内容，由其供职的岗位职责决定，主要包括：保密法制、保密宣传教育、保密指导管理、保密科技工作和技术保障服务、保密监督检查等。从保密部门工作功能上划分，保密干部的工作同一切机关、单位的工作一样，大体分为决策和决策参谋、具体工作的组织实施和后方保障服务等3个层面。

保密法制建设，一是建立规则，制定规矩，如制定保密规章制度和政策性规定；二是组织和推动保密法律制度和方针政策的贯彻实施。**保密宣传教育**，一是对社会的保密宣传，如普及保密法，引导公民树立履行保密义务的意识和自觉性；二是对机关、单位工作人员特别是领导干部和涉密人员进行保密教育培训，增强他们的保密责任意识，传授必备的保密防范常识。**保密指导管理**，涉及政治、经济、国防、外交、文化、教育、民族、宗教等各个领域的保密工作。其中，产生国家秘密较多、较为密集的直接关系国家核心安全和重大利益的重点行业领域、重点区域是指导管理的重点。**保密科技和技术保障服务**，一是制定保密科学技术发展规划、计划和政策性措施，制定保密技术标准；二是确定保密技术研究开发方向和具体项目，组织和管理保密科学技术研究开发活动，对研究项目进行审查论证，推进科技研究成果转化；三是组织保密技术的推广应用和重点保密技术装备配备；四是为重大涉密会议、涉密活动提供保密技术支持和服务保障；五是开展保密科技测评工作。**保密监督检查**，一是指导各机关、单位开展自查自纠工作；二是直接组织开展保密检查活动。三是督促机关、单位对所发生的违规行为和泄密问题依法进行查处；四是对重大泄密案件直接组织调查处理。

保密干部的素质

素质是指人在政治、思想、作风、道德品质、知识、能力等方面所具备的素养，是人的一种较为稳定的属性，对人的行为及行为方式能起到长期的持续的影响。保密干部的职业特点及保密工作性质和任务，对干部的素质有特殊的要求。

1、政治素质。保密干部必须讲政治，对党忠诚，对国家忠诚，对保密事业忠诚。有坚定的政治信仰和政治敏锐性、政治警觉性、政治原则性，能够准确把握和正确运用马列主义、毛泽东思想、邓小平理论、“三个代表”重要思想和科学发展观的立场、观点、方法，以及中央关于保密工作的方针政策，处理好保密工作面临的复杂情况和问题。

2、思想素质。保密干部必须具有强烈的责任意识，在履行保密管理职责时，严格按政策办事，不徇私情，不牟私利；必须具有很强的组织纪律观念，自觉遵守法纪，严格执行组织决定；必须具有实事求是、严谨细致、勇于开拓和深入扎实的工作作风。

3、专业素质。保密工作是一项专业性很强的工作，保密干部必须懂法律，特别是要全面掌握和熟练运用法律制度规定，能按照法定程序处理保密工作问题；必须懂技术，了解现代窃密技术和保密技术发展现状，能运用现代保密防护技术和检查技术开展保密管理；必须懂管理，能准确把握保密管理工作的基本规律和特点，同时对工作所涉及领域的基本知识和管理要求有比较深入的了解。

4、能力素质。保密管理是行政管理工作，要求保密干部必须具备机关工作能力，能够应对复杂情况，处理好各种问题；具备调查研究和文字语言表达能力；还要有安于清贫、无私奉献、甘当无名英雄的心理承受能力和较好的身体素质。

如何监管涉密会议、活动

保密行政管理部门需采取的保密管理措施：在职权范围内，对涉密会议、活动的保密工作进行监督和指导。对重大涉密会议、活动，需派驻保密工作人员参与全过程管理。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检测，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。

主办单位需采取的保密管理措施：1、严格审查参加人员。应根据涉密程度和工作需要，确定参加人员范围，审核其资格，登记姓名、单位、职务等情况，并保存相关材料。2、严格涉密载体管理。对涉密会议、活动使用或形成的涉密文件材料及其他涉密载体，在制作、分发、存放、回收、销毁等环节落实保密管理措施。3、严格场所设备检查。涉密会议、活动应在符合保密要求的场所进行，使用的扩音、录音等电子设备、设施应经安全保密检查检测，携带、使用录音、录像设备应经主办单位批准。不得使用无线设备或装置，不得使用不具备保密条件的电视电话会议系统。4、严格保密要求。对参加人员（含列席人员以及工作、服务人员）进行保密教育，要求其妥善管理涉密文件资料和其他涉密载体，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。5、严格新闻报道审查。接受采访或进行公开报道应当经过批准。

保密干部职业化的重点

保密干部职业化的重点是保密干部队伍建设和队伍素质的培养。根据保密工作实际和职业化发展的要求，着重是要解决保密干部的职业意识、职业水准、职业操守问题。

职业意识首先是专业意识。要求从业人员必须认识和理解保密工作是一门综合性很强的科学，有着自身客观规律和与之相适应的知识体系、工作法则和技术标准，有专门的知识、技术和要求，这是保密干部入门从业的门槛。责任意识是职业意识的重要内容。它要求从业人员必须把保密工作作为“天职”，对保密事业有强烈的责任感、使命感。职业意识还包括荣誉意识和归属意识。它要求从业人员必须懂得进入保密行业、从事保密职业是一种责任，应自觉做到爱岗敬业，忠于职守。

职业水准，就是要求从业人员必须知道，保密工作在各个方面有严格的职业规范和知识需求，必须具备一定的职业能力和从业技能。

职业操守，则要求从业人员必须具有依法行政、廉洁自律、遵纪守法、严谨细致、埋头实干和淡泊名利的职业道德。

涉密载体有哪些种类？

涉密载体，是指以文字、数据、符号、图形、图像、声音等方式记载国家秘密信息的纸介质、光介质、电磁介质等各类物品。

纸介质涉密载体是指传统的纸质涉密文件、资料、书刊、图纸等。

光介质涉密载体是指利用激光原理写入和读取涉密信息的存储介质，包括 CD、VCD、DVD 等各类光盘。

电磁介质涉密载体包括电子介质和磁介质两种。电子介质涉密载体，是指利用电子原理写入和读取涉密信息的存储介质，包括各类 U 盘、移动硬盘等；磁介质涉密载体，是指利用磁原理写入和读取涉密信息的存储介质，包括硬磁盘、软磁盘、磁带等。

密品是直接含有国家秘密信息的设备、产品等。这种设备、产品有的可以通过外观观察获得国家秘密信息，有的则需要通过一定手段进行测试或相关数据资料分析获得国家秘密信息。

保密宣传进行时

做好保密工作是日益复杂的国际形势需要，也是保证国家政治稳定、经济持续、快速发展的根本前提。近年来，我国关于保密工作的法规、政策不断完善，保密工作得到不断规范，但国内外敌对势力总是想方设法，不择手段地窃取我国国家机密，蓄意破坏我国政治安定、经济发展的和谐局面。我们要更加清醒地认识到保密工作的重要性，全方位地做好保密工作，为政治、经济发展奠定坚实基础。

1、保密工作的作用

一是维护国家安全和社会主义制度的重要手段；二是维护国家综合国力竞争优势的重要手段；三是维护改革发展和稳定大局的重要手段。

2、国家秘密具备的要素

一是实质要素：关系国家安全和利益，是国家秘密的本质属性，是国家秘密区别于其他秘密的关键所在；二是程序要素：依照法定程序确定；三是时空要素：在一定时间内只限一定范围的人员知悉

3、国家秘密保密期限除另有规定外，绝密级不超过三十年，机密级不超过二十年，秘密级不超过十年。

4、涉密人员分类按照涉密程度分为核心涉密人员、重要涉密人员和一般涉密人员，实行分类管理

5、法律法规

《中华人民共和国保守国家秘密法》《中华人民共和国保守国家秘密法实施条例》。

如何开展保密法制建设

开展保密法制建设，主要包括两方面工作：一是建立规则，定制规矩，如制定保密规章制度和政策性规定；二是组织和推动保密法律制度和方针政策的贯彻实施。

保密规章制度是用以规范涉密行为的准则、规矩。保密干部制定制度规范时，要深入实际调查研究，特别是要认真研究泄密案例和实践中的保密工作方法、经验，分析哪些行为容易造成国家秘密失控，易于导致国家秘密泄露；哪些做法行之有效，合乎情理，符合政策规定，然后将其归纳提炼，形成条文式的制度规定。制度规定要做到“堵”“疏”结合，既要有“堵”的禁止性规定，又要有“疏”的引导性规定。制度要明确地告诉大家哪些能做、如何做，哪些不能做、如何防范。

组织和推动保密法律制度和方针政策的贯彻实施，是制定保密规章制度的目的。工作中，一要做好工作规划，提出目标要求和推进贯彻落实的具体措施；二要及时引导和加强督促检查，总结推广工作经验，促进法规制度贯彻工作平衡推进。

从互联网及其他公共信息网络上拷贝信息资料到涉密计算机上应如何操作？

为确保涉密信息安全保密，应当严格禁止从互联网或其他公共信息网络直接向涉密计算机拷贝信息。如果确因工作需要拷贝的，可以通过以下途径：

1、将要拷贝的资料刻录到空白光盘中，再通过光盘将资料复制到涉密计算机上。

2、先将互联网上的资料拷贝到单设的中间机上，彻底清除窃密程序和查杀病毒后，再拷贝到涉密计算机上。

3、使用经国家保密行政管理部门批准的信息单向导入设备。

提示：严禁使用除光盘外的移动存储介质从连接互联网的计算机上直接拷贝文件、资料到涉密计算机上。

党政机关工作人员手机泄密隐患

手机、平板电脑等早已成为人们工作、生活和娱乐不可或缺的“利器”。但也正因其功能强大，稍有不慎，“伤”到自己的情况也较为普遍。网络钓鱼、木马病毒、敌特机关精心设计的陷阱大量充斥在无形的网络空间，身处特殊重要岗位和涉密程度较高的人员应当尤为注意。

1、不要过于详细地记录联系人信息为了弄清“谁是谁、在何处、什么单位”等情况，一些人便在通讯录中增加了备注信息，或直接将这些信息加在联系人的姓名后，如：张三，北京，XX局局长；李四，XX部队团长……

殊不知，此做法在方便自己区分的同时，也方便了敌特分子和诈骗人员。一旦手机丢失或被植入木马，极易造成隐私和敏感信息外泄。为此，大家在存储手机号码时切莫过于详细，如若想方便区分，可添加一些易于自己记忆的代号或记录在纸质通讯录中。

2、不要轻易将智能终端操作系统破解

即通常我们说的“越狱”（IOS系统）、“ROOT”（安卓系统）等提高权限的操作。

然而，在系统被破解后，系统更新通常也无法正常运行，以致系统BUG和安全漏洞无法修补，严重影响智能终端安全。以苹果产品为例，“越狱”后的苹果产品，大大增加了遭遇恶意程序和木马病毒的风险，且病毒同样可以获得系统最高权限。一旦中招，你的声音、图像和手机里的一切信息将“被分享”。倘若不会分辨、不加甄别，便更容易中招。

为此，在没有特殊需求的情况下，尽量不要破解系统或将手机系统刷成非官方的系统。

3、不要轻易连接免费Wi-Fi和无加密防护的Wi-Fi网络使用免费或没有加密防护的Wi-Fi网络，除极易被“钓鱼”外，通信内容也极易被监听和篡改。若是连上了“黑”Wi-Fi，手机还可能遭到攻击和被植入木马。特别要说明的是，使用像“Wi-Fi万能钥匙”“免费Wi-Fi”等软件并不安全，若使用，你所掌握的Wi-Fi密码自然也有可能被与人分享。若被别有用心的人由此连上了你的路由器并监听其中数据，那么，你的网络访问便也毫无安全可言。

4、不要轻易打开GPS定位功能

手机的GPS模块可能暴露我们的位置信息。当用户的位置信息积累到一定量，通过分析很容易推断出用户的工作地点、工作性质、家庭住址、生活规律等。目前，市面上有许多软件也都会访问和收集用户的位置信息，如一些社交类软件、导航类软件，甚至影音娱乐软件等。

我们关闭定位功能后，系统中的许多软件将无法获取用户终端的位置信息，这在一定程度上提高了手机的安全性，所以，在平时应尽量将GPS开关置于关闭状态。

5、不要轻易扫描来路不明的二维码

单从二维码本身并看不出其中隐藏了什么内容，这也正好成了一些别有用心之人可钻的空子。他们将恶意程序和木马病毒制作成二维码在网络上大肆传播，一旦用户扫描，手机便会在后台自动下载并安装病毒程序，从而威胁你的隐私和财产安全。

因此，扫描二维码前一定要确定其来源，必要时，可使用一些二维码安全鉴别软件来识别恶意二维码。

6、不要随意乱拍照

现在的智能终端都具有拍照功能，并且像素非常高，手机也是如。手机等已然成为许多人的相机和“记事本”，甚至一些文件资料和证件都用手机拍下来，以方便使用。

殊不知，在拍照的同时，手机会将你拍摄的时间和空间信息存于其中，如若保管不当或设置不当，照片外流，很可能给你的隐私和文件资料安全造成威胁。

因此，在没有需求的情况

电信通信存在哪些泄密隐患？

电话、手机、传真机是目前普遍使用的大众电信通信工具，此外，电子邮件、QQ、MSN、手机短信、飞信、微信、微博等也越来越受到人们的欢迎。电信通信的泄密隐患主要有：

1、有线传输线路辐射泄密。有线通信传输线路工作时，会向周围空间辐射发射电磁波，利用相应设备可接收并还原所传输的信息。

2、网络串音泄密。相邻线路之间因各种原因极易产生串音。

3、无线传输泄密。微波、卫星、短波、超短波等无线信道广泛用于通信传输，所传输的信号暴露在空中，使用相应的接收设备，选择合适的位置，就可接收并还原通信内容。

4、通信设备电磁泄漏发射泄密。通信设备，如电话机、传真机、交换机等，工作时会产生电磁泄漏发射，通信信号会被辐射到数百米之外，利用相关技术设备就可以接收通信信号并还原通信内容。

5、现代通信网广泛使用计算机控制的程控交换机，如果计算机被置入“木马”间谍程序，程控交换机就会将通信信息发送给窃密者。

6、利用互联网进行语音通讯的网络电话软件，如 Skype，可能会被非法控制或监听，造成泄密。

传递涉密载体有哪些保密要求？

1、在市内传递机密级和秘密级涉密载体，可通过机要文件交换站进行，也可以派专人传递，绝对不能委托无关人员代为传递。

2、寄往市外的涉密载体，要通过机要交通或机要通信部门传递，不得通过普通邮政邮寄。

3、直接传递涉密载体时，应由专门人员负责，传递途中不能办理私事或进入无关场所。传递绝密级载体，需专车二人护送。

4、传递涉密载体，应由收文（件）机关、单位的机要室或收发室签收，不能随意由无关人员代收。

下，最好关闭相机的位置标签功能和 GPS 开关，在敏感、涉密场所或处理特殊公务时不要用手机拍照，更不要用手机拍摄涉密、敏感的文件资料和重要证件。尤其值得注意的是，即便手机拆下电池，也不能带入重要涉密场所。

7、不要把手机当 U 盘使用

这样做存在安全隐患：一方面，手机与其他设备频繁连接，增加了交叉感染木马病毒的可能性；另一方面，手机连接网络，容易被植入木马病毒或造成信息泄露。

特别应注意的是，不要将手机连接在涉密计算机上充电，如此，相当于建立了一座涉密计算机通向互联网的桥梁，应格外注意。

8、不要轻信、乱传网络上的伴“段子”随着网民素质的提高，这些负能量的转发大量减少。然而，一些“新伎俩”频频现身，即把谣言和负能量以“白 + 黑”的模式化妆起来，让人看起来像真理、正能量，以蒙混过关，达到传播负面信息的目的。

9、不要轻易使用“云备份”功能或开启自动备份开关

目前，几乎所有品牌的智能手机都有“云备份”功能，该功能主要是将用户的通讯录、短信、照片等数据上传至云端，以实现节省本地空间、易于转移调用、方便故障恢复等目的。然而，使用“云备份”，用户都需要承担传输信息安全和存储信息安全的风险，且信息上传到云服务器后，谁又能保证这些数据是否会被丢失、浏览或篡改呢？所以重要数据资料还是备份在自己手中为好，如 U 盘、移动硬盘等。

10、不要轻易出售废旧手机

废旧手机及存储卡通常存储有用户的通讯录、短信文电和图文数据，即便删除，也极易运用软件恢复，从而威胁用户的隐私、财产和数据安全。所以，废旧手机还是谨慎处理为好。

高校被策反学生遍及十余省：为境外提供情报

广东省安全机关还公布一起境外情报机构通过网络策反境内人员，窃取中国军事机密的案件，案犯李某被判处有期徒刑10年。《环球时报》记者从国家有关部门获悉，同一境外情报机构近年针对中国大陆学生实施了数十次网络策反活动，境外间谍以金钱诱使涉世未深的大学生甚至中学生参与情报搜集、分析和传递。来自权威消息源的案例显示，多数学生在网上求职或网聊过程中被境外间谍盯上，他们最初提供信息时并不知情，但部分人在觉察对方身份的情况下仍因贪利而持续配合，直至被国家安全机关依法处理。

◆由一篇网上求助帖而起

求职求助的学生、调研邀请、计件发酬，策反总是在看似合情合理的场景中揭开序幕。2012年4月，当广东省某航海学校专科生徐某考入该省某重点大学时，他在QQ群里发了一条求助帖。徐某的父母都在农村，家里生活不宽裕，他在网上“寻求学费资助2000元”。

不久，一网名为“Miss Q”的人回帖，询问了徐某的全名、手机号、就读院校和专业，然后表示愿意提供帮助。徐某喜出望外，把银行卡号告诉对方，第二天就收到2000元人民币汇款。徐某按这名“好心人”的建议，写了收条，用手机拍了照，然后通过QQ传给对方。徐某当时知道的是，“Miss Q”是“一家境外投资咨询公司的研究员”，需要为客户“搜集解放军部队装备采购方面的期刊资料”，希望徐某协助搜集，作为资助学费的回报。徐某痛快地答应了，但没能在航海学校的图书馆找到相关资料，而“Miss Q”也未强求。

这么好赚的钱，让当时正在实习的徐某心理发生变化，他开始觉得实习“又苦又累钱又少”。2012年5月，徐某主动联系“Miss Q”，对方向他提供了一份“田野调研员”的兼职，月薪2000元。徐某所在的广东某大城市有一个军港码头和一家历史悠久的造船厂，他的“调研”工作就是到军港拍摄军事设施和军舰，到船厂观察、记录在造在修船舰的情况，并将有船舰方位标识的电子地图做成文档，提供给“Miss Q”。双方约定的传送方法是，手机短信约好时间，这边徐某把加密文档上传至网络硬盘，那边“Miss Q”立即从境外登录下载。

一年后案发，徐某后来承认，做“调研员”不久，他就意识到对方是搜集我军事情报的境外间谍。他曾因内心极度不安主动放弃学校的一些荣誉，但利诱当前，又难以拒绝对方。2013年5月，徐某被国家安全机关依法审查。

有权威渠道的匿名人士告诉《环球时报》记者，境外情报机构最初与学生接触时，只提简单要求，如到图书馆查找资料、订阅学术期刊等，这些公开信息大多难以具备情报价值，但持续联系的过程，尤其是定期酬金支付极易让年轻学生形成依赖。随着要求具体深入，多数学生会觉察到对方身份，一些学生主动终止联系，一些人被威胁，也有人因贪利而继续配合。

该境外情报机构重点选定大陆一些地区和高校，勾连策反特定专业在校生。在涉及北方某重点航空航天院校的一起策反案中，该校一名大四学生在校内论坛找兼职时，看中一则待遇不错的“网络兼职”信息，并主动发邮件联系“雇主”。之后5个月里，这名学生多次向网名为“吉娜”和“Roby”的两名境外间谍提供航天、航空、船舶、武器装备类学术资料，并帮助他们订阅和翻拍内部学术期刊。

◆鼓动报考涉密岗位公务员

广东方面5月4日披露的案件中，境外间谍“飞哥”利用“网上书店”、军事爱好者网站等渠道，7年来在广东收买利用12人，在全国20余个省市收买利用40人。《环球时报》记者从权威消息源获取的资料显示，“飞哥”所属的境外情报机构，同样利用网络渠道收买利用大陆学生。从近

年的多起案例看，该境外机构以20岁左右的在读高校生为主要目标，借助网聊工具、校园论坛、招聘网站等物色“调研员”。“受聘”学生先做一些搜集、整理、汇总的活儿，即便提供的信息不具价值，也会定期收到数百或数千元酬金。

一名安全官员告诉记者，当学生对这种快速的收益上瘾后，该间谍机构将进一步安排更有针对性和机密性的信息搜集任务。如果学生不从，对方会威胁将此前的联系内容和金钱交易报给中国安全部门。在这一过程中，一些学生被发展为“情报员”，领取固定月薪，当这种控制力达到一定程度，境外情报机构开始安排和支配学生的就业选择和发展道路。

2012年下半年，浙江某重点大学毕业生宋某在招聘网站投递简历。12月初，“市场研究公司专员李华”发来邮件，邀宋某加盟。李华称，该公司主要业务是为在大陆投资的外资企业提供信息服务，宋某的工作是搜集中央政府部门的政策研究资料和撰写调研报告，报酬在2000元-5万元不等，高质量报告奖金丰厚。

宋某先后接到中央经济工作会议、农村工作会议、行业重组、能源产业发展等10项“调研课题”，他通过学校图书馆、论文期刊数据库、校内学术讲座等渠道搜集资料，向李华提交多份“研究报告”。其间，李华曾让宋某到他所在高校台湾研究所搜集两岸关系材料，但宋某不熟悉台研所的人事和情况，没能做成。

李华的要求逐渐深入，他要宋某积极培养人脉，从政府和有官方背景的智库、学者那里抓幕后、听观点，“拉关系的钱全由公司出”。2013年1月，宋某着手报考公务员，李华表示全力支持，为让宋某全心备考，还暂时停掉“调研课题”，并提供每月3000元生活补助。李华还对宋某报考的基层公务员岗位提出异议，因为“对公司获取信息没有帮助”，建议报考省级机关、智囊和研究部门。

上述安全官员对《环球时报》表示，鼓动境内学生报考省级或国家公务员、安全部门、军情机要等涉密岗位，是境外情报机构的惯用手段。案发后宋某承认，李华是“放长线钓大鱼”，将来会要求他提供更多内部机密信息。

◆高校“窝案”令人心惊

据统计，2012年以来，仅由该境外情报机构实施、证据确凿、被国家安全机关依法审查的网络策反境内学生案件，就有近30起，遍及中国大陆十余省市。有接近情况的匿名人士告诉记者，之前境外间谍也对年轻学生下手，2012年以来校园案发率上升，“这些机构越来越不择手段，利诱对象包括未成年人”。

《环球时报》记者梳理近年相关案例发现，涉案学生初期防范意识薄弱，中后期无法克制贪念，且对自身行为的危害性和法律后果认识不足。目前，有效的安全观教育在校园和社会缺失。记者进行简单的网络搜索，仅能获得极个别境外情报机构在中国大陆活动的当代案例，且信息简单，难以起到警示教育作用。网上倒是流传着一份2009年上半年出现的“中国民间防间谍不完全手册”。这份来源不明的手册介绍了当代间谍活动的基本手段，以及美国、欧洲、台湾等国家和地区针对中国大陆学生和留学生的策反思路，一度受到热捧。

传统上，情报机构主要靠金钱利诱，以情色或经济问题要挟，许诺未来和个人成就，以及通过冷战时期相当管用的意识形态诉求等手段勾连策反，被发展的本地情报员负责搜集、刺探、窃取、分析信息，其中部分人负责前方人员和后方总部间的信息传递，术语称“交通”。情报员也会策反他人，拓展情报来源。

网络策反学生的案例中，境外情报机构主要以积极兑现酬金的形式吸引和黏住学生，兼以要挟等手段，但不见面。涉案学生多数是个体行为，较为恶劣的案例中，境外间谍会诱导、建议学生发展自己的同学。2008年四川成都某高校就发生一起“窝案”：本科生吴某通过Skype找英语聊友，结识自称“外籍华商”的境外间谍。吴某介绍同学冯某加入，冯某又在校内论坛发布招聘广告，吸收同校研究生刘某、赵某。4人均在联系初期即觉察到对方“网特”身份，但仍签订“保密工作合同”，先后提供国内政治、经济、教育等领域大量内部期刊资料，其中包括多份“秘密级”刊物。案发时，4人共获得报酬4万余元。

◆国家安全不容微小隐患

通常，境内涉案学生短期内能接触到的核心信息和人员都比较有限，多数人案发时尚未造成

购置用于处理涉密信息的计算机要注意哪些问题?

国外特别是西方国家设计生产并出口的计算机设备往往设置有“后门”,存在泄密隐患。

此外,有的计算机具有无线互联功能,有的安全性能达不到标准。购买这样的计算机并用于处理涉密信息,存在很大的安全风险。

选购用于处理涉密信息的计算机时,应特别注意:

1、应当优先选购政府采购名录中的国产计算机设备。如需选购进口计算机及配套设备时,要选购经国家相关主管部门检测和批准的计算机及其设备。

2、要随机选购,不要事先预订。一旦选定,应当及时购买提货,防止被人设置、安装窃密装置。

3、使用前必须拆除具有无线互联功能的硬件模块。

4、使用前要请有关部门进行专门的安全保密技术检测,确定不存在泄密风险和安全隐患后,才能用于处理涉密信息。

上述要求适用于购买其他涉密办公设备。

汇编、摘抄涉密载体有哪些保密要求?

1、汇编、摘抄国家秘密文件、资料,应当经文件、资料原制发机关、单位批准。

2、经批准汇编的秘密文件、资料的密级、保密期限和知悉范围,应与原件保持一致。

3、秘密文件、资料汇编本,应当按所汇编秘密文件、资料的最高密级和最长保密期限做出国家秘密标志,并按相应密级进行管理。

4、摘录、引用国家秘密内容的笔记本,要做出与原件一致的国家秘密标志,按原件同样的保密措施进行管理。

严重的现实危害,有关部门强调,对“认罪悔过态度较好”的年轻学生要教育挽救。对此,国家安全部门官员接受《环球时报》记者采访时表示,和其他社会人员涉案情况不同的是,若发现学生犯案,有关部门往往会第一时间警示学生,要求其中止与对方联系,而不会刻意放线,这么做“全部是出于对孩子的保护”。

2011年湖南湘潭曾发生一起性质较为严重的策反案,涉案人年仅16岁,但作案情节包括窃取政府文件和为境外间谍传递加密资料。这名安全官员说:“境外间谍机构利用年少懵懂的未成年人去做明确构成犯罪的‘交通’角色,非常恶劣。”

最初,这名涉案的张姓高中生在网上谎称自己毕业于军事院校,境外间谍主动与他接触,要求提供部队内部文件。张某收到对方汇来的400美元后,编造了一份“演习计划”,但难以蒙混过关。张某于是改口称,自己真实的工作单位是教育局,之后根据境外情报机构要求,他先后组织多名同学进入教育局办公室,窃取“红头文件”。

按对方指示,张某开始接收快递包裹,并对包裹内夹藏的存储卡内加密资料进行处理,通过电子邮件发送出去。《环球时报》记者从权威渠道获得的信息显示:这些资料是一名被境外机构策反的我重要单位人员出卖的涉密资料。

案发时,张某总计收取报酬约合人民币2万余元,其行为已涉嫌犯罪。国内有关部门接受《环球时报》采访时表示,考虑到张某年龄较小,希望他能改过自新、拥有未来,“我们在法律允许的范围内对他进行了从轻处理”。

“但任何一个被发现的隐患,无论大小,都必须消除”,上述部门官员对《环球时报》记者强调,国家安全如空气,和每个人相关,须人人有心。

机关单位微信朋友圈里的八项注意

微信目前，微信已经取代短信、电话，成为工作中最常用的沟通方式。

但微信毕竟是新生事物，在工作方式比较严谨和传统的机关单位，使用不当会出现很多问题。很多时候你自己并无意识，却已用微信给别人留下负面印象。这几点一定要注意。

不要滥用截屏截屏

功能与职场大多数礼仪背道而驰。两个人的聊天是非常私密的行为，发送出去与暴露他人和自己的隐私没有区别。在职场上使用微信截图要格外谨慎，不要随意截屏为证，更不可随意把截屏发送给第三者。

反过来说，以现在的技术，除非是腾讯内部调取，其他方式无法验证微信截图真假。所以，微信截图没有任何法律效力。

群里也要讲规矩单位群的感情交流功能相对弱一些，主要是为了工作。所以在工作群里聊天，如果不是工作必要，一定要适可而止。同时，不要随便拉陌生人进入群里，以免泄露工作秘密。

慎用语音

虽然微信交流方式很丰富，有文字、语音、表情等，但交流时对方性格、身处环境、职位高低等都是必须要考虑的。对于那些职位比自己高很多的人，最好的方法是直接电话过去，除非是私下关系极好，一般不要使用语音。为了工作方便和准确无误，在大多数情况下不要使用语音。

注意沟通效率

单位里使用微信沟通，一定要考虑对方处境。比如对方身处领导岗位，事务极其繁忙，这时候切勿使用“看到请回复”“在吗”这些词，要直接切入主题。如果稍微感到沟通效率低下，可马上致电询问。设想沟通对象处境，随时调整沟通节奏，工作会更加顺畅。

区分朋友圈和工作圈

朋友圈是每个人的一张网络面孔。若工作和生活共用一号，一定要注意朋友圈分组。你发了一条在亲戚朋友们看来逗趣的内容，同事老板看到了可能是另一个感受，或许会不知不觉间造成一些误会和偏见。在人际关系和社交工具使用上，一定要因人而异，这一条是常识。

勿滥用私人化表情

对私人化、真人截图等比较特殊的表情的认可，一般限于私人圈子，但在单位群里用可能会使一些人生厌。单位群年龄差异大，不太适宜使用各种怪异表情，你只是想活跃气氛，但实际上是增加了负面印象。

不要处理太复杂的问题

机关工作，准确和效率永远是第一位的，微信的即时性提高了工作效率，但在严谨程度上却是短板。对于复杂问题，不论你是长篇大论还是长谈良久，都很容易出现误解和误判，还是电话或面谈更好。及时回复信息及时回复他人信息是一种美德。

保密要害部门部位的管理要求

中央和国家机关及直属单位保密要害部门部位由各机关单位确定，报国家保密行政管理部门确认；省级机关及直属单位保密要害部门部位由各机关单位确定，报所在省（区、市）保密行政管理部门确认，并报国家保密行政管理部门备案；中央和国家机关下属单位和省级以下机关单位确定保密要害部门部位，应报中央和国家机关保密工作机构或省（区、市）保密行政管理部门审核确认。

保密要害部门部位工作人员上岗前要进行涉密资格审查和保密教育培训，审查合格后签订保密承诺书，并定期进行在岗保密教育培训和考核，不得擅自离岗离职或隐因私出国（境）。

保密要害部门部位应当确定安全控制区域，根据周边环境特点和工作需要，采取电子监控、防盗报警等必要的安全防范措施。同时，确定进入人员范围，安装身份鉴别装置，或采取其他控制人员进入的措施，对工勤人员应严格监督管理。

保密要害部门部位应按照国家保密标准配备保密技术防护设备，对使用的信息设备，特别是进口设备和产品进行保密技术检查检测。保密要害部门禁止使用普通手机。保密要害部位禁止带入手机，确需将专用手机带入的，应经机关单位保密委员会（领导小组）批准，并登记备案。未经批准不得带入有录音、录像、拍照、信息存储等功能的设备。

间谍行为有哪些？这些红线你必须知道

哪些行为属于间谍行为？

《反间谍法》对间谍行为进行明确定义，明确了以下行为属于间谍行为，这是中国首次对具体间谍行为进行法律认定。

1、间谍组织及其代理人实施或者指使、资助他人实施，或者境内外机构、组织、个人与其相勾结实施的危害中华人民共和国国家安全的活动。

2、参加间谍组织或者接受间谍组织及其代理人的任务的。

3、间谍组织及其代理人以外的其他境外机构、组织、个人实施或者指使、资助他人实施，或者境内机构、组织、个人与其勾结实施的窃取、刺探、收买或者非法提供国家秘密或者情报，或者策动、引诱、收买国家工作人员叛变的活动。

4、为敌人指示攻击目标的。

哪些人容易被策反？

据国家安全机关统计，目前被境外间谍机关策反的群体并不罕见，退伍军人、留学生、高校师生、军事发烧友以及军工企业、国防科研单位、政府机关人员等，都是其着重关注的对象。尤其是一些年轻的网友，很可能会在不知不觉中被境外人员利用。近年来，境外间谍情报机关策反活动的目标群体正在由专业人士向普通公民扩展。境外间谍情报机关起初会要求被策反者提供一些简单资料，通过丰厚酬金使其产生金钱依赖，再布置更多的敏感“作业”。

境外间谍情报机关人员大多会用很多身份来伪装自己，如研究人员、学者、军事发烧友等，在勾连网民时往往使用研究所、咨询公司、军事杂志社等各种掩护名义，借助金钱拉拢、资助出国、美女交友诱惑等手段，实施欺骗拉拢。当被策反者表示不愿意再干时，他们就直接威胁：“你已经干了不怕人知道么？”

从披露的案件来看，很少有人会主动去做境外间谍的同伙，往往是掉进了他们布控的陷阱，进而被威胁讹诈。

《反间谍法》规定：“一切国家机关和武装力量、各政党和各社会团体及各企业事业组织，都有防范、制止间谍行为，维护国家安全的义务。”这是从总体上对政府和社会公众维护国家安全的要求，确保积极有效配合专门机关依法开展反间谍工作。同时，还就公民和组织如何履行维护国家安全的基本义务作了具体规定，主要包括：防范、制止间谍行为；为国家安全机关提供便利条件、协助；及时报告、如实提供间谍行为的情况和证据等。

间谍行为该当何罪？

根据我国《反间谍法》的相关规定，如果不明情况，被诱骗落入境外间谍机关的圈套，一定要终止违法行为。如果受到对方威胁，不要害怕，更不要被对方牵着鼻子走。

《反间谍法》第二十七条规定：“实施间谍行为，有自首或者立功表现的，可以从轻、减轻或者免除处罚；有重大立功表现的，给予奖励。”

如果明知对方是间谍还不采取措施，那么不仅危害国家安全，自身也可能付出惨重代价。

依据《中华人民共和国刑法》规定：“以窃取、刺探、收买方法，非法获取军事秘密的”，根据情节严重与否，处以五年以下、五年至十年或十年以上有期徒刑不等的惩罚。如果将军事秘密提供给境外机构，那么将被处十年以上有期徒刑、无期徒刑或者死刑。

间谍窃密案频发！保密管理应该如何做？

近些年来，频发的间谍窃密案件不得不引起我们的警惕。从黄宇案件中，黄宇本人获取国家秘密的途径，我们可以看到保密管理工作的泄密漏洞。

黄宇案是一起特别严重的间谍窃密案，作为一个涉密单位的普通职员，他是如何搜集、获取如此大量的国家秘密信息的呢？

基本案情

黄宇，1974年7月28日出生，四川省自贡市人。1997年7月计算机专业毕业后进入一家涉密科研单位，由于其工作态度不端正，能力平平，业绩一直落后，2004年被解职。为此，黄宇心怀不满，以手中私自留存的保密资料为筹码，主动在互联网上与某境外间谍机构勾联，出卖国家秘密获取经费，终于沦为一名为境外势力效力的间谍。随后，黄宇又通过策反同事，窃取其妻子唐某、姐夫谭某和其他同事的计算机文件资料等手段，在10年里先后向境外提供15万余份资料，其中绝密级国家秘密90项，机密级国家秘密292项，秘密级国家秘密1674项，涉及我密码领域大量机密情报，对我党政军等核心要害部门安全构成了重大威胁。黄宇因“间谍罪”被依法判处死刑，剥夺政治权利终身。唐某、谭某因犯过失泄露国家秘密罪，被分别判处5年、3年有期徒刑，有关单位的29名责任人受到不同程度的处分。

从案例中分析，主要有以下几个途径：

一、在工作中私自留存资料文件

本案中，黄宇2002年首次在网上与境外间谍机构勾联，将手中私自留存的3份有关军用保密机的电子文档拷贝给对方，收取1万美元奖金，后陆续将离职前窃取的国家秘密出卖给境外间谍机构，获取70多万美元间谍经费。保密法第十六条规定，国家秘密的知悉范围应当根据工作需要限定在最小范围。第三十八条规定，涉密人员离岗离职实行脱密期管理。第二十五条对加强机关单位国家秘密载体管理提出了明确要求。

黄宇在涉密科研所工作期间，其知悉并私自留存大量涉密文件资料未被发现，暴露出有关单位存在国家秘密知悉范围确定过于宽泛、国家秘密载体管理过于松懈、涉密人员离职时涉密载体清退不彻底、脱密期监管不到位等问题。

二、伺机复制其妻唐某的涉密文件资料

本案中，黄宇的姐夫谭某与其在同一单位供职，担任总工程师。谭某习惯将单位的资料拷贝到笔记本电脑上，带回家留作备份。有一天，谭某家中的电脑坏了，叫黄宇帮忙修理，黄宇趁其不备，用间谍U盘放置木马程序窃取了电脑里的保密文档。保密法第二十一条规定，国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁，应当符合国家保密规定。第二十六条规定，禁止非法复制、记录、存储国家秘密。

谭某在家中使用的笔记本电脑为单位配发的涉密计算机，则暴露出了有关单位存在涉密计算机未安装安全保密防护设备、擅自携带外出且未按保密要求进行维修等问题；如该笔记本电脑为谭某个人所有，则有关单位的保密管理存在极其严重的泄密隐患。

三、向同事打听消息，获取内部刊物

本案中，黄宇利用在原单位的关系，窃取同事电脑上的资料，向好友郑某等人打探科研动态消息，并利用他人窃取科研所内部刊物。保密法第二十六条规定，禁止在私人交往和通信中涉及国家秘密。第三十二条规定，保密要害部门、部位按照国家保密规定和标准配备、使用必要的技术防护设施、设备。

黄宇离职后，仍能出入该涉密科研所，接触窃取同事电脑上的涉密资料，其好友郑某还将科研动态消息、内部刊物等私下透露给黄宇，暴露出有关单位涉密人员保密意识不强，要害部门部位或涉密场所人防、物防、技防措施不到位等问题。

间谍窃密案的发生，往往被认为是某个人的

思想出了问题，私欲熏心，投敌卖密。但从以上分析不难看出，我们一些涉密单位在保密管理中存在的严重漏洞，为这些别有用心之徒提供了便利，间接导致了大量国家秘密信息被窃取。

启发建议

纵观黄宇案始末，应当从以下四方面入手，筑牢保密工作防线。

1、从宣传教育入手，提高全民保密意识

国家秘密关系国家安全和利益，保密教育首先是爱国主义教育，保守国家秘密是每个公民的义务，任何危害国家秘密安全的行为，都必须受到法律追究。

当前，党政机关、涉密单位的工作人员可以通过各种渠道接受一定程度的保密教育，而广大公民接受保密知识普及和保密意识培养的渠道、教育体系尚不完善，亟须加强。首先，应当广泛综合运用电视、网络、微信等媒体平台宣传保密知识，加强对典型案例的报道，以案为鉴，以案说法，增强公民的敌情意识和保密意识。其次，逐步将保密法及其实施条例等保密教育内容纳入国民教育，从小抓起，形成体系，提升全民的保密知识和保密技能水平。最后，继续强化党政机关、涉密单位工作人员的“两识”教育，对涉密人员严格执行岗前审查、持证上岗、在岗培训、离岗管理等保密要求，努力确保涉密人员的思想过硬、忠诚可靠。

2、从核心重点入手，强化涉密载体管理

保密管理的核心是确保国家秘密安全，做好保密工作重点是管好用好国家秘密载体。按照国家秘密载体的存在方式，主要分为纸介质、光介质、电磁介质等载体。

一是管好纸介质国家秘密载体。重点是严格执行国家秘密载体保密管理规定，对纸介质文件资料从制作、收发、传递、使用、复制、保存、维修和销毁进行全生命周期的闭环管理模式，做好文字记录并存档备查。二是管好光介质、电磁介质等国家秘密载体，包括涉密信息系统、涉密移动存储介质等。重点是按照保密要求建设涉密信息系统，经测评后投入使用（单机应采取防护措施）；对涉密移动硬盘、U盘、光盘等移动存储介质登记编号、统一发放、定期检查、集中管理；禁止在任何非涉密设备（含计算机、网络、移动存储介质、手机等）中存储、处理涉密信息；涉密介质的维修、销毁要符合保密要求。三是管好保密要害部门部位。保密要害部门部位是保密管理的重中之重。保密法规定，机关单位应当将涉及绝密级或者较多机密级、秘密级国家秘密的机构确定为保密要害部门；将集中制作、存放、保管国家秘密载体的专门场所确定为保密要害部位。重点是强化“三铁一器”等防护措施，要对进入人员进行严格审批管控。

3、从保密自查入手，及时堵塞泄密漏洞

保密自查是机关单位及时发现存在问题，采取防范措施，消除泄密隐患，防止泄密窃密事件发生的重要手段。

自查中应注意3个重要环节，确保检查质量和效果。一是组织实施。大部分机关单位的保密办虚设，人员较少，难以独立完成检查（特别是技术检查）。建议层层抓落实，充分调动基层单位开展自查的积极性。对自查发现问题的，应予以表扬并指导整改；而对保密办抽查发现问题的，应给予通报并严肃处理。二是整改落实。整改落实是保密检查工作成果的具体表现。建议在自查结束后，及时认真总结发现问题，制定有效整改方案，并监督整改落实，形成保密工作长效机制。三是违规处理。建议对三令五申、屡教不改的违反保密法律法规问题，依法依纪严肃查处并通报批评，充分发挥案件的警示震慑作用。

4、从技术防护入手，降低人为窃密风险

间谍窃密案往往是内部人员被境外策反，监守自盗，防不胜防。在科技高速发展的今天，计算机信息系统、网络已经逐渐替代了传统的纸质传递方式，应当充分利用现代计算机技术成果，探索建立一套以加密处理、权限控制、文件密钥和非法获取自毁等防护措施的涉密公文运转体系。

涉密文件一经产生，就在确保安全的信息系统中流转，任何人无法使文件脱离系统，从而使涉密信息存在于客观的安全系统环境之内。改变现有依靠涉密人员自觉执行制度达到保密目的的被动现状，实现客观层面的主动安全，减少人为因素，防止境外通过策反内部人员即形成“无密可保”的被动局面。通过加强技术防护与监管，提高窃密成本与风险，时刻提醒那些别有用心的人“伸手必被捉”。

如何复制、复印、摘抄、汇编涉密载体

对国家秘密载体的管理，保密法中作了原则性规定，保密法实施条例中也有相关规定。根据这些规定，绝密级文件，非经原确定密级的机关单位或者上级机关批准，不得复制和摘抄。复制、复印、摘抄、汇编机密级和秘密级文件，必须经过批准并履行审批手续。复印、复制本机关本单位产生的密件，应当经本机关本单位主管领导批准；复印、复制上级机关下发或其他机关单位制发的密件，应当经制发机关批准。复印、复制密件不得改变其原定的密级和保密期限。复印、复制件须编制序号，控制发放范围，采取与原件同样的保密管理措施。

涉密文件、资料未经批准不得擅自汇编。汇编的密件，属于本机关本单位产生的，必须经单位主管领导批准；属于上级机关下发或者其他单位产生的，必须经发文机关单位同意。收录汇编的密件，应当分别标明原有密级和保密期限。汇编本封面应当按照收录密件的最高密级和最长保密期限标注。密件汇编应当按照其中最高密级的文件所限定的范围发放，不能擅自扩大范围；确需扩大发放范围的，应当经密件制发单位同意。密件汇编应当按照密件的保密要求进行管理。

如何开展保密监督检查工作

工作中，保密干部通过开展保密监督检查，督促、指导、推动机关单位履行保密工作职责，正确开展保密工作，保证各项任务和措施要求落实到位，确保国家秘密安全。保密监督检查工作体现在两个方面，一是指导各个机关单位开展自查自纠工作；二是直接组织开展保密检查活动。保密检查要有目的性，即明确保密检查的目标、项目，又要有计划性和针对性，即制定具体的有操作性的保密检查方案；还要严格监督检查程序，即严格按照规定的步骤、方法、方式、时间和设备使用规定开展检查活动。

保密检查是现代保密管理体系的重要组成部分，作为一项综合性的保密管理手段，保密检查在现代保密管理体系中既相对独立，又对各方面、各环节产生重要作用。邓小平同志曾经指出："保密委员会要搞个班子，搞十几、二十几个政治可靠、懂得科学技术的干部，天天检查找岔子。"应当说，保密检查不仅是为了发现问题，更要通过发现问题，解决问题，发挥以查促教、以查促改、以查促防、以查促管作用。通过组织开展保密检查，可以有效促进保密法规制度的贯彻落实，督促机关单位加强保密管理。作为一种执法手段，保密检查必须依法进行，无论是在依据还是内容上，都要在法定范围内进行。

如何开展保密科技工作

保密科技工作包括4个方面：一是制定保密科学技术发展规划、计划和政策性措施，制定保密技术标准；二是确定保密技术研究开发方向和具体项目，组织和管理保密科学技术研究开发活动，对研究项目进行审查论证，推进科技研究成果转化；三是组织保密科学技术的推广应用和重点保密技术装备配备；四是为党政领导机关和本地的重大涉密会议、涉密活动提供保密技术支持和服务保障。

开展保密科学技术工作，要密切关注国内外相关技术发展应用的调研和情报信息的收集分析，紧盯信息化建设的发展现状和趋势，着眼于信息安全保密需求，着力于保密技术抗衡和防护能力的形成。担负保密科技工作的干部，既要具备一般保密干部的素质要求，又要懂得相关领域特别是信息技术领域的基本知识。

商业秘密与国家秘密有哪些联系和区别？

商业秘密与经济、科技领域中的国家秘密，都是具有保密价值的信息，二者间是互相联系、互可转变的。国家秘密在一定条件下可以转变为商业秘密，商业秘密也可以转变为国家秘密。例如，随着时间的推移，生产发展了，科技进步了，有些经济、科技领域的国家秘密会失去其国家秘密属性，此时的国家秘密就可能转变为商业秘密。又如，企业开发、研制属于商业秘密的科技项目，对国防军事有着巨大的潜在价值，具有国际领先水平，或对国民经济产生重大影响，在这种情况下，商业秘密就“关系国家安全和利益”了，就要确定为国家秘密。

商业秘密与国家秘密的区别主要表现在以下四个方面：

1、涉及的利益不同。国家秘密关系国家安全和利益，其内容涉及国家的政治、军事、外交和外事、国民经济和社会发展、科学技术、国家安全和刑事司法等领域。国家秘密一旦泄露，会使国家的安全和利益受到损害。而商业秘密仅仅是涉及权利人经济利益和竞争优势的信息，其内容也局限于与科研、生产、经营有关的技术信息和经营信息。商业秘密一旦泄露，损害的是商业秘密权利人的利益。

2、确定的程序不同。国家秘密必须依照法定的程序确定，依据国家有关部门保密范围的规定，确定国家秘密及其密级。商业秘密的确定没有法定的程序，只要符合商业秘密的基本条件，权利人又采取了合理的保密措施，就可以受到法律的保护。

3、处置权不同。国家秘密是一种公权，而商业秘密属于私权。国家秘密未经法律授权的机关审查批准，任何人不得擅自对外提供或转让。而商业秘密只要权利人自己决定，就可以参与市场交易，进行有偿转让或随意转让给他人，除非这种转让会对他人的权益或公共利益造成损害，否则是不受法律限制的。

4、法律责任不同。国家秘密一旦被泄露，损害的是国家的安全和利益，侵害的是国家的保密制度，对泄密行为人必须依照法律、法规追究其刑事责任或行政责任。商业秘密一旦被泄露，商业秘密的权利人可以追究侵权人的法律责任，也可以不追究其责任。

涉密场所的声、光、电磁防护

涉密场所常见的窃听方式包括：有线搭线窃听、无线窃听（包括无线窃听器、手机窃听、智能终端窃听等）、激光探测窃听、定向探测窃听等。防止有线窃听，可通过建设专用电话网、采用光纤传输等方式进行防范；防止无线窃听，可通过建设电磁屏蔽室等方式进行防范；防止激光窃听，可通过加装能够阻挡激光的遮盖物或安装语音干扰装置等方式进行防范；防止定向窃听和振动窃听，可通过限制声源大小、实施隔声防护和管道消声、布置声掩蔽装置等方式进行防范。

涉密场所常见的窃照方式包括：间谍卫星窃照、高空侦察机窃照、照相器材窃照、手机窃照和专用小型设备窃照等。针对间谍卫星、高空侦察机对场所景象、建筑布局结构、大型设备等的窃照，可采取伪装技术手段进行防范；针对照相器材、手机、专用小型设备等的窃照，可采取出入口控制（门禁）、视频监控等控制手段和微型电子设备检测、金属探测等检查手段进行防范。

涉密场所常见的电磁泄露发射方式包括：传导发射、辐射发射、耦合发射等。针对电磁泄露发射，涉密设备分散、涉密程度高的场所，可采用低泄射计算机进行防护；涉密设备集中、涉密程度高的场所，可采用建设电磁屏蔽室、配置电磁屏蔽机柜的方式进行防护；处理机密级及以下密级信息的设备，可采用配备视频干扰器的方式进行防护。

涉密计算机启用前，应进行保密技术检测。其中的数据加密设备和加密措施，必须是经国家密码管理局批准的。涉密计算机应按照所存储、处理信息的最高密级管理，并登记在册，不得擅自卸载、修改涉密计算机安全保密防护软件和设备，不得接入互联网等公共信息网络，不得使用无线网卡、无线鼠标、无线键盘等设备。

涉密计算机应严格按照国家保密规定和标准设置口令。处理秘密级信息的计算机，口令长度不少于8位，更换周期不超过1个月。处理机密级信息的计算机，应采用IC卡或USB Key与口令相结合的方式，且口令长度不少于4位；如仅使用口令方式，长度不少于10位，更换周期不超过1个星期。处理绝密级信息的计算机，应采用生理特征（如指纹、虹膜）等强身份鉴别方式，也可采用IC卡或USB Key与口令相结合的方式，且口令长度不少于6位。涉密计算机口令设置，应采用多种字符和数字混合编制。

涉密计算机的保密管理

涉密计算机的软硬件和保密设施的更新、升级、报废等，必须进行保密技术处理。改作非涉密计算机使用，应经本机关本单位主管领导批准，并采取拆除信息存储部件等安全技术处理措施。不得将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或改作其他用途。拆除的部件如作淘汰处理，应严格履行清点、登记手续，交由专门的涉密载体销毁机构销毁。自行销毁的，应当使用符合国家保密标准的销毁设备和方法。

涉密计算机如何设置口令字？

口令字是计算机及其信息系统的第一道安全防线，涉密计算机信息系统通过口令字验证用户身份，区分和控制访问权限。计算机口令字设置如果达不到足够长度，非常容易被破解。口令字一旦被破解，破解者就可以冒充合法用户进入涉密计算机任意获取信息。涉密计算机应严格按照保密规定设置口令：处理秘密级信息的口令长度不少于8位，更换周期不超过1个月；处理机密级信息的口令应采用IC卡或USB?Key与口令相结合的方式，且口令长度不少于4位；如仅使用口令方式，则长度不少于10位，更换周期不超过1个星期；设置口令时，要采用多种字符和数字混合编制。处理绝密级信息的口令应采用生理特征（如指纹、虹膜）等强身份鉴别方式。

提示

我有关部门检测发现，境外情报机构常利用“口令破解”技术手段，有组织地对我重要涉密信息网络进行大规模入侵攻击，迅速破解我信息网络用户不够长度的口令字，以控制涉密计算机，窃取大量涉密文件、资料，造成非常严重的后果。

涉密人员的定义

按照保密法及其实施条例规定，在涉密岗位上工作的人员为涉密人员。机关单位按照涉密程度的不同，确定涉密人员的类别，实行分类管理。

1、核心涉密人员。日常工作中产生、经管或者经常接触、知悉绝密级国家秘密事项的岗位为核心涉密岗位，在核心涉密岗位工作的人员为核心涉密人员。

2、重要涉密人员。日常工作中产生、经管或者经常接触、知悉机密级国家秘密事项的岗位为重要涉密岗位，在重要涉密岗位工作的人员为重要涉密人员。

3、一般涉密人员。日常工作中产生、经管或者经常接触、知悉秘密级国家秘密事项的岗位为一般涉密岗位，在一般涉密岗位工作的人员为一般涉密人员

涉密人员的权利

涉密人员的权利，是指其在处置、管理国家秘密的过程中，为确保国家秘密安全，合法行使的权力和应当享受的利益。涉密人员主要享有以下权利：

要求配备保密设施设备的权利。

涉密人员有权要求所在单位为其履行保密义务、保守国家秘密提供必需的物质保障和工作条件（如提供保密室、保险柜、运送涉密载体的交通工具），提供处理涉密信息所需的保密技术装备等。

参加保密教育培训的权利。

涉密人员有要求参加保密知识培训、学习等受教育的权利。其所在机关单位应当提供机会，满足其合理要求，提供必备的条件。

行使保密监督的权利。

涉密人员对所在机关单位乃至党的保密组织、保密行政管理部门的工作，有权提出建议、意见和给予批评。有权对本机关本单位人员，包括领导干部故意或者过失违反保密规定的行为予以制止、批评、帮助。

获得补偿的权利。

涉密人员为保守国家秘密做出重大贡献，有获得精神和物质奖励的权利。涉密人员为保守国家秘密，放弃个人正当权益的（如不能自由择业、科研成果论文涉及国家秘密而不能公开发表等），有关部门和政府应当按照规定予以补偿。

申诉和控告的权利。

涉密人员为履行职责，确保国家秘密安全，提出正当工作要求，而受到不公正待遇；或因坚持原则，制止违反保密法规和保密纪律的行为，而受到打击报复；或根据政策规定提出正当的补偿要求，而得不到解决时，有权向上级机关或纪检、监察机关，或保密工作部门提出申诉和控告。有关机关应当受理其申诉和控告，并对涉密人员的正当权益予以保护。

涉密人员的义务

涉密人员的义务，是指涉密人员在保守国家秘密、维护国家安全和利益方面，依照法律规定应尽的责任。我国保密法律、法规和规章中关于保密制度的一系列规定，构成了涉密人员保密义务的基本内容。

1、采集、制作、收发、使用、管理、传输、存储、销毁涉及国家秘密的信息及信息载体，必须严格执行相关保密管理规定，不得泄露国家秘密。

2、不得以任何方式私自对外提供国家秘密载体和涉密信息。向新闻出版媒体部门投寄稿件、接受采访不得泄露国家秘密。不得向境外组织、机构和人员投寄含有国家秘密信息的稿件和其他类型的作品。

3、未经主管部门批准，不得私自出境，或弄虚作假以其他身份出境。经批准同意出境的，不得与境外组织、机构和人员有非组织交往行为，不得滞留境外不归。

4、不得在私人交往、通信、谈话和家庭生活等个人活动中泄露国家秘密。不得将涉密载体带回家中。不得用普通通信设备传输涉及国家秘密的信息。不得带无关人员进入涉及国家秘密的保密要害部门部位。不得在公共信息网络上处理涉及国家秘密的信息。

5、不得擅自离职，经批准辞职、离职或正当退休的，必须自觉清理并向单位交还全部国家秘密载体。在脱密期内，不得私自出境，不得应聘到境外组织、机构任职。

6、发生违反保密规定的行为，应当及时自我终止；泄露国家秘密的，应及时向单位报告并采取补救措施，不得对单位隐瞒自己的泄密行为和泄密事实。

7、发现他人违反保密规定，实施泄露国家秘密行为的，要及时予以制止，并向组织及时报告。拾得国家秘密载体，应及时就近交给国家保密工作部门或其他有关国家机关，不得私自处理。发现国家秘密载体安全保密受到威胁时，要奋力抢救，确保国家秘密的安全。

8、自觉接受保密教育和保密监督检查。

涉密人员离岗、离职有哪些保密要求

涉密人员离岗、离职，应清退涉密载体、签订保密承诺书，接受脱密期管理。

涉密人员离岗、离职要清退涉密载体。包括个人所持有和使用的国家秘密载体和涉密信息设备，如文件资料、软盘、U盘、光盘、涉密信息设备等。移交时，必须认真清理清点，登记在册，办理移交手续，并作为办理离岗、离职手续的条件。

涉密人员离岗、离职要签订保密承诺书。保密承诺书应明确涉密人员离岗、离职后应履行的保密义务以及违反承诺应承担的法律责任。

涉密人员离岗、离职要接受脱密期管理。脱密期内，未经审查批准，不得擅自出境；不得到境外驻华机构、组织或者外资企业工作；不得为境外组织人员或者外资企业提供劳务、咨询或者服务。一般情况下，核心涉密人员脱密期为3—5年，重要涉密人员脱密期为2—3年，一般涉密人员脱密期为1—2年。脱密期自机关、单位批准涉密人员离开涉密岗位之日起计算。对特殊的高涉密人员，可以依法设定超过上述期限的脱密期，甚至在就业、出境等方面予以终身限制。

涉密人员离岗（离开涉密工作岗位，未离开本机关、本单位）的，脱密期管理由本机关、本单位负责。涉密人员离开原涉密单位，调入其他涉密单位的，脱密期管理由调入单位负责。涉密人员被解聘或者本人提出辞职的，应先调离涉密岗位，在本单位履行脱密期后再行办理解聘、辞职或调离手续。涉密人员退休的，由原机关、单位负责脱密期管理。属于其他情况的，由保密行政管理部门或者公安机关负责。

涉密人员如何分类

涉密人员分类，是指将在不同涉密岗位工作的人员分为核心涉密人员、重要涉密人员和一般涉密人员。

《保密法》第三十五条规定，在涉密岗位工作的人员，按照涉密程度分为核心涉密人员、重要涉密人员和一般涉密人员，实行分类管理。

目前，对涉密人员的分类主要依据涉密岗位的不同进行。涉密岗位，是指在日常工作中产生、经管或者经常接触、知悉国家秘密事项的岗位。日常工作中产生、经管或者经常接触、知悉绝密级国家秘密事项的岗位为核心涉密岗位；日常工作中产生、经管或者经常接触、知悉机密级国家秘密事项的岗位为重要涉密岗位；日常工作中产生、经管或者经常接触、知悉秘密级国家秘密事项的岗位为一般涉密岗位。在上述岗位工作的人员分别为核心涉密人员、重要涉密人员和一般涉密人员。机关、单位应根据有关规定和工作实际，制定具体划分标准和管理办法。

《保密法》第三十六条规定，涉密人员上岗应当经过保密教育培训，掌握保密知识技能，签订保密承诺书，严格遵守保密规章制度，不得以任何方式泄露国家秘密。

涉密网络中使用的设备、软件应当满足哪些保密要求？

需要选用进口设备的，应进行详细调查和论证并进行必要的检测，不得选用国家保密行政管理部门规定禁止使用的设备或部件。?涉密网络中的安全保密产品，应选用经过国家保密行政管理部门授权的检测机构测评，确认符合国家保密标准要求的产品，计算机病毒防护产品应选用公安机关批准的国产产品，密码产品应选用国家密码管理部门批准的产品。

涉密人员上岗有哪些保密要求

涉密人员上岗应接受任前审查、上岗培训，并签订保密承诺书。

涉密人员上岗应经过严格审查。机关、单位任用、聘用涉密人员应当由组织人事部门会同保密工作机构，依据涉密人员任职条件进行审查。审查内容主要包括：个人和家庭基本情况、现实表现、主要社会关系，与国（境）外机构、组织、人员交往等情况。

涉密人员上岗应当经过保密教育培训。机关、单位任用、聘用涉密人员必须坚持先培训、后上岗，应当根据涉密岗位的工作性质、涉密范围和特点，结合实际工作需要，对拟任用、聘用的涉密人员进行有针对性的岗前保密教育培训。

《保密法》第三十六条规定，涉密人员上岗应当经过保密教育培训，掌握保密知识技能，签订保密承诺书，严格遵守保密规章制度，不得以任何方式泄露国家秘密。

涉密人员上岗应签订保密承诺书。上岗前签订保密承诺书，对于增强涉密人员保密意识、强化保密责任具有重要意义。保密承诺书的主要内容包括：了解并遵守各项保密制度，知悉并履行保密义务，自愿接受保密审查，承担法律责任等。机关、单位应当把保密承诺书的签订和管理作为一项经常性工作来抓，建立健全保密承诺长效管理机制。同时，可结合工作实际，根据涉密人员的涉密事项和涉密程度，适当补充相关内容或组织签订专项保密承诺书。

涉密文件资料的立卷、归档

涉密文件资料的立卷、归档工作，主要是按照档案法及其配套的法律法规和档案主管部门的要求办理。涉密文件资料在立卷、归档或者向档案馆移交时，应当对其密级和保密期限重新鉴定。属于本机关本单位产生的密件，凡是可以解密、降密或变更保密期限的，应当按照保密法规规定的程序进行解密、降密和变更保密期限，再移交档案馆馆藏。不属于本机关本单位产生的密件，原产生机关单位未作出解密、降密和变更保密期限决定的，不得擅自变更密级和保密期限。已经立卷、归档的密件，保密期限届满的，应当及时解密。

需要立卷、归档的密件，在立卷、归档时经鉴定仍然属于国家秘密的，应当在档案卷宗封面或者首页上做出与卷内密件密级和保密期限相同的标志。卷内有多份密件的，卷宗封面或者首页按最高密级和最长保密期限做出标志。

非档案管理人员查阅涉密档案，应当办理批准手续，并严格控制接触范围。关于馆藏涉密档案的密级及保密期限的变更和解密以及如何控制使用范围的问题，应按国家保密局和国家档案局制定下发的《各级国家档案馆馆藏档案解密和划分控制使用范围的暂行规定》办理。

涉密载体为什么不能随意交他人保管和处理？

使用、处理和保管涉密载体是工作需要的职权行为，随意将涉密载体交给不属于知悉范围内的人员保管和处理，是擅自扩大国家秘密知悉范围的违规行为，容易造成涉密载体失去有效控制，从而导致泄密事件的发生。

涉密载体的销毁

所有涉密载体均不得擅自销毁，严格禁止将涉密载体作为废品出售。销毁涉密载体应当符合《国家秘密载体销毁管理规定》，使用符合国家保密标准的销毁设备和方法，确保国家秘密信息无法还原。“无法还原”是指载体销毁后形成的残留物或残片上不存在可以读取的任何涉密信息，而且采用现有的技术措施无法恢复。

涉密载体销毁的基本程序：送销前，机关单位应当认真履行清点、登记手续，报机关单位主管部门审核批准，并存放在符合安全保密要求的专门场所。送销时，机关单位应当分类封装、安全运送，并派专人现场监销。需要注意的是，涉密载体必须送交专门的销毁工作机构或者保密行政管理部门指定的承销单位销毁，禁止送交其他任何单位销毁。实际工作中，一些机关单位会有少量密级较高、需立即销毁的涉密载体，可自行组织销毁，但必须严格履行清点、登记和审批手续，并使用符合国家保密标准的销毁设备和方法。机关单位自行销毁使用的设备应通过保密行政管理部门的检测。

涉密载体必须送交专门的销毁工作机构或者保密行政管理部门指定的承销单位销毁，禁止送交其他任何单位销毁

涉密载体销毁的登记、审批记录应当长期保存备查。

如何开展定密监管工作

定密监管主体主要包括三类：一是定密的机关单位，包括党政领导班子和保密组织机构。二是定密机关单位的上级机关和业务主管部门。三是保密行政管理部门。定密监督是保密行政管理部门的法定职责之一。监管主体开展定密监督，应当重点检查是否存在越权定密、定密不准、定密程序不规范、标志不规范、没有及时变更和解密等行为。

保密行政管理部门的定密监管责任包括：有计划地组织定密专业人员进行业务培训，组织开展定密工作理论研讨活动和编写定密工作培训教材资料；对所辖区域内各机关单位的定密工作进行业务指导；对各机关单位落实定密制度的情况进行检查验收；协调解决国家秘密事项范围执行中存在的疑难问题；掌握所辖区域内各系统或行业国家秘密事项的分布和动态变化情况，做好定密统计和分析工作；通报本地区定密工作情况，总结推广本地区有关机关单位的定密工作经验做法；纠正和查处定密工作中的错误或违法违规行为。

为什么不能将他人的文件、资料随意拷贝到涉密计算机上？

他人的计算机或U盘可能连接过互联网并被植入特种“木马”间谍窃密程序或感染了病毒。如果随意将他人计算机或U盘上的文件、资料拷贝到涉密计算机上，极有可能使涉密计算机被植入窃密程序或感染计算机病毒。

为什么不能在政府门户网站上登载涉密信息？

政府门户网站是供政府信息公开使用的网络平台，是政府面向社会开放的信息窗口。政府门户网站是与互联网相连接的开放信息网络，在政府网站登载涉密信息，实际上就是将涉密信息放在互联网上。

手机上网的泄密风险

随着信息技术的飞速发展，移动互联网已经渗透到我们日常工作生活的方方面面。通过移动互联网，人们可以很方便地获取信息，但也可能随时泄露信息。在这种背景下，每一名党政机关工作人员都应该具有防范泄密的常识。

1、认识误区

当前，手机和移动互联网已经成为人们工作生活中不可或缺的一部分。很难想象，不上网、不用手机，我们的工作生活会变成什么样。但是，人们对手机和移动互联网的认识普遍存在以下几个误区：

移动互联网应用是“免费的”。我们使用各种各样的APP（平板电脑、手机等移动设备上的第三方应用程序）从来没有付费的习惯，也把这种免费当成必然。但天下从来就没有“免费的午餐”，当你使用社交、网购、导航、杀毒、交通、娱乐等免费APP的时候，你个人的数据就已经成为这些应用软件厂家的囊中之物。可以这么说，移动互联网时代的免费盛宴是以广大用户牺牲个人隐私数据的方式换来的。

个人信息并不重要。很多人都有这样的经历，某个网站或APP注册就有奖励，为了礼券或者折扣很轻易就填写了自己的手机号、身份证号、居住地址等信息。殊不知，这些真实的信息，捅破了网络世界和真实世界之间的“窗户纸”，让我们不知不觉沦为了信息时代的“透明人”。

个人信息与单位安全保密无关。很多人觉得手机是跟朋友、同事和家人沟通的私人物品，还有各种各样的APP，与单位的保密工作无关。实际上，在大数据时代，大量个人单条、孤立信息的汇聚，能把我们工作的特点规律勾勒出来。如果不注意，就会对单位安全保密造成威胁。因此，从这个意义上来讲，保护个人信息就是保护国家安全。

2、泄密风险

移动互联网的特点是无线高速上网。手持多媒体智能终端，就可以时时处处在线，信息获取、处理、分发瞬间完成。这使得机关单位传统的安全保密措施受到很大挑战。所以说，移动互联网是把“双刃剑”，在给人们工作生活带来便利的同时，也存在泄密的风险。

个人无意中泄密。前面已经提到，平常通过智能终端，连接移动互联网，使用各种APP，我们留下了大量个人信息。手机厂商、电信运营商、应用开发商、安全厂商以及手机操作系统提供商，几乎所有的移动互联网产业链参与者，出于各种各样的目的，都在大量收集用户信息。这些信息是大数据分析的基础。由于这些信息涉及个人隐私和工作内容，所以一旦泄露，将对单位的安全保密工作带来巨大威胁。以手机通信录为例，实际上它是一个人社会关系的描述。通过分析联系人信息，就可以把一个人的工作关系、朋友关系和亲属关系分析得清清楚楚。再结合位置信息判定用户的单位地址、家庭住址，进而确定用户的身份，直至锁定目标，进行全面的信息监控。

木马病毒窃密。由于移动互联网的开放性，使用智能终端所面临的各种木马病毒威胁，比有线网络中的个人电脑平台要严重得多。目前智能终端的主流操作系统Android、iOS和Windows，都不同程度存在着漏洞和后门，使系统可能遭受攻击。针对手机的攻击手段可谓花样百出，如彩信植入恶意链接、采用钓鱼WiFi引诱用户无线联网、通过二维码扫描传播恶意程序等。这些恶意软件轻则带来垃圾信息、盗用用户流量、吸取用户话费，重则把手机变成窃听器、窃照器，大肆窥探用户隐私，甚至对用户进行全面监视，直至盗取用户网络支付信息和银行账户资金。

外国情报机构窃密。“棱镜计划”暴露后，人们才知道某国国家安全局“碟火”项目每天收集大约两亿条短信信息、50亿条手机定位记录；人们也才知道，很多重要的互联网企业都是某国国家安全局的合作伙伴，他们为某国的情报部门服务，为政府部门提供数据和访问便利。而相关企业几乎垄断了当前智能终端的操作系统，借助这样的便利，他们可以轻而易举地收集用户信息。

微信为何成了泄密渠道？

当前正在处于互联网信息高速发展的时代，特别是微信等综合移动社交媒体平台的兴起，给我们的工作和生活带来很大便利，同事也给保密工作带来严峻挑战。

微信为何成泄密新渠道

微信等社交软件具备使用人员多、传播速度快覆盖范围广等特点，一旦发生泄密，涉密信息往往激素扩散，事态难以遏制，危害十分严重。微信之所以能够成为泄密渠道，主要源于以下几个原因。

一是智能手机的普及。随着信息化的发展，手机已逐渐成为人们工作、生活中必不可少的工具之一。而微信以手机为载体存在，打破了电话和短信等常规、传统的人际交往和交互模式，沟通交流更为便捷。据保守估计，全国微信用户群体已超过6亿，这也给保密监管工作出了难题。

二是内置功能的强大。微信支付支持发送语音、视频、图片和文字，群聊、群发和朋友圈等方式进一步满足了受众群体的各种交流互动和娱乐需求，使微信变成了“电子社区”。

三是缺少必要的审核。微信具有即时语音聊天、多人群聊、查找陌生人、摇一摇等强大的交互功能，且用户未采用实名制，无法根据简单的用户资料判定身份，在使用过程中很容易泄露个人隐私、工作甚至国家秘密。而且信息的发布简单不需要审核，所有人都可以浏览、转发，国家秘密一旦被泄露，就会在极短的时间内在极大的范围内新型传播，导致事态失控。

如何防范微信泄密隐患

防范微信泄密，当从一下几个方面做起。

一是加强保密教育，强化保密意识。保密管理，人是根本。微信仅仅是一款便利大家沟通的社交工具，泄密与否关键在于使用者。要有效杜绝失泄密事件，还是要从管“人”这个根本入手，在走“心”上下功夫。不仅要加强涉密人员的保密教育，也要加强机关干部和社会人员的教育。

二是狠抓制度建设，落实保密责任。各机关单位要狠抓保密制度落实。在涉密文件的传阅、使用、保管、销毁等工作中，必须要严格遵守各项保密管理规定，严禁擅自扩大传阅范围，确保涉密文件安全，更要把执行各项保密要求转化为落实保密责任的具体行动，维护制度的强制力和权威性。对违反保密法律法规，造成泄密的，严格追究党政纪政责任，对情节严重的还要追究刑事责任，坚决遏制微信泄密事件的高发态势。

一个个典型案例，一次次深刻教训，让我们知道保密有“底线”“红线”，要守住“底线”，把住“红线”，严格涉密信息传递范围，时刻提醒保密人员“泄密就在瞬间”，必须从小事做起，不可马虎大意，真正把保密意识内化于心，外化于行。

从这个角度来看，目前广泛使用的智能手机简直就是为我们量身定制的窃密终端。

3、如何防范

对于使用移动互联网存在的风险，我们没必要因噎废食，但作为党政机关工作人员，必须采取相应的防范措施。

首先，要遵守单位保密工作部门所有相关规定和要求。比如，不在手机中谈论涉密事项、不处理敏感信息，在保密要害部位和涉密活动中不使用手机等。这些规定和要求，都是保密工作部门根据当前威胁设定的防范底线，必须严格遵守。在当前的形势下，各种攻击窃密手段远远超乎一般人的想象，切勿掉以轻心。

其次，在使用移动互联网时要保护好个人信息。尤其是党政机关工作人员，因为身份特殊，应避免在网络应用中泄露个人信息和工作内容。如，微信、微博中不谈论、分享工作内容；不使用线上到线下的互动式应用（比如网购），以免被锁定网络和真实身份；不使用云服务存储个人生活和工作信息。

最后，使用手机要采取防范措施。如，尽量使用国产手机；关闭手机系统设置中的自动备份、位置跟踪等监控类功能；不在机场、车站、宾馆、餐馆等公共场所连接WiFi；关闭蓝牙等无线数据连接设置；只在正规可靠的应用电子市场下载APP等。

小心您身边的信息陷阱！

相信大多数人都收到过类似“测一测”的链接或分享，例如：“输入姓名测桃花运”“输入手机号码测今生最缺什么”“输入身份证号码看看你的前世是谁”等。然而，笔者想提醒的是，如果你按照上述要求输入了相关信息，你就已经上了圈套。

时下，类似“输入XX信息，测一测你的XX”的网页链接，以各种花样频频出现在我们的社交平台和网络上，这些链接总能以人们感兴趣的话题吸引人们输入个人信息，有的甚至要求分享后才能得知结果。很多人并不认为这有什么不妥之处，因为觉得不管反馈的结果有没有用，都没有任何损失，无非是消遣娱乐罢了。

然而事实上，并不是所有的链接都是娱乐性质的，有的很可能是专门为套取个人信息而设下的陷阱。

大家只要稍加观察就会发现，无论网上“测一测”的话题是什么，基本都要求输入诸如姓名、生日、手机号等信息，有的还会以方便发放奖金奖品为由，要求留下通信地址甚至身份证号。

万变不离其宗，这一切的矛头都指向一处：个人信息。你也许好奇，他们拿这些信息来做什么？

据统计，在我国，绝大多数公民的各类密码都是由姓名、生日、纪念日、电话号码等与个人息息相关的信息构成，只是组合的方式和复杂程度不同而已。

通过收集个人信息，可以大大降低破解其各类账号密码的难度，如社交软件QQ、微信、微博等密码，此外还有信用卡、支付宝、网银等密码。同时，这些个人信息还可以作为“商品”在网上出售，严重影响公民的人身和财产安全。近年来频发的电信诈骗案件就与公民个人信息泄露有很大关系。然而，这些问题还不是最可怕的。在大数据时代，对一个国家公民基础信息的收集、分析和整理，通常可以得出许多十分有价值的推论，如根据一个国家或地区人口的年龄结构、知识结构、消费水平，甚至可以推算出这个国家或地区的劳动力水平、战斗潜力等。因此，只要对个人信息数据进行充分挖掘和分析，必然可以归纳总结出大量有用的数据信息，这对一个国家而言，显然是很大的安全隐患。

因此，不论是出于个人的人身财产安全考虑，还是站在国家安全的层面上，都不能小看个人信息泄露这个问题，更不能抱着“明知会泄露还去试一试”的无所谓心态随性而为。

保守国家秘密，要从保护个人信息做起。在提供个人信息前一定要三思而后行，避免落入别有用心之人设下的“华丽”陷阱。

携带涉密载体外出有哪些保密要求？

一般不要携带涉密载体外出。确因工作需要携带外出的，须经机关、单位主管领导批准，并采取严格的保密防护措施，使涉密载体始终处于本人有效监控之内。

禁止携带绝密级涉密载体外出。确因工作需要携带的，须经本机关、本单位主管领导批准，并严密封装，至少应有两人同行。

参加涉外活动时，不要携带涉密载体。确因工作需要携带机密级、秘密级涉密载体的，应当经本机关、本单位主管领导批准，并采取严格保密措施。禁止在境外人员面前展示涉密载体。

严禁携带绝密级涉密载体参加涉外活动。携带涉密载体外出，如遇涉密载体安全受到威胁时，应当立即就近请求保密、公安、安全部门或其他机关、单位帮助处理，并尽快与本机关、本单位取得联系。

携带涉密笔记本电脑外出应当注意什么问题？

在一般情况下，不要携带涉密笔记本电脑外出。确因工作需要携带的，应按以下要求处理：

1、必须经机关、单位主管领导批准。

2、将涉密笔记本电脑中存储的涉密文件、资料复制到涉密移动存储介质中，并将存储介质留在机关、单位保存，同时对携带的计算机中的涉密文件、资料使用符合保密标准的工具进行清除处理。外出途中，必须采取严格的保密措施，确保涉密笔记本电脑始终处于携带人严密监控之下，做到“机不离身”。

3、将需要使用的涉密文件、资料复制到更易于保管的涉密移动存储介质中，然后将电脑中的涉密文件、资料进行彻底清除处理，使笔记本电脑不带有任何涉密信息。外出途中妥善保管好涉密移动存储介质，做到“盘不离身”。第四外出途中使用电脑生成的涉密信息，要及时复制到随身携带的涉密移动存储介质中，并对电脑硬盘中的涉密信息及时作清除处理。第五无论以何种方式，都应当妥善保管好涉密笔记本电脑和涉密移动存储介质，防止丢失和被盗窃。一旦发现或发生丢失、被抢、被盗或其他异常情况，要及时向单位报告。

携运或邮寄涉密载体出境有哪些保密要求？

禁止邮寄或非法携运国家秘密载体出境。确因工作需要寄往境外的，必须交由外交信使（含临时信使）办理。目的地不通外交信使或外交信使难以携运，确需自行携运出境的，应当根据携运国家秘密载体的密级，分别到有权批准的部门办理审批手续：

1、携运机密级涉密载体出境，须经中央和国家机关保密工作机构或省、自治区、直辖市保密行政管理部门批准。

2、携运秘密级涉密载体出境，须经中央和国家机关保密工作机构或地市级（含）以上地方保密行政管理部门批准。

3、申请办理审批手续时，需要向有关保密行政管理部门和保密工作机构提交涉密载体产生机关和本单位同意携运出境的证明。

4、禁止携运绝密级涉密载体出境。经批准携运涉密载体出境后，凡可以由我国驻外使领馆或其他政府驻外机构代为保存的，使用完毕后应尽快交其代为保存。无法交使领馆保存的，应采取严格的保密措施。携运出境的涉密载体，必须存放在具有防盗报警和防窃照技术装置的专制保密箱中。严格禁止把涉密载体夹放在行李中托运。如遇紧急情况时，要尽快与我驻外使领馆或其他政府驻外机构取得联系，并及时报告国内。携带涉密笔记本电脑和涉密移动存储介质出境，按以上规定办理。

【案例警示】

2005年10月，某海关在出入境检查时发现，某单位高某携带秘密级文件出境。经查，高某确因工作需要携带该文件出境考察，但没有按相关规定办理审批手续。事件发生后，有关部门给予高某行政记过处分。

泄密无大小　防范最重要

——保密工作从你我做起

为提高公司员工的保密安全意识，行政部特邀江苏省国家安全厅技术安全保卫办公室吕艳处长，于2016年6月29日赴我公司，围绕PC客户端和手机客户端如何做好保密等内容，为我公司员工作保密安全专题讲座。来自交科院检测中心、交规院隧道所、交科院桥梁所、发展部、行政部、道路所、养护中心等部门的20余位代表，聆听了本次讲座。

保密案例分析连载一："轮渡"木马病毒

互联网络通全球，居家能晓天下事。如今，现代人越来越离不开互联网了。在享受互联网方便、快捷服务的同时，与之相伴而生的各种风险也给人们带来了许多意想不到的麻烦：黑客攻击、网上陷阱、网络犯罪、网上窃密等令人防不胜防。近期发生于的泄密事件多与互联网病毒有关，尤其是"轮渡"木马病毒，其窃密手段非常隐蔽，用户在不经意间极易造成泄密。

所谓"轮渡"木马病毒，就是运行在互联网上的名为AutoRun.Inf和sys.exe的病毒程序，其"感染"的主要对象是在国际互联网和涉密计算机间交叉使用的U盘。当用户在上国际互联网的计算机上使用U盘时，该病毒便以隐藏文件的形式自动复制到U盘内。如果用户将该U盘插入涉密电脑上使用，该病毒就会自动运行，将涉密电脑内的涉密文件以隐藏文件的形式拷贝到U盘中。当用户再用该U盘连接国际互联网时，该病毒又会自动运行，将隐藏在U盘内的涉密文件暗中"轮渡"到互联网上特定邮箱或服务器中，窃密者即可远程下载涉密信息。

"以下两起案例，是近年发生真实泄密事件，都属于典型的由"轮渡"木马病毒造成的无意识泄密事件。

1、小刘，是某机关一名干部，平时好学上进，表现突出，被组织上定为政工干部培养苗子。2006年经组织推荐，小刘被送政工班培训。去学习前，小刘特意将自己平时在机关撰写的计划、总结等涉密资料存入U盘，准备在学习期间进行学术交流。学习期间，小刘多次上网查阅资料，并用该U盘下载参考资料。在此过程中，"轮渡"木马病毒自动驻存于U盘中，将小刘存储的涉密资料悉数"盗"入国际互联网。事后查明，小刘泄密的资料达32份，他因此受到降职、降衔的严肃处理。

2、董教授，是某大学知名教授，平时工作兢兢业业，经常加班加点在家备课。由于需要查阅资料，他家中的电脑接入了国际互联网。董教授白天在办公室办公电脑上工作，晚上在家用个人电脑工作，经常用U盘将未完成的工作内容在两个电脑间相互拷贝。自2005年以来，董教授办公电脑内的二百多份文件资料竟鬼使神差般地"跑"进了互联网，造成重大泄密。经上级保密委员会审查鉴定，涉密文件资料达三十多份，董教授受到降职降衔、降职称的严肃处理。

因保密防范知识缺乏造成的泄密实在令人遗憾！但在日常工作和生活中，类似这样不该发生的一幕却在不断上演。这两起案例非常具有代表性，充分反映了部分涉密人员保密观念淡薄、信息技术知识特别是网络安全防范知识欠缺、单位网络管理不规范等问题。当前，在一些单位，由于缺乏对安全保密知识的宣传教育，缺乏对移动存储介质使用的严格管理，涉密人员对安全保密防范知识不懂不会的现象比较普遍，有的甚至连安全保密的基本常识都不了解，由此造成的泄密事件防不胜防。因此，抓好安全保密知识的宣传教育，严格对互联网的使用管理，不仅是各单位当前的一项紧迫任务，也是一项经常性、基础性工作，必须认认真真抓好，确保人人了解，人人知悉，这样才能有效地防范泄密。

以制度强化涉密人员管理

近日，中央组织部、国家保密局等八部门联合下发了《关于进一步加强涉密人员保密管理工作的意见》（以下简称《意见》）。这是贯彻习近平总书记等中央领导同志关于保密工作的重要指示精神，落实保密法及其实施条例要求的重要举措。对于进一步加强涉密人员保密管理、维护国家安全和利益，具有重要的意义。

《意见》是应对保密工作严峻形势的重大举措

涉密人员作为国家秘密的直接管理者、使用者，始终是境内外敌对势力渗透、攻击的重要目标。当前，保密工作面临的形势十分严峻。一方面，针对我国的情报窃密活动更加猖獗；另一方面，市场经济深入发展和对外开放不断扩大，涉密人员流动加快、流向复杂，特别易受各种不良思潮、观念的影响，管控难度进一步加大。中央保密委员会高度重视涉密人员管理，将其作为“三大攻坚战”之一。《意见》的出台，是应对保密工作严峻形势，改进涉密人员管理的一项重大举措，必将推动涉密人员保密管理工作再上新的台阶。

《意见》是依法管理和科学管理的具体体现

涉密人员管理是保密工作的重要内容，管好涉密人员的前提是依法管理、科学管理。《意见》立足实际，一方面，依托现有的法律法规，做到于法有据，又充分吸收近年来一些地方、部门的好经验、好做法，做到切实可行，为涉密人员管理提供了规范化依据。另一方面，《意见》也十分注重涉密人员管理的科学性。涉密人员作为保守国家秘密的骨干，是保密管理的重要对象，也是做好保密工作的中坚力量，管理既要严格细致不留死角，也要科学适度权责一致，充分维护涉密人员的合法权益。

《意见》是做好涉密人员保密管理的工作指南

《意见》聚焦难点，突出重点，简明管用，对涉密人员管理进行了总体布局，具有很强的指导性和可操作性。各地区各部门要认真学习，以此为指导，加强对涉密人员的管理。重点把好“三关”：一是入口审查关，要准确确定涉密岗位、涉密人员和涉密等级，先审后用，确保可信可靠；二是日常管理关，要加强保密教育培训，落实保密承诺书、重大事项报告、考核考察等制度，严格出国（境）备案审批，加强权益保障，做到常抓不懈；三是离岗出口关，严格落实离岗离职脱密期管理，做到善始善终。严格出国（境）备案审批。

《意见》是群策群力密切合作的重要成果

涉密人员管理是一项全面复杂的系统工程，保密行政管理部门必须与各有关部门通力合作、共同攻关。《意见》中涉密人员分类确定、任（聘）用审查、出国（境）审批、脱密期管理、涉密人员权益保障等制度是保密行政管理部门会同组织人事、公安、国家安全、人力资源和社会保障、财政、国防科工等部门深入研究、反复论证的成果，是集思广益、引智聚力的结晶，是“最大公约数”。制定出台《意见》是第一步，关键是要抓好落实。下一步，保密行政管理部门要与各有关部门加强组织协调，积极探索实践，推动具体制度落实。只有各部门各司其职、各尽其责，形成齐抓共管的工作格局，才能唱响涉密人员管理的“最美和声”。

深入推进涉密人员保密管理，是一项长期而艰巨的任务。《意见》的出台，开篇破题，首战告捷。让我们借贯彻实施《意见》的东风，抓住机遇、乘势而为，推动保密工作再创新佳绩。

有些秘密

打死你也不能说

通过手机聊天工具找兼职，受到每月几千元的外快诱惑，对外偷卖所在国防军工单位的涉密信息，原以为“打打擦边球”就可以掩人耳目，没想到很快就被国家安全机关抓获。

近期，针对境外间谍情报机关围绕我国防军工领域实施情报窃密活动，四川省国家安全机关开展了代号“扫雷”的专项行动，一举抓获4名涉嫌危害国家安全的人员，这4人均从业于同一家国防军工单位，互不认识，却分别被境外间谍情报机关发展利用。

1、“境外记者”求购内部资料，职员多次泄露军品信息，赚每月3200元“外快”。

2014年10月的一天，某国防军工单位热表车间的90后青年文某像往常一样玩起了手机聊天软件，“附近的人”一栏中弹出一网名为“H”的网友，资料显示“附近厂职工需要兼职的联系我”。

在文某表明了自己该国防军工单位职员的身份后，“H”喜出望外，自称是境外某报社记者，希望文某提供工作中接触的内部资料，并承诺支付每个月3200元的报酬。在经济利益的驱使下，文某先后多次向“H”提供了所在单位生产军品的型号、每月量产情况、使用的特殊材料等涉密信息。

2、“网络兼职”高薪诱惑，频频偷卖军品信息，他原以为是“打擦边球”。

90后的王某在该国防单位技术部任职员，父母均是国家公职人员的他，因对现实工资待遇不满，在网上寻找兼职时“偶遇”了“H”，“招厂内的同志，兼职赚外快，待遇优，非直销，诚信至上”的手机聊天软件签名引起了王某的兴趣。

此时的王某已经被兼职每月三四千的收入冲昏了头脑，认为提供的单位动态性情况，只要不属于涉密信息，就可以“打打擦边球”。在利益诱惑下，王某频频为对方提供军品设计定型情况、样品编号、试验时间节点、出现故障情况等信息，案发被抓后，王某悔恨交加。

3、“猎头公司顾问”百万年薪诱惑，摇摆不定的他，成为境外间谍发展目标。

2014年，参加工作近10年的吴某有了离职的想法，他在某招聘网站上投放简历，并留下了联系电话。工作履历一栏中，与一般求职者不一样的是，“有某国防军工单位的工作经历”。

不久，吴某便收到了一封电子邮件，某“猎头公司顾问”要求吴某提供工作证明，以便求职。吴某按要求将自己与单位签订的劳动合同，以及印有自己照片、所在部门、姓名的工作证件，扫描后发送至对方邮箱。

很快，对方通知吴某被聘用，工作内容就是提供该国防军工单位尚未公开的内部信息，年薪高达50至120万元！面对如此丰厚的报酬，吴某虽然心动了，但犹豫着，结合曾在单位接受的保密教育及自身认识，意识到对方可能系境外间谍人员。吴某摇摆不定的态度，使其成为境外间谍情报机构发展的重点目标。

4、“境外朋友”寻找策反目标，为境外朋友推荐同学，结果同学被策反。

2013年初，在该国防军工单位技术部门供职的李某接到大哥电话，称一境外朋友（网名“S”）想了解一些航空航天方面的知识，有着保密意识的李某婉言拒绝了，但在大哥多次劝说下，李某与“S”建立了联系。

“S”以公司做市场调查准备进军航空航天领域为由，要求李某利用工作之便搜集关于航空航天方面的期刊、杂志、论文等资料，还劝导李某努力工作，争当领导，以便日后可以帮大忙。

由于单位内部资料管理较严，李某多次借阅资料未果，未能如期完成“S”交待的任务。为顾及情面，李某向“S”推荐了在某航空航天大学读研究生的同学程某，导致程某被策反，成为境外间谍情报机关的帮凶。

【国家安全机关提醒】：

利用工作便利提供情报信息危害国防军事工业

以上犯罪嫌疑人均涉嫌利用工作便利，窃取、刺探、非法向境外提供所在国防军工单位高新武器研发、测试、生产、列装部队等涉密情报信

长知识，这些保密规定你知道吗？

1、国家秘密信息管理方面的禁止性规定：

（1）禁止非法复制、记录、储存国家秘密；

（2）禁止在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密；

（3）禁止在私人交往和通信中涉及国家秘密。（《中华人民共和国保守国家秘密法》第二十六条）

2、新闻出版、广播影视、网络及其他传媒保密管理规定

新闻出版、广播影视、网络及其他传媒受众面广、传播迅速，一旦泄密，难以补救，必须加强保密管理。

3、涉密采购保密管理

涉密采购，是指本身涉及国家秘密、公开后会危害国家安全和利益的工程、货物和服务的采购行为。

4、对外提供国家秘密和境外人员因工作需要知悉国家秘密的保密管理

机关、单位对外提供国家秘密时，应确定范围，进行保密审查并做必要的技术处理，报有审批权限的部门批准，执行政府间保密协定或与对方签订保密协议，任何组织和个人不得擅自对外提供国家秘密。

5、涉密会议、活动的保密管理

举办会议或者其他活动涉及国家秘密的，主办单位应当采取下列保密措施：

（1）根据会议、活动的内容确定密级，制定保密方案，限定参加人员范围；

（2）使用符合国家保密规定和标准的场所、设施、设备；

（3）按照国家保密规定管理国家秘密载体；

（4）对参加人员提出具体保密要求。（《中华人民共和国保守国家秘密法》第二十七条》）

6、保密要害部门部位的保密管理

机关、单位确定保密要害部门属于法定义务，必须依法严格执行。确定保密要害部门部位应坚持两个基本原则：一是分级确定原则，二是最小化原则。

7、军事禁区和属于国家秘密不对外开放的涉密场所、部位的保密管理

军事禁区和属于国家秘密不对外开放的其他场所、部位应严格人员出入管控，需要对外开放或扩大开放范围的，应按照规定报经有关部门批准。

息，并通过自身人脉关系，为境外间谍人员物色、推荐国防军工领域易被引诱利用的科研人员。

这些行为严重危害了我国国防军事工业，对国家利益造成了无法挽回的巨大损失。四川省国家安全机关此次“扫雷”行动及时清除了境外谍报机关策反安插在国防军工领域的多名“钉子”，消除了重大危害。

不难看出，别有用心的境外间谍情报机关瞄准的，不仅仅是国防军工单位的核心技术人员，任何外围人员乃至每一个公民都有可能在不知情的情况下被利用。

随着我国综合国力不断增强，国防军工事业不断发展，特别是部分高新武器的曝光，境外间谍情报机关针对我高新武器研制、生产的国防军工单位开展间谍和破坏活动已经成为常态，境外间谍人员对我国公民的渗透策反可以说是无孔不入、无所不在的。

国家安全机关提醒广大民众：要增强维护国家安全的意识，增强法治意识，切莫一步走错，悔恨终身。特别是涉密人员网上求职要当心，切莫泄露曾经工作单位相关信息，以免引火烧身；天上不会掉馅饼，切莫为了网络中陌生人给予的蝇头小利犯下大罪；对于亲戚朋友提出的帮忙请求，切莫麻痹大意，成为“叛国”的帮凶。

制作涉密载体有哪些保密要求？

制作涉密载体应当由机关、单位或者具有国家秘密载体印制资质的单位承担，制作场所应当符合保密要求。

1、起草秘密文件、资料形成的过程稿、送审稿、讨论稿、修改稿、征求意见稿等，都要严格按照秘密文件、资料保密管理规定妥善保管，不能随意丢弃。

2、秘密文件、资料一旦定稿，应当严格履行定密程序，由承办人对照有关《保密事项范围的规定》拟定密级、保密期限和知悉范围；再送交定密责任人审批。整个定密过程可以结合办文流程进行。

3、制作秘密文件、资料应注明发放范围、制作数量和编排顺序号。需要委托印刷厂印制的，须送具有国家秘密载体印制资质的单位印制。禁止将秘密文件、资料委托非印制资质单位印制。

4、印制过程中的废页、废料、残页、残料、校对稿、胶片、胶版等，需要保存的，要按照国家秘密载体保密管理规定妥善保管；不需要保存的，须按照销毁管理规定及时销毁，不得随意处置，不得作为废品出售给废旧物资回收单位或个人。

5、刻录涉及国家秘密的电子文本资料，应当在本机关、本单位内部进行，并在电子文档适当位置标注国家秘密标志，禁止托交其他社会单位或无关人员刻录、制作涉密电子文档资料。

6、严格按照批准的数量制作，承办人员及其他任何人都不能多制、私留涉密载体。

为什么不能在普通电话中谈论或发送国家秘密内容？

普通电话存在串音和载波辐射问题，有的电话线是暴露在外的，可以被搭线窃听，如果在通话中谈论国家秘密，就会造成泄密。

境外敌对势力在我国周边地区、海上设立许多侦听台站，在太空中布有侦察卫星，就是为了对我国的通信进行全方位电子侦听。

手机通信传输系统，是开放的无线通信系统，通信信号是在空中传输的，只要有相应技术设备，就可以截听通话内容。同时，手机还可以与互联网无线连接，所以在手机通话中谈论涉密内容或用手机发送或存储涉密信息，很容易造成泄密。

保密法规定的12种严重违规行为是什么？

保密法列举了12种最常见、最典型的严重违规行为，这些违规行为导致保密措施失效，国家秘密失控，保密技术防护体系受到破坏，严重威胁国家秘密安全。这些行为是：

（1）非法获取、持有国家秘密载体的；

（2）买卖、转送或者私自销毁国家秘密载体的；

（3）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；

（4）邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的；

（5）非法复制、记录、存储国家秘密的；

（6）在私人交往和通信中涉及国家秘密的；

（7）在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密的；

（8）将涉密计算机、涉密存储设备接入互联网及其他公共信息网络的；

（9）在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换的；

（10）使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息的；

（11）擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；

（12）将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途的。

保密法规定，有上述行为之一的，依法给予处分；构成犯罪的，依法追究刑事责任；有上述行为尚不构成犯罪，且不适用处分的人员，由保密行政管理部门督促其所在机关、单位予以处理。

机关、单位违反保密法规定，有关人员要承担哪些行政责任？

机关、单位违反保密法规定，发生重大泄密案件的，由有关机关、单位依法对直接负责的主管人员和其他直接责任人员给予处分；不适用处分的人员，由保密行政管理部门督促其主管部门予以处理。

机关、单位违反保密法规定，对应当定密的事项不定密，或者对不应当定密的事项定密，造成严重后果的，由有关机关、单位依法对直接负责的主管人员和其他直接责任人员给予处分。

共产党员泄露党和国家秘密要受到哪些党纪处分？

《中国共产党纪律处分条例》第138条明确规定，丢失秘密文件资料或者泄露党和国家秘密，情节较轻的，给予警告或者严重警告处分；情节较重的，给予撤销党内职务或者留党察看处分；情节严重的，给予开除党籍处分。

在保密工作方面不负责任，致使发生重大失密泄密事故，造成或者可能造成较大损失的，对负有主要领导责任者，给予警告或者严重警告处分；造成或者可能造成重大损失的，对负有主要领导责任者，给予撤销党内职务务处分。

刑法对泄露国家秘密的犯罪有哪些规定?

刑法第111条规定,为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密或者情报的,处5年以上10年以下有期徒刑;情节特别严重的,处10年以上有期徒刑或者无期徒刑;情节较轻的,处5年以下有期徒刑、拘役、管制或者剥夺政治权利。

刑法第282条规定,以窃取、刺探、收买方法,非法获取国家秘密的,处3年以下有期徒刑、拘役、管制或者剥夺政治权利;情节严重的,处3年以上7年以下有期徒刑。

非法持有属于国家绝密、机密的文件、资料或者其他物品,拒不说明来源与用途的,处3年以下有期徒刑、拘役或者管制。

刑法第398条规定,国家机关工作人员违反保守国家秘密法的规定,故意或者过失泄露国家秘密,情节严重的,处3年以下有期徒刑或者拘役;情节特别严重的,处3年以上7年以下有期徒刑。

非国家机关工作人员犯前款罪的,依照前款的规定酌情处罚。

此外,刑法第431条、第432条分别对故意、过失泄露军事秘密罪作出规定。

依照有关司法解释,故意泄露国家秘密,涉嫌下列情形之一的,应予立案:

(1)泄露绝密级国家秘密1项(件)以上的;

(2)泄露机密级国家秘密2项(件)以上的;

(3)泄露秘密级国家秘密3项(件)以上的;

(4)向非境外机构、组织、人员泄露国家秘密,造成或者可能造成危害社会稳定、经济发展、国防安全或者其他严重危害后果的;

(5)通过口头、书面或者网络等方式向公众散布、传播国家秘密的;

(6)利用职权指使或者强迫他人违反国家保守秘密法的规定泄露国家秘密的;

(7)以牟取私利为目的泄露国家秘密的;

(8)其他情节严重的情形。

过失泄露国家秘密,涉嫌下列情形之一的,应予立案。

(1)泄露绝密级国家秘密1项(件)以上的;

(2)泄露机密级国家秘密3项(件)以上的;

(3)泄露秘密级国家秘密4项(件)以上的;

(4)违反保密规定,将涉及国家秘密的计算机或者计算机信息系统与互联网相连接,泄露国家秘密的;

(5)泄露国家秘密或者遗失国家秘密载体,隐瞒不报、不如实提供有关情况或者不采取补救措施的;

(6)其他情节严重的情形。

国家公务员泄露国家秘密和工作秘密要承担哪些行政责任?

《行政机关公务员处分条例》第26条规定,泄露国家秘密、工作秘密,或者泄露因履行职责掌握的商业秘密、个人隐私,造成不良后果的,给予警告、记过或者记大过处分;情节较重的,给予降级或者撤职处分;情节严重的,给予开除处分。

维修保养涉密计算机和涉密移动存储介质特别要做到这几点！

涉密计算机和涉密移动存储介质出现故障，不能正常工作时，应尽量由本机关、本单位技术人员进行维修。

请其他人员维修时，应在本单位内部进行，现场要有专门人员监督，防止数据被复制。

涉密计算机和涉密移动存储介质需要送销售公司维修时，应在维修前将硬盘拆卸保存，不能拆卸硬盘或需要重装操作系统的，机关、单位应安排人员在维修现场监督维修或安装。

需要送外单位维修保养的，应送涉密设备定点维修单位维修。

谨慎！涉密计算机、移动存储介质岂能随意淘汰处理！

计算机或移动存储介质中的信息做简单删除或格式化处理，难以达到彻底消除信息的目的，仍然可以通过相关技术手段恢复。

因此，必须采用专业技术进行销密。专业销密是指采用专门技术手段，彻底消除涉密计算机和涉密移动存储介质中存储的涉密信息，使之无法通过任何技术手段还原信息内容。淘汰、报废的涉密计算机、涉密移动存储介质仍属于涉密载体，不能随意转送、捐赠他人或作为废品出售。

防范对策

1.涉密计算机等办公自动化设备退出使用之前，应使用符合国家保密标准的技术设备对涉密信息或内部敏感信息进行清除，确保不被还原。

2.将准备淘汰的涉密计算机等办公自动化设备送交保密行政管理部门建立的销毁机构或指定的承销单位销毁。

（选自《保密科学技术》）

保密无小事

任何时候都不能懈怠

内部资料

注意保存