

保密基础知识

第一篇：保密基础知识

一、保密基础知识

1、什么是保密？

‘保密’，是指国家、公民、法人或社会组织对关系自身安全和利益，公开后会对自身利益造成损害的秘密信息，控制其知悉范围，对其采取保护措施，保障其安全的一种保护行为。在人类社会发展的进程中，自‘秘密’产生后，就有了‘保密’的行为，小至个人、家庭，大到组织、政党、国家，为了维护其秘密信息，都需要‘保密’。

2、什么是国家秘密？

《中华人民共和国保守国家秘密法》(以下简称《保密法》)第二条规定：‘国家秘密是关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。’从这一定义看，国家秘密由三个基本要素组成：

(1)关系国家安全和利益。这是构成国家秘密的实质要素，是准确判定某一信息是否属于国家秘密的关键问题。

(2)依照法定程序确定。这是国家秘密的程序要素。关系国家安全和利益的信息，必须在履行确定相应密级的程序后，才能成为法律认可的国家秘密。所谓法定程序，是指《保密法》和《中华人民共和国保守国家秘密法实施办法》(简称《保密法实施办法》)就确定、变更国家秘密的密级和保密期限以及解密所做出的一系列相应的规定。国家秘密的这一要素，是强调确定国家秘密的统一性与合法性，防止主观随意性。

(3)在一定时间内只限一定范围人员知悉。这是国家秘密的时空要素。国家秘密不可能是永远的秘密。随着一定的时间和客观情况的变化而发生变化，或变更密级或解密。在特殊情况下，也会发生密级由低变高的现象。国家秘密的接触、知悉的范围必须限定在需要知悉的范围内，不能控制知悉范围的信息就不能称其为国家秘密。

国家秘密的三个基本要素互相联系，缺一不可。

3、什么是保密工作？

保密工作是指按照我国《保密法》的规定，为保守国家秘密而进行的工作。

我们党和国家的保密工作主要包括以下几方面：一是由各级党委、党组保密委员会实施的领导和决策工作；二是由各级政府保密工作部门实施的保密管理工作；三是由各级党政军机关及国有企事业单位内的保密工作机构实施的保密管理工作；四是由具体业务部门承担的、渗透在各项业务工作之中的保密工作。

4、保密工作的指导思想和基本方针是什么？1983年5月，党中央批准了中央保密委员会提出的，提高革命警惕，贯彻突出重点、积极防范的方针，坚持内外有别、既便利工作又确保秘密的原则，确保党和国家的核心秘密，有领导、有控制地放宽对非核心秘密的限制，更好地为社会主义现代化建设服务'的保密工作指导思想。这一指导思想对我国新时期保密工作总的方针、原则，保密工作的根本任务和基本政策做了比较完整、科学的概括和表述，从思想、组织、制度和措施上改革和加强保密工作，以适应改革开放新形势发展的要求。

1988年9月，第七届全国人民代表大会常务委员会第三次会议通过的《保密法》在第四条中规定：，保守国家秘密的工作，实行积极防范、突出重点、既确保国家秘密又便利各项工作的方针。‘

1997年，中共中央在《关于加强新形势下保密工作的决定》中提出了新形势下保密工作的指导思想：，以邓小平建设有中国特色社会主义理论和党的基本路线为指导，以《中华人民共和国保守国家秘密法》为依据，坚持积极防范、突出重点，既确保国家秘密又便利各项工作的方针，实行专门工作与群众路线相结合、保密工作部门与业务部门相结合，依法管理国家秘密，不断提高技术防范能力和现代化管理水平，更好地为社会主义改革开放和现代化建设服务。‘

5、我国保密组织机构分为哪些类型和层次？我国保密工作组织机构分为领导机构和管理机构两大类。领导机构的基本形式是各级党组织的保密委员会(保密领导小组)。中央保密委员会是我国保密工作的最高领导层，省(自治区、直辖市)、地(市、州、盟)、县(市、区)三级党

委保密委员会是各地区保密工作的领导机构。上级保密委员会对下级保密委员会的工作负有指导和监督的职权，但是上下级保密委员会之间没有直接隶属关系。各级保密委员会都是由本级党委组建，受本级党委直接领导，代表本级党委对其职权范围内的保密工作进行领导，对本级党委负责。保密委员会的负责人一般由本级党委领导班子中的负责同志担任；委员由党委、政府及有关部门的负责同志担任。委员会内部实行委员分工负责制。保密委员会下设办公室，负责处理保密委员会的日常工作。

除地方各级党委保密委员会外，中央和国家机关、地方各级党政机关，以及国有企事业单位也都设立有保密委员会，负责领导本部门、本单位及本系统的保密工作。

保密工作管理机构的基本形式是政府的保密局和机关、单位的保密办。国家保密局是全国保密工作的最高管理层，是国务院的职能部门，主管全国的保密工作。省(自治区、直辖市)、地(市、州、盟)、县(市、区)保密局，是各级政府管理保密工作的职能部门，对本级政府负责。国家保密局与中央保密委员会办公室为一个机构，两块牌子。地方政府保密局与本级党委保密委员会办公室，也是一个机构，两块牌子。

除各级政府保密局之外，中央国家机关、县级以上国家机关和涉及国家秘密的单位(如高校、大型企业单位、大型事业单位)，一般也设立保密工作管理机构(通常称保密办公室或保密处)或指定某个部门承办日常保密管理工作。

6、各级党委的保密委员会的主要职责是什么？

(1)在本级党委的领导下，统一领导本行政区域的保密工作，贯彻执行党和国家有关保密工作的指导思想、方针、政策、法律、法规和决定，贯彻执行上级保密委员会和本级党委有关保密工作的指示；

(2)制定本地区保密工作发展规划和年度保密工作计划；(3)研究决定本行政区域保密工作的重大问题；(4)组织开展保密宣传教育工作；(5)提出保密立法建议；

(6)制定保密技术发展规划并指导、组织实施；(7)开展保密监督检

查工作，组织、协调、查处本行政区域内发生的重大泄密事件，特别是对本级党委组织人事部门管辖干部的泄密案件的查处工作；

(8)向本级党委和上级保密委员会报告工作，并提出改进和加强保密工作的意见、建议。

7、对党政领导干部的保密要求有哪些？

党政领导干部，是指在各级党的组织和国家机关中担任县、处级以上(含县、处级)领导职务的干部，包括在社会团体、事业单位担任县、处级以上领导职务的干部及国有大、中型企业中担任相当县、处级及其以上领导职务的负责人。由于领导干部在党和国家的各项工作中所处的地位和所负的责任不同于一般人员，决定了领导干部接触国家秘密的事项多、知密的范围广，特别是高级领导干部大量接触国家的核心秘密，所以，对领导干部在保密方面必须有特别的要求。中共中央保密委员会专门下发了《关于党政领导干部保密工作责任制的规定》，明确规定了领导干部必须遵守的十条保密守则。这十条守则是：(1)不泄露党和国家秘密；

(2)不在无保密保障的场所阅办、存放秘密文件、资料；(3)不擅自或指使他人复制、摘抄、销毁或私自留存带有密级的文件、资料。确因工作需要复印的，复印件应按同等密级文件管理；

(4)不在非保密笔记本或未采取保密措施的电子信息设备中记录、传输和储存党和国家秘密事项；

(5)不携带秘密文件、资料进入公共场所或进行社交活动，特殊情况确需携带时，须经本单位保密部门或主管领导批准，并由本人或指定专人严格保管；

(6)不准用无保密措施的通信设施和普通邮政传递党和国家秘密；

(7)不准与亲友和无关人员谈论党和国家秘密，管好身边工作人员和配偶、子女；

(8)不在私人通信及公开发表的文章、著作，讲演中涉及党和国家秘密；

(9)不在涉外活动或接受记者采访中涉及党和国家秘密；确因工作需要涉及或提供党和国家秘密的，应事先报经有相应权限的机关批准；

(10)不在出国访问、考察等外事活动中携带涉及党和国家秘密的文件、资料或物品；确因工作需要携带的，须按有关规定办理审批手续，并采取严格的保密措施。

8、党政领导干部应当履行的保密责任是什么？

党政领导干部在对自己主管或者分管的业务工作负责的同时，必须对其中的保密工作负责。中央保密委员会为此专门制定下发了《关于党政领导干部保密工作责任制的规定》。

领导干部保密工作责任制，就是指担任县、处级以上(含县、处级)领导职务的干部，在其职权范围内对保密工作所承担的领导和管理责任。这种责任应当根据领导干部的职务、分工及职权范围的不同，有所区别。总的原则是：实行保密工作谁主管，谁负责；主管什么业务，同时领导和管理该项业务工作中的保密工作，业务工作管到哪一级，其中的保密工作也同时管到哪一级。就一般情况来讲，领导干部应负的保密工作责任，主要是《党政领导干部保密工作责任制的规定》第7条所分列的内容：

(1)健全和完善保密组织，由一名领导主持保密委员会的工作，选配保密干部从事日常的保密管理工作。

(2)及时组织传达学习上级的保密工作文件和批示，有计划地开展保密宣传教育工作。(3)贯彻执行保密法规，制定实施保密工作计划。组织依法定密工作，健全各项保密规章制度，加强保密管理，进行督促检查。(4)对涉密的通信和办公自动化设备，负责采取保密技术防范措施。

(5)对本地区、本部门主办的涉及党和国家秘密的重要活动、会议或项目，组织制定保密方案，采取保密措施。

(6)认真总结本地区、本部门的保密工作，组织查处失泄密事件，表彰保密工作的先进单位和先进个人。

(7)积极支持保密部门依法开展保密工作，切实帮助解决工作中的困难，为保密部门和保密干部做好工作创造必要的条件。

9、如何区分国家秘密与工作秘密？

国家秘密与工作秘密有六个方面的区别：

(1)利益主体不同。工作秘密直接涉及的利益主体是有关国家机关。工作秘密一旦泄露仅对有关国家机关履行国家赋予的权力和职责等局部利益造成危害。而国家秘密直接涉及的利益主体是国家。国家秘密一旦泄露会对国家的整体利益造成危害；

(2)确定方式不同。工作秘密的确定以各级国家机关自行确定为主，对少数中央国家机关有统一规定或明确授权的，才从其规定。国家秘密的确定则必须依法进行，必须在国家保密工作部门会同有关中央国家机关制定和颁发的《国家秘密及其密级具体范围的规定》的范围内操作，不得随意确定；

(3)标志不同。属于工作秘密的文件、资料及其他载体，可以以‘内部’作标志，不得标上国家秘密的密级标志；

(4)管理不同。各级国家机关对工作秘密的管理可以参照国家秘密的管理办法，但不需要按照法定的程序加以规范。例如，传递国家秘密文件、资料或其他物品，必须通过机要邮政，不得通过普通邮政传递；传递工作秘密的文件、资料或其他物品则没有统一的要求，可以由各机关自行选择。又例如，对外提供属于国家秘密的文件、资料和其他物品，必须经法定授权的机关审查批准；对外提供属于工作秘密的文件、资料和其他物品，只需要经产生这些事项的机关同意即可；

(5)适用的法律不同。对工作秘密加以保护所适用的法律规范是《国家公务员法》，主要以行政手段对工作秘密给予法律保护。而对国家秘密的保护则适用《保密法》，不仅可以使使用行政手段，而且还可以使用刑法等法律手段；

(6)责任不同。工作秘密泄露后，有关责任人只承担行政责任，只会受到相应的行政处分；而国家秘密泄露后，则要根据可能产生的危害后果及其他情节确定有关责任人应当承担的法律责任。情节轻微，后果不严重的可以承担行政责任，情节和后果严重的则要承担刑事责任。

总之，由于工作秘密与国家秘密各自所涉及的利益主体不同，一旦发生泄露后所造成的危害后果在范围和程度上都有很大差别。因此，对工作秘密保护的力度明显要小于对国家秘密的保护力度。其他各方

面的差别都由此而来。

10、哪些事项泄露后会对国家安全和利益造成损害后果，需要确定为国家秘密？

《保密法实施办法》规定了下列事项泄露后会对国家安全造成损害后果之一的，要确定为国家秘密。(1)危害国家政权的巩固和防御能力；(2)影响国家统一、民族团结和社会安定；(3)损害国家在对外活动中的政治、经济利益；(4)影响国家领导人、外国要员的安全；(5)妨害国家重要的安全保卫工作；

(6)使保护国家秘密的措施的可靠性降低或失效，(7)削弱国家的经济、科技实力；(8)使国家机关依法行使职权失去保障。12．什么是国家秘密的具体范围？

国家秘密的具体范围(以下简称保密范围)，是指在国家秘密基本范围之内的、由国家保密局会同中央有关机关规定的某一业务工作方面的国家秘密及其密级具体范围的规定。

《保密法》虽然规定了国家秘密的基本范围，但还不能直接确定某一方面的秘密事项是否属于国家秘密和属于何种密级，还需要依据国家秘密基本范围，规定各业务部门‘保密范围’。

11、国家秘密的密级是如何划分的？

国家秘密的密级即国家秘密的等级，是指依据保密范围所规定的事项同国家安全和利益的关系程度，特别是国家秘密一旦被泄露后，可能会给国家安全和利益造成的不同损害程度而做出的等级划分。

《保密法》第九条规定，我国的国家秘密的密级分为‘绝密’、‘机密’、‘秘密’三个等级。

划分三个等级的标准是：‘绝密’是最重要的国家秘密，泄露会使国家的安全和利益遭受特别严重的损害；‘机密’是重要的国家秘密，泄露会使国家的安全和利益遭受严重的损害，‘秘密’是一般的国家秘密，泄露会使国家的安全和利益遭受损害’。以法律的形式对国家秘密等级做出基本规定，具有重要的意义。一是区分了不同密级与国家安全和利益的关系程度不同，泄露后所造成的损害程度是有区别的；二是不同密级的国家秘密，所采取的保密措施也不同，特别是绝

密级的国家秘密，应采取特别的保密措施；三是为规定保密范围、区分不同密级提供了法律依据。

二、保密管理知识 1．什么是保密制度？

保密制度是指国家保密法律、行政法规和规章所要求人们共同遵守的保密规则或行为规范。

2．对涉密人员管理都有哪些基本规定？

第一，先审查后使用。先审查后使用是保障国家秘密安全的一项重要措施。涉密人员与普通公民不同，他们因工作需要，经常接触或知悉国家秘密，如果不规定特殊要求，就有可能发生泄密问题，损害国家的安全和利益。因此，做好涉密人员的审查工作是很有必要的。审查的主要内容包括：一是本人政治条件的审查；二是本人品质的审查；三是家庭社会关系审查；四是接触国家秘密必要性审查；五是其他方面的审查。

第二，批准接触。《保密法》第二十七条规定：国家秘密应当根据需要，限于一定范围的人员接触。绝密级国家秘密，经过批准的人员才能接触。这包括了两层意思：一是根据需要接触。接触国家秘密不是一种政治待遇，更不能按行政级别接触。只要工作需要，行政级别低的涉密人员也可以接触重要的国家秘密。二是要经过批准。什么人可以接触国家秘密，要经过各机关、单位的主管领导批准，上级机关或产生国家秘密的单位已规定接触范围的，应当按规定的接触范围接触，不能随意扩大或者缩小接触国家秘密的范围。

第三，因私出国(境)审查。重要涉密人员是指在国家重要部门或岗位的人员，如：国防、外交、军事、国家安全等特殊部门的人员，从事尖端武器生产的技术人员，情报人员，机要人员，密码人员等。重要涉密人员因私出国(境)要经过人事任命机关批准。国务院有关主管机关认为出境后将会对国家安全造成危害或者对国家利益造成重大损失的，不得批准出境。

3．涉密人员在交往中应当注意哪些保密问题？

(1)注意私人交往与通信的保密。在现代社会，人与人的交往是不可少的。在与他人的交往中，如果不注意保密问题，不分地点、场合，随便讲话或是吹嘘，往往会造成泄密。邮寄国家秘密载体时，必

须交由机要交通或机要通信传递，不能使用普通邮政或特快专递传递。普通邮政或特快专递没有特别的安全保卫措施，所邮寄的国家秘密载体处在不安全的环境中，就有可能发生国家秘密载体丢失、被盗、非法接触等问题，造成泄密。特别是在境外与国内的单位或亲戚朋友联系时，不能在信里涉及国家秘密或我内部情况，以免造成泄密，或引起不必要的麻烦。(2)不在公共场所谈论国家秘密。涉密人员因工作需要知悉许多一般公民所不知悉的国家秘密、工作秘密，这些秘密只限一定范围内的人员知悉，如不注意地点和场合随意谈论，就会造成泄密。(3)不携带国家秘密载体外出办事，确因工作需要携带时，必须经单位领导批准，并采取安全措施，特别是携带绝密级国家秘密必须两人以上同行，不得使国家秘密载体离开本人。在运输国家秘密设备或产品时，必须由专人或派武装警察押运。

(4)在涉外活动中未经批准不得涉及国家秘密。在现实生活中，有的人保密观念淡薄，在对外交流时不分场合和地点，不该说的乱说，造成泄密。还有的人为了谋取个人私利，一味迎合外国人，要什么给什么，不惜损害国家利益，结果受到国家法律的制裁。这些教训，也是应引以为戒的。(5)涉密人员不得擅自流动。特别是在重要部门或重要岗位工作的重要涉密人员流动，须经有权批准的部门批准后才能流动。

4、什么是国家秘密载体？

国家秘密载体是指以文字、数字、图像、声音等方式记载国家秘密信息的纸介质、磁介质、光盘等各类物品。

国家秘密和载体之间既相互联系又有区别。国家秘密必须借助一定的载体来存储和传递。国家秘密是一种特殊的信息，载体是它的存在形式。二者不能等同。5．国家秘密载体有哪些种类？

国家秘密载体形式多样。主要有以下几类：

纸介质载体。是以文字、图形、符号等书面形式记录国家秘密的纸介质载体。如国家秘密文件、文稿、文书、档案、电报、信函、图纸及其他图文资料等。人们通常把这类载体统称为国家秘密文件、资料。国家秘密文件、资料是目前实际工作中使用最多、最常见的国家

秘密载体。

磁介质载体。以磁性物质记录国家秘密的载体。如记录着国家秘密信息的计算机的磁盘(含软盘、硬盘、U 盘)、磁带、录音带、录像带等。光介质载体。以光信号记录、传输国家秘密信息的载体，如光盘。随着信息技术的发展，磁介质和光盘类的国家秘密载体将越来越多。

此外，还有以物理方式记录、承载信息的设备、产品、物品等。这类载体有的可以从外观上直接反映出国家秘密的属性，也有的需要通过测试、分析等物理或化学手段获得国家秘密信息。6．什么是密件和密品？

密件是指以文字、数字、图像、声音的形式载有国家秘密的物件。它包括传统的多为纸介质的文件、资料，也包括磁介质和光介质等国家秘密载体。

密品是指直接含有国家秘密信息的设备、产品。这种设备、产品通常不是直接裸露国家秘密，但通过测试、分析等手段可以获得国家秘密信息。

7．国家秘密载体的收发、传递有哪些保密要求？

国家秘密载体产生以后，收发人员要按照保密规定进行核对、登记，严格按照发文范围收发密件，并掌握国家秘密载体的分布情况。

(1)收发国家秘密载体，应履行登记、编号、签收手续，签收时必须逐件清点、核对；

(2)密件包装应当由单位的机要保密人员或有关专门人员拆封。(3)接收人员应当对接收的密件，及时在收文(件)登记簿上登记造册。分发密件时，严格分发范围，遵守相关规定。

(4)传递、运输国家秘密载体必须交由专门的部门(如机要交通、机要通信部门)，不得通过普通邮政邮寄或交给无关人员捎带；确需自行传递、运输的，要选择安全的交通线路和交通工具，采取严密的保密措施。设有机要文件交换站的城市，在本市区内传递机密级、秘密级秘密载体，可以通过机要文件交换站进行；(5)向境外邮寄、携运秘密载体时必须通过外交信使传递，确需个人携运的，要按照国家秘密物品出境管理规定办理；

(6)采用现代通信或计算网络等手段传输国家秘密信息，应当遵守有关保密规定。

8．国家秘密载体的使用有哪些保密要求？

(1)传达、阅读国家秘密文件、资料，要按照工作需要和规定的范围，限定在可以知悉该项国家秘密的范围内的人员；使用密件，也只能是可以接触该项国家秘密的范围内的人；(2)机关、单位工作人员阅读、处理国家秘密文件、资料，应在办公室进行。不允许将秘密文件、资料带回家中或者带到公共场所阅办；

(3)机关、单位的领导阅读秘密文件、资料，可以采用传阅的方式进行。传阅国家秘密文件、资料应当由经办人员负责，专夹专阅，并填写‘传阅卡’。记载夹内密件份数、编号和阅读时间等。传阅的密件，阅读者不能擅自抽出、留存，阅读者之间不能横传，不得随意抄录密件内容，更不能私自复印；

(4)借阅、借用密件，要经借出单位的主管领导批准，并办理相关手续；

(5)绝密级文件，未经密级确定机关、单位或其上级机关批准，禁止复制、复印、摘抄、汇编。复制、复印、摘抄、汇编机密级和秘密级的密件，必须经批准并履行审批手续。9．国家秘密载体的保存有哪些保密要求？

(1)保存秘密载体，应当选择安全保密的场所和部位，并配备必要的保密设备；

绝密级秘密载体应当在安全可靠的保密设备中保存，并由专人管理。

(2)工作人员离开办公场所，应当将秘密载体存放在保密设备里；

(3)涉密机关、单位每年应定期对当年所存秘密载体进行清查、核对，发现问题及时向保密工作部门报告。

按照规定应当清退的秘密载体，应及时如数清退，不得自行销毁；

(4)涉密人员、秘密载体管理人员离岗、离职前，应当将所保管的秘密载体全部清退，并办理移交手续；

(5)需要归档的秘密载体，应当按照国家有关档案法律规定归档；

(6)被撤消或合并的涉密机关、单位，应当将秘密载体移交给承担其原职能的机关、单位或上级机关，并履行登记、签收手续。10．国家秘密载体的销毁有哪些保密要求？

(1)销毁秘密载体，必须要履行清点、登记手续，经机关、单位的主管领导批准，严禁私自销毁；

(2)销毁时要确保秘密载体的内容无法还原。销毁磁介质、光盘等秘密载体，应当彻底销毁，也可采取粉碎、烧毁或化学腐蚀等方式进行；

(3)需集中销毁的密件应当送往文件销毁定点单位销毁。有关人员要在场监销，并由监销人员和销毁人员共同签名，禁止将秘密载体当作废品出售；(4)送往定点单位销毁的密件，应当装袋、封紧，专人专车押送，防止运送途中散失。销毁工作完毕后，应对销毁现场进行认真清理。

对机构撤销、合并时，原单位的秘密文件，发文单位要求收回的，要如数收回清退发文单位；发文单位不收回的，要移交有关部门，或者登记销毁。

11．复制国家秘密载体有哪些规定？

(1)复制绝密级秘密载体，应当经密级确定机关、单位或其上级机关批准；

(2)复制制发机关、单位允许复制的机密、秘密级秘密载体，应当经本机关、单位的主管领导批准；

(3)复制秘密载体，不得改变其密级、保密期限和知悉范围；(4)复制秘密载体，应当履行登记手续；

(5)复制件应当加盖复制机关、单位的戳记，复制件应视同原件管理；

(6)涉密机关、单位不具备复制条件的，应当到复制国家秘密载体定点单位复制。

12．国家秘密载体的汇编、摘录和引用有哪些规定？(1)汇编国家秘密文件、资料应当经原制发机关、单位批准；(2)经批准汇编秘密文件、资料时，不得改变原件的密级、保密期限和知悉范围，确需改变

的，应当经原制发机关、单位同意；(3)汇编秘密文件资料形成的秘密载体，应当按照其中的最高密级、最长保密期限管理；

(4)摘录、引用国家秘密的内容形成的秘密载体，应当按照原件密级、保密期限管理。

13．携带国家秘密载体外出应遵守哪些规定？

(1)确因工作需要随身携带国家秘密载体外出的，应当经本机关、单位主管领导批准，并使秘密载体始终处于携带人的有效控制之下；

(2)携带绝密级国家秘密载体外出必须二人以上同行；

(3)未经批准，禁止携带国家秘密载体参加外事活动和进入境外机构；

(4)个人因公外出，如遇所带国家秘密载体的安全受到威胁的紧急情况时，应当立即就近请求保密、公安、国家安全部门或其他机关、单位的帮助，并尽快与本机关、单位取得联系，如实报告情况。

14．个人投寄稿件、著书立说时应当注意哪些问题？

(1)个人接受新闻采访时，如果采访内容涉及机关、单位公务方面内容的，应经单位主管领导批准，并对采访内容进行审查。接受记者采访不得涉及国家秘密。确需涉及国家秘密的，应对记者申明涉及国家秘密的内容。要求记者履行保密义务。如果接受记者采访纯属个人行为，不得涉及国家秘密、工作秘密和商业秘密；

(2)向报刊杂志、电台、电视台投寄稿件、音像资料和发表文章，在公共信息网络上发布信息，属于公务方面的，应经机关单位主管领导或主管部门批准并进行审查。属于个人行为的，不得涉及任何秘密内容(属于作者的个人秘密除外)；

(3)个人著书立说不得涉及国家秘密，所引用的资料一般也不得涉及机关、单位的工作秘密或商业秘密，确需引用的，必须经机关主管领导批准。所用资料涉及他人商业秘密的，应经其权利人同意；

(4)向境外新闻媒体、杂志刊物、互联网及学术组织、机构邮寄稿件，一律不得涉及国家秘密、机关单位的工作秘密和他人的商业秘密。如涉及相关公务方面内容的，也应当事先经机关、单位同意。

15．阅读、传达国家秘密文件都有哪些保密要求?(1)阅读、传达

国家秘密文件、资料，要严格限制在规定的范围内，不得擅自扩大范围；

(2)阅读国家秘密文件、资料，必须在办公室或阅文室等有保密保障的场所进行；

(3)阅读国家秘密文件、资料，应当进行登记，不得由阅件人直接传给他人；

(4)不得擅自存留传阅的国家秘密文件、资料；

(5)传达国家秘密文件时，不得使用无线话筒等无保密保障的设备；

(6)听传达的人员应当遵守保密纪律，需要录音、录像的，应当经过批准。

16．特殊场所、部位保密制度是什么？

特殊场所部位主要是指军事禁区和不对外开放的其他涉密场所和部位。军事禁区的保密措施，在 1990 年 2 月 23 日七届人大常委会第十二次会议通过的《军事设施保护法》及其配套法规中，作了详细、具体的规定。其他场所部位的保密措施，则由其主管机关制定或与有关的保密工作部门共同商定。由于军事禁区和其他涉密场所、部位是按照有关法律、法规、规章划定的，因而其对外开放及扩大开放范围，须按照国家有关规定经国家有关部门批准。

17．哪些部门、部位应该确定为保密要害部门、部位？

在日常业务工作中产生、传递、使用和管理绝密级或较多机密级、秘密级国家秘密的内设机构，应确定为保密要害部门；

机关、单位内部集中制作、存储、保管国家秘密载体的专门场所，以及涉及国家秘密较多的省部级以上领导干部的办公场所，应确定为要害部位。

18．对保密要害部门、部位的具体保密要求有哪些？

符合保密要害部门、部位条件的机关、单位应按照一定的原则和程序确定要害部门、部位；对保密要害部门、部位具体的保密要求有以下几方面：

(1)由机关、单位主管保密工作的领导人负责，定期研究和部署保密工作；

(2)建立机关、单位保密工作岗位责任制，与保密要害部门、部位主要负责人及所属工作人员签订保密责任书，将保密工作任务落实到具体人员；(3)对在要害部门、部位工作的人员，必须坚持经常性的保密教育、培训，并进行涉密资格审查，严格履行保密义务；

(4)结合部门、部门的实际，制定严格的保密管理制度和防范措施，并认真组织落实；

(5)定期检查保密要害部门、部位的保密管理和保密技术防范情况，解决存在的问题，组织查处泄密事件。19．什么是泄露国家秘密的行为？

泄露国家秘密，是指违反保密法律、法规和规章的下列行为之一：
(1)使国家秘密被不应知悉者知悉的；

(2)使国家秘密超出了限定的接触范围，而不能证明未被不应知悉者知悉的。

上述第一种行为是泄露国家秘密的行为，这是不言而喻的。第二种行为为什么也是泄露国家秘密的行为呢？这是因为，违反保密法规，使国家秘密失去合法的有效的控制可能会出现如下两种情况；一是能够确认国家秘密未被不应知悉者知悉；二是不能够确认国家秘密未被不应知悉者知悉。第一种情况未造成泄密，可按违反保密制度论处；第二种情况则应视为泄密。因为在实际生活中，使国家秘密超出限定的接触范围后，在绝大多数情况下，都难以确认国家秘密未被不应知悉者知悉。同时，国家秘密失控或泄露后，其危害后果往往是潜在的，不能马上显露，有的甚至在相当长的时期内都无法得到证实。如果把危害后果规定为构成泄密 96 必要条件，那么，在泄密案件的处理上，就会出现久拖不决的现象，对严重的违法泄密犯罪行为也难以给予及时准确的打击和制裁。这对保守国家秘密，维护国家的安全和利益是不利的。

20．什么是故意泄密？什么是过失泄密？

(1)故意泄露国家秘密，是指行为人明知自己的行为会造成使国家秘密失控，给国家的安全和利益造成损害的结果，却希望或放任这种结果发生；

(2)过失泄露国家秘密，是指行为人应当预见到自己的行为会造成泄露国家秘密的后果，却因思想麻痹，疏忽大意，不按照有关规定对国家秘密实施有效的管理而泄露国家秘密，或虽然已经预见到自己的行为会造成泄露国家秘密的后果，却因过于自信，心存侥幸，而泄露国家秘密。

过失泄露，尽管行为人没有主观上的故意，但是，给国家的安全和利益所造成的损害却是显而易见的。在现实生活中过失泄密在泄密事件中所占的比例也较高。明确了情节严重的过失泄密是一种犯罪行为，有利于提高人们的警觉，减少泄密事件的发生，维护国家的安全和利益。至于情节严重与否，则可从行为人的主观恶性，泄密行为发生的前后表现，泄密行为发生的特定时间与地点，以及已经造成或可能造成的危害后果等来考察判断。按照《保密法》第三十一条第一款的规定，不管是故意泄密还是过失泄密，只要是‘情节严重的’，就应当依照刑法的规定，追究刑事责任。21．泄露国家秘密的渠道主要有哪些？

泄密的形式有多种，渠道也有很多，但概括起来主要有几个方面：
(1)对外交往与合作中的泄密；(2)新闻宣传和出版方面的泄密；(3)通信和办公自动化方面的泄密；(4)互联网上泄密；

(5)人员流动造成的泄密。

22．造成泄露国家秘密的原因主要有哪些？

造成泄露国家秘密的主要原因有以下几方面：

(1)有法不依，有章不循，思想麻痹，保密观念淡薄；(2)缺乏保密常识，过失泄密；

(3)保密管理措施不严，存在泄密隐患；(4)保密防范和保密检查技术落后；(5)对泄密查处不力。

23．防止泄露国家秘密的主要措施有哪些？

(1)抓涉密人员的审查。对进入涉密岗位的工作人员，要严格把关，按照要求对人员进行严格审查，并且经常进行教育和观察；(2)抓保密教育。保密教育要突出重点，在广泛开展保密宣传教育的基础上，重点抓好涉密人员的保密教育；

(3)抓监督管理。加强对承办、使用、管理国家秘密的涉密人员的监督和管理，明确保密权利和义务，使涉密人员在从事涉及国家秘密的活动中严格遵守保密法规、规范办事，防止泄密问题的发生；

(4)抓违纪处理。对违反保密规定造成泄密的人员，必须依纪依法严肃处理。严肃查处泄密事件及其责任人，可以教育本人和警示他人，这同样是防止泄露国家秘密的一项重要措施。

三、保密技术知识 1．什么是保密技术？

保密技术，是对保护国家秘密安全的所有技术手段的统称。保密技术是适应保护对象的客观实际需要而产生和发展的。保密技术应用面广，种类很多。按其用途及功能划分，主要分为保密防范技术和保密检查技术两大类。2．通信泄密隐患主要有哪些？

通信系统是由交换设备、传输设备和终端设备组成的，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，会像天线那样向周围空间辐射发射电磁波，所传输的信号频率越高，辐射越强，传输越远，把通信信息带到空间，利用相应设备可接收还原信息。

(2)网络串音泄密：电话用户与电话局之间由许多电话线(光缆除外)捆扎在一起。用户通话时通话的声音变成话音电流。相邻电路或线路之间因各种原因极易产生串音，即在某一线路或电路可以收到其他线路或电路的通信信号。例如，我们打电话有时会听到别人通话声音，就是串音。人耳能听到的串音称作可闻串音，一般是由故障或其他非正常原因造成的，通过维修可以排除。特别要指出的是，对于不可闻或者一般设备接收不到的串音，我们可能不觉察，不注意，但窃密者可用专门研制的设备接收还原信息。(3)无线传输泄密：当前，微波、卫星、短波、超短波等无线信道广泛用于通信传输，所传输的信号暴露于空中，只要有相应的接受设备，选择合适的位路，就可接收还原通信信息。

(4)通信设备电磁泄漏发射泄密：通信设备，包括电话机、传真机、交换机等，工作时会产生电磁泄漏发射，通信信号会被调制携带数百米之外，被接收者利用有关设备接受还原。

(5)现代电信网广泛使用程控交换机，实质是计算机控制的交换机，如果被植入木马程序，就会在某种预先设定条件下将通信信息发射到空间或发送给窃密者。

3. 使用通信工具时，应当遵守哪些保密规定?(1)不准在私人通信中泄露国家秘密。

(2)召开涉及国家秘密内容的会议不使用无线话筒。

(3)在有线、无线通信中传递国家秘密的，必须采取保密措施。(4)不准使用明码或者未经有关机关审查批准的密码传递国家秘密。

(5)任何组织或者个人不得利用电信网络制作、复制、发布、传播含有泄露国家秘密内容的信息。(6)严禁密电明复或密明混用。在特殊情况下，明电或电话必须涉及密电时，不得暴露有关密电日期，也不得引用有关密电的具体内容。凡事先发了密电，而后又需要发明电的，对明电的措辞必须要严格审查。

(7)使用电信网络传输信息的内容及其后果由电信用户负责。

4. 通信保密技术主要有哪些?

(1)密码保密技术，利用密码对通信信息加密，使窃收者虽然能收到通信信号，但还原不了信息，偷不到通信内容。

(2)物理保护技术，采用专缆、专孔、专机、专用电源、专用机房或其他隐蔽措施，使窃收者收不到通信信号。例如党政专用电信网。

(3)使用符合标准的低泄射通信设备。(4)使用屏蔽机房、屏蔽电缆。(5)加装通信干扰器等。

5. 使用党政专用电话网有哪些保密要求?

(1)所用电话机必须符合《电话机电磁泄漏发射限值和测试方法》(BMBI—94)保密技术标准，并具有国家保密局颁发的进网许可证。(2)严禁在专网上使用无绳电话机。

(3)不得在专网上私自连接其他终端设备，确有必要必须经过专网局批准，并经过安全保密检查合格后方可使用。

(4)避免在同一房间同时使用专网电话和普网电话，以免因声音偶合造成泄秘。

6. 计算机信息系统存在哪些主要安全威胁?(1)非法访问，窃取秘密

信息。

(2)利用搭线截收或电磁泄漏发射，窃取秘密信息。(3)利用特洛伊木马和其他后门程序窃取秘密信息。(4)篡改、插入、删除信息，破坏信息完整性。

(5)利用病毒等非法程序或其他手段攻击系统，使系统瘫痪或无法服务，破坏系统可用性。

(6)传播有害国家安全和稳定的信息，传播低级下流黄色信息，利用系统进行有害信息渗透。

(7)冒充领导发布指示，调阅密件；冒充主机、冒充控制程序欺骗合法主机和用户，套取或修改使用权限、口令字、密钥等信息，非法占用系统资源，破坏系统可控性。(8)行为者否认自己发送过或接收到相关信息，产生抵赖行为。7.计算机信息系统主要存在哪些泄密隐患和途径？

计算机信息系统是通信、计算机、网络技术综合产物，具有通信系统所有泄密隐患和途径，例如有线、无线传输泄密等，同时还有一些其他泄密隐患：

(1)信息设备电磁泄漏发射。计算机信息系统使用的信息设备，包括主机、服务器、磁盘机、打印机、显示器等，工作时都会产生不同程度的电磁泄漏发射。一种是通过电磁波向空中发射，称作辐射发射；一种是经电源线、信号线、地线等导体发射，称作传导发射。信息设备所处理的信息会随发射电磁波发送出去，数百米外可以接收还原。

(2)系统后门、隐通道、漏洞。计算机信息系统讲求的是互联互通，远程访问，资源共享，为攻击者提供了实现攻击的途径。计算机信息系统操作系统程序量大，通信协议复杂，不可避免存在各种配置漏洞、操作系统漏洞、协议漏洞、后门、隐通道等，可被窃密者利用。如果是人为的预留后门、隐通道、漏洞，将更加危险。

(3)磁介质剩磁数据可复原。磁介质存储信息难以清除。当我们删除一个文件时，只是在文件目录表中对该文件加删除标志，该文件所占用的扇区标识为空闲，磁盘上的数据并未真正清除。通常所说的格式化程序(例如 Format)，并未清除数据，只是重写了文件分配表 FAT

表而已；分区硬盘，也只是修改引导记录，大部分数据并未改变。经过删除、格式化或分区硬盘后，一般用户再看不见数据，但使用专用程序却能找到并恢复数据。

有研究表明，即使对磁介质进行物理格式化仍会留有信息痕迹，利用专用工具可恢复。

(4)操作系统工作时，为了某种需要，可能会做一些人们不希望做而又无法控制的事。例如在进行写操作时，在硬盘或软盘上自动建立某些临时文件，将某些信息暂时存在这里，使用者不会觉察，窃密者却有可能提取这些信息。

(5)主要软硬件进口不可控，这是很大的隐患。

8. 《计算机信息系统保密管理暂行规定》有哪些主要内容?(1)明确了保密工作部门在计算机信息系统中的管理职责。即：国家保密局主管全国计算机信息系统的保密工作。各级保密工作部门和中央、国家机关保密工作机构主管本地区、本部门的计算机信息系统的保密工作。

(2)对涉密计算机信息系统的规划、研制、建设、联网做出了若干保密规定。其中有：规划建设计算机信息系统，应当同步规划落实相应保密设施；计算机信息系统的研制、安装和使用，必须符合保密要求；计算机信息系统应当采取有效的保密措施，配装合格的专用设备，防泄密、防窃密。所采取的保密措施应与所处理信息的密级要求相一致；计算机信息系统联网应当采取系统访问控制、数据保护和系统安全保密监控管理等技术措施；计算机信息系统的访问应当按照权限控制，不得进行越权操作，采取技术安全保密措施的数据库不得联网。

(3)对涉密信息的存储、处理、传递、密级标志等作了规定。其中有：涉密信息 and 数据必须按照保密规定进行采集、存储、处理、传递、使用和销毁；计算机信息系统存储、处理、传递、输出的涉密信息要有相应的密级标志，密级标志不能与正文分离；国家秘密不得在与因特网联网的计算机上存储、处理和传递。(4)对涉密载体的使用、管理、维修、销毁等做出规定。载体通常指存储涉密信息的介质，包括磁盘、光盘等载体。其规定有：存储国家秘密的载体，应按所存储信息的最

高密级标明密级，并按相应密级文件进行管理。存储在计算机信息系统内的信息应当采取保护措施；存储过国家秘密信息的载体不能降低密级使用。不再使用的载体应及时销毁；存储过国家秘密信息的计算机载体的维修应保证所存储的国家秘密信息不被泄露；计算机信息系统打印输出的涉密文件，应当按相应密级的文件进行管理。(5)对涉密信息系统的环境提出要求。处理涉密信息的场所应当按照国家有关规定，与境外机构驻地、人员住所保持相应的安全距离；处理涉密信息的场所应当根据涉密程度和有关规定设立控制区，未经管理机关批准无关人员不得进入；处理涉密信息场所应当定期或者根据需要进行保密技术检查；计算机信息系统应采取相应的防电磁信息泄漏的保密措施；计算机信息系统的其他物理安全要求应符合国家有关保密标准。

(6)对系统管理的责任制、管理制度、人员、技术检查等做出了规定。计算机信息系统的保密管理应实行领导负责制，由使用计算机信息的机关、单位的主管领导负责本单位的计算机信息系统的保密工作，并指定有关机构和人员具体承办。各单位的保密工作机构协助本单位的领导对计算机信息系统的保密工作进行指导、协调、监督和检查；计算机信息系统的使用单位应根据系统所处理的信息涉密等级和重要性制订相应的管理制度；各级保密工作部门应依照有关法规和标准对本地区的计算机信息系统进行保密技术检查；计算机信息系统安全保密管理人员应经过严格审查，定期进行考核，并保持相对稳定；各单位保密工作机构应对计算机信息系统的工作人员进行上岗前的保密培训，并定期进行保密教育和检查；任何单位和个人发现计算机信息系统泄密后，应及时采取补救措施，并按有关规定及时向上级报告。(7)对在计算机信息系统保密工作中做出显著成绩或违反规定、泄露国家秘密的行为，做出了奖惩的规定。

9. 涉密计算机信息系统保密管理基本原则是什么？

概括起来说，涉密计算机信息系统管理基本原则是：同步建设，严格审批，注重防范，规范管理。

同步建设是涉密计算机信息系统防范和管理的基础和前提。同步

建设就是涉密计算机信息系统与保密设施同步建设，包括同步规划，

同步预算，同步设计，同步实施。同步建设有利于整体考虑，统筹协调，简化环节，符合标准。

严格审批就是系统建成后报经地(市)级以上保密部门审批后才能投入使用。这是涉密系统管理的关键环节。通过审批，把隐患和漏洞排除在使用之前，有利于信息保密，有利于日后管理。严格就是要有高度负责的精神，实事求是的科学态度，严格遵守和执行有关规定、标准。

注重防范是保密工作，积极防范'指导思想的具体体现，建设、使用、运行维护，自始至终都要注重防范。

规范管理是涉密系统保密防范能力获得并始终保持的根本保证。技术是基础是手段，管理是保证是关键，三分技术七分管理。审批非常重要，但绝不是一劳永逸，必须加强日常管理。10．涉密计算机信息系统建设保密管理主要有哪些环节？

(1)资质管理。涉密系统集成单位必须经过保密工作部门资质认定，并取得《涉及国家秘密的计算机信息系统集成资质证书》。涉密系统建设单位应当选择具有《资质证书》的集成单位承建涉密系统。

(2)方案设计及评审。应当按照《涉及国家秘密的计算机信息系统安全保密方案设计指南》的规定，进行系统设计，并组织专家对方案评审。

(3)实施阶段。涉密系统建设单位应当与承接涉密系统集成的单位签订协议，规定集成单位应履行的保密义务。选择工程监理单位应当符合国家有关保密规定。

(4)审批。系统建成后应当报地(市)级以上保密部门审批同意，方可投入使用。如有必要，保密部门审批中的现场考察测试，可由国家保密局授权的信息系统安全保密测评机构进行测评。11．机信息系统有哪些主要的安全保密要求？

(1)涉密信息的定密制度和管理制度应当符合《中华人民共和国保守国家秘密法》及其实施办法和有关法规。

(2)应当符合《计算机信息系统保密管理暂行规定》。(3)涉密系统不得直接或间接国际联网，必须实行物理隔离。(4)物理安全。通过环

境安全、设备安全、媒体安全等措施，保护计算机信息系统设备、设施、媒体和信息，使之不因自然灾害、环境事故以及人为物理操作失误或错误，不因各种以物理手段进行违法犯罪活动，而造成破坏、丢失。

(5)运行安全。通过备份与恢复、病毒检测与消除、电磁兼容等等措施，保证系统能持续运行。

(6)信息安全保密。通过物理隔离、身份鉴别、访问控制、传输加密、存储加密、完整性校验、防电磁泄漏发射、审计跟踪、安全保密性能检测等措施以及相应管理，保证信息的保密性、完整性、可用性、可控性以及行为的不可否认性，防止不良信息渗透传播。

12．计算机需维修、淘汰时应如何处理？

用于存储国家秘密信息的计算机在维修、淘汰时，应当做到：(1)维修涉密计算机时，必须进行登记。到保密工作部门指定的单位维修，不得送到社会上的维修点维修；

(2)保修期内的计算机，在送往销售单位保修时，必须将存储国家秘密信息的磁介质拆卸，必须派责任心强的涉密人员，对送修计算机实行现场监督，确保涉密信息安全；(3)淘汰计算机时，要进行清点、登记后，经单位领导批准。然后交保密工作部门指定的单位做淘汰处理；

(4)各机关单位的保密工作机构负责本系统、所属二级单位存储国家秘密信息的计算机维修、淘汰的管理工作。

13．公众信息网保密管理基本原则是什么？

概括起来说，公众信息网保密管理基本原则是：控制源头，加强检查，明确责任，落实制度。

控制源头，就是，国家秘密信息不得在与国际网络联网的计算机信息系统中存储、处理、传递。‘就是涉密信息不上网，上网信息不涉密。控制源头就是采取一切法律的、行政的和技术的措施，千方百计防止国家秘密信息进入这类网络。

加强检查，就是一旦有故意的或者过失的将涉密信息上到这类网络，保密工作部门和有关部门能及时发现，及时采取措施。就是检查

有关管理和防范措施落实情况，检查有关网络保密法规制度执行情况。

明确责任，落实制度，就是建立责任制，制订管理制度与措施，逐项落实。

14．计算机国际联网的保密管理制度有哪些？计算机信息系统国际联网，是指中华人民共和国境内的计算机信息系统为实现信息的国际交流，同外国的计算机信息网络相连接。

计算机信息系统国际联网的保密管理，实行控制源头、归口管理、分级负责、突出重点，有利发展的原则。计算机信息系统国际联网的保密制度有：

(1)涉及国家秘密的计算机信息系统，不得直接或间接与国际互联网或其他公共信息网相连接，必须实行物理隔离。

(2)涉及国家秘密的信息，包括在对外交往与合作中经审查、批准与境外特定对象合法交换的国家秘密信息，不得在国际联网的计算机系统中存储、处理、传递。

(3)上网信息的保密管理实行谁上网谁负责的原则。凡向国际联网的站点提供或发布信息，必须经过保密审查批准。保密审查实行部门管理，有关单位应当根据保密法规，建立信息保密审查领导责任制。提供信息的单位应当按照一定的工作程序，健全信息保密审查制度。

(4)凡以提供网上信息服务为目的而采集信息，除在其他新闻媒体上已公开发表的，组织者在上网发布前，应当征得提供信息单位的同意；凡对网上信息进行扩充或更新，应当认真执行信息保密审查制度。

(5)凡在网上开设电子公告系统、聊天室、网络新闻组的单位和用户，应由相应的保密工作机构审批，明确保密要求和责任。任何单位和个人不得在电子公告系统、聊天室、网络新闻组上发布、谈论国家秘密信息。面向社会开放的电子公告系统、聊天室、网络新闻组，开办人或其上级主管部门应认真履行保密义务，建立完善的管理制度，加强监督检查。发现有涉密信息，应及时采取措施，并报告当地保密工作部门。

(6)用户使用电子函件进行网上信息交流，应当遵守国家有关保密

规定，不得利用电子函件传递、转发或抄送国家秘密信息。互联单位、

接入单位对其管理的邮件服务器用户，应当明确保密要求，完善管理制度。

(7)互联单位与接入单位，应当把保密教育作为国际联网技术培训的主要内容。互联单位与接入单位、接入单位与用户所签订的协议和用户守则中，应当明确规定遵守国家保密法律，不得泄露国家秘密信息的条款。

四、保密法律知识

1. 我国保密法律的基本框架是什么？我国保密法律的基本框架主要是由以下法律、法规和规章构成：(1)根本法

《中华人民共和国宪法》第五十三条关于公民保密义务的规定。

(2)法律

①《中华人民共和国保守国家秘密法》。

②其他法律(如《刑法》、《专利法》、《档案法》等)中的有关保密规定。(3)行政法规

①《中华人民共和国保守国家秘密法实施办法》

②其他行政法规(如《专利法实施细则》、《档案法实施办法》等)中的有关保密规定。(4)地方性法规

①省、自治区、直辖市人大或其常委会制定的省、自治区、直辖市《保密法实施细则》。

②地方法规中的有关保密规定。

(5)中央和国家机关有关部门制定的保密规章。(6)地方人民政府制定的地方保密规章。2. 什么是保密法的适用？

保密法的适用，是指国家保密工作部门、工作人员及其被授权管理保密事务的单位依照其职权范围，通过法定程序实施保密法律规范的一种方式。它是国家保密工作部门、工作人员及其被授权管理保密事务的单位的专项活动，具有公务性质；它严格依照法定的职权范围适用保密法律规范，既不能随意超出职权范围，也不能自由放弃或拒绝行使其法定职权；它依照法定程序把保密法律规范的一般规定应用于具体情况，导致一定的法律后果，并表现为一定法律文件的活动方式来实现保密法律规范，如保密工作部门对违反保密法律的行为做出

的行政处罚决定，并以一定法律文件形式宣告法律关系的产生、改变或废止等。3.《保密法》的效力指的是什么？

《保密法》的效力，是指《保密法》的生效范围。任何一部法律都有一定的适用范围，它只能在规定的范围内生效，超出此范围便不能适用。《保密法》的效力分空间效力、时间效力和对人效力。如

《保密法》开始生效的时间是1989年5月1日，1951年6月中央人民政府政务院颁布的《中央人民政府政务院保密国家机密暂行条例》随之废止。空间效力，即《保密法》生效的地域范围。如《保密法》适用于我国除港澳台地区以外的其他地区。对人效力，即对什么人发生法律效力。如《保密法》对中国境内外的中国公民和中国境内外国人、无国籍人均有效力。上述范围的人均不得有泄露、刺探、收买、非法提供或非法获取我国国家秘密等违反《保密法》的行为，否则，就会对我国的保密法律制度造成侵害，构成犯罪。

4. 最高人民检察院关于泄露国家秘密罪的立案标准是什么？2006年7月26日，最高人民检察院公布了《关于渎职侵权犯罪案件立案标准的规定》(高检发释字(2006)2号)，其中规定了关于泄露国家秘密罪的立案标准：(1)故意泄露国家秘密罪

故意泄露国家秘密罪，是指国家机关工作人员或者非国家机关工作人员违反保守国家秘密法，故意使国家秘密被不应知悉者知悉，或者故意使国家秘密超出了限定的接触范围，情节严重的行为。

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保守国家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。

(2)过失泄露国家秘密罪

过失泄露国家秘密罪，是指国家机关工作人员或者非国家机关工

作人员违反保守国家秘密法，过失泄露国家秘密，或者遗失国家秘密载体，致使国家秘密被不应知悉者知悉或者超出了限定的接触范围，情节严重的行为。

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。

5．泄露国家秘密应承担的法律责任？

《保密法》第三十一条规定，违反本法规定，故意或者过失泄露国家秘密，情节严重的，依照刑法的规定追究刑事责任。违反本法规定，泄露国家秘密，不够刑事处罚的，可以酌情给予行政处分。第三十二条规定，为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密的，依法追究刑事责任。（1）泄露国家秘密应承担的党纪责任

《中国共产党纪律处分条例》第一百三十八条规定：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，给予撤销党内职务处分。

第五十二条规定：参加国(境)外情报组织或者向国(境)外机构、组织、人员非法提供情报的，给予开除党籍的处分。（2）泄露国家秘密应承担的行政责任

行政责任是同民事责任、刑事责任并列的三大法律责任之一，它是指行政法律关系主体因违反行政法律规范而依法所承担的法律后果。

《中华人民共和国保守国家秘密法实施办法》根据《保密法》有关泄

露国家秘密，不够刑事处罚的，可以酌情给予行政处分'的规定，对泄露国家秘密行政处分作了如下具体规定：①第二十九条规定：凡泄露国家秘密尚不够刑事处罚的，有关机关、单位应当根据被泄露事项的密级和泄密行为的具体情节，给予行政处分。

②第三十条规定：对泄露国家秘密尚不够刑事处罚，有下列情节之一的，应当从重给予行政处分：泄露国家秘密已造成损害后果的；以谋取私利为目的泄露国家秘密的；泄露国家秘密危害不大但次数较多或者数量较大的；利用职权强制他人违反保密规定的。③第三十一条规定：泄露国家秘密已经人民法院判处刑罚的以及被依法免予起诉或者免予刑事处罚的，应当从重给予行政处分。④第三十二条规定：泄露秘密级国家秘密，情节轻微的，可以酌情免予或者从轻给予行政处分；泄露机密级国家秘密，情节轻微的，可以酌情从轻给予行政处分，也可以免予行政处分；泄露绝密级国家秘密，情节特别轻微的，可以酌情从轻给予行政处分。如 2003 年，中国电子科技集团第 28 研究所一名技术人员违反保密规定，将自己在工作中使用的存有机密级信息的移动硬盘私自带回家，并联接在接入互联网的计算机上。经查，该计算机与国际互联网联接并植入了后门程序，攻击者可利用植入程序完全控制该计算机。为此，该技术人员被调离重点工作岗位，并受到行政警告处分。

（3）泄露国家秘密应承担的刑事责任

1997 年 3 月 14 日经第八届全国人民代表大会第五次会议修订后的《中华人民共和国刑法》，涉及泄密犯罪的条文共有八条，刑罚从剥夺政治权利、管制、拘役、有期徒刑、无期徒刑直至死刑。《刑法》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，处五年以上十年以下有期徒刑；情节特别严重的，处十年以上有期徒刑或者无期徒刑；情节较轻的，处五年以下有期徒刑、拘役、管制或者剥夺政治权利。对国

第二篇：保密基础知识试题

保密基础知识试题

一、填空题

1.国家秘密是指关系国家的 安全 和 利益，依照法定程序确定，在 一定时间内只限 一定范围 的人员知悉的事项。

2.各级国家机关、单位对所产生的国家秘密事项，应当按照 国家秘密及其密级具体范围 的规定确定密级。

3.保守国家秘密是我国公民的一项 基本义务。4.涉密人员是指因工作需要，接触、知悉、管理和掌握 国家秘密 的人员。

5.涉密人员脱密期届满的，对其知悉的国家秘密仍负有 保密义务。

6.涉密人员脱离涉密岗位必须实行脱密期管理，其中核心涉密人员脱密期为 3-5 年，重要涉密人员为 2-3 年，一般涉密人员为 1-2 年。

7. “绝密” 是 最重要 的国家秘密，泄露会使国家的安全和利益遭受 特别严重 的损害。

8.保密期限需要延长的，由 原确定密级 和 保密期限 的机关、单位或者其上级机关决定。

9.不准通过普通邮政、快递、物流方式传递属于国家秘密的 文件、资料 和 其他物品。

10.个人因公外出，应把所携带 涉密载体 存放在保密设备里。11.不得在涉密计算机和非涉密计算机上 交叉 使用移动存储介质。

12.涉密系统不得直接或间接连接国际互联网，必须实行 物理隔离。

13.计算机一旦存储和处理过一份涉密信息，就应当确定为 涉密计算机，并粘贴相关密级标志。

14.未经本单位 信息化 管理部门批准，不得自行对涉密计算机进行格式化并重装操作系统。

15.在涉密工作区域，禁止使用 无标志的 存储介质。

16.涉密办公自动化设备现场维修时，应由有关人员 全程 陪同。

17.单位通过互联网发布信息应当进行 保密审查。

18.严禁将用于处理国家秘密信息的具有打印、复印、传真等多功能的一体机与 普通电话线。

19.机密级国家秘密是重要的国家秘密，泄露会使国家的安全和利益遭受 严重 的损害。

20.秘密级国家秘密是 一般 的国家秘密，泄露会使国家的安全和

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/246134041123010135>