2024年保密工作知识讲课稿4篇

作者：小六 来源：网友投稿

在日常学习、工作或生活中，大家总少不了接触作文或者范文吧，通过文章可以把我们那些零零散散的思想，聚集在一块。范文书写有哪些要求呢？我们怎样才能写好一篇范文呢？下面我给大家整理了一些优秀范文，希望能够帮助到大家，我们一起来看一看吧。

保密工作知识讲课稿篇一

（一）国家秘密的含义及基本范围

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。国家秘密有三个基本要素，缺一不可：

首先,关系国家的安全和利益，是指秘密事项如被不应知悉者所知，对国家的安全和利益将造成各种损害后果。

其次,依照法定程序确定，是指国家赋予这一管理职权的单位，根据国家秘密及其密级具体范围的规定，对该事项履行确定密级的手续后，该事项才能作为国家秘密受国家有关法规的认可和保护，特殊情况下，需经有关保密工作部门审定后，确定为密或非密以及属于何种密级。任何不经法定程序产生的秘密事项，都不是国家秘密。

第三,在一定时间内只限一定范围的人员知悉，是相对于公开而言的，即尚未公开且被人们加以保密的事项，就是对国家秘密在保密时间和接触范围上的控制，擅自公开或擅自扩大接触范围就是泄密。

根据《保密法》规定，国家秘密的基本范围包括以下事项：

1.国家事务的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.其他经国家保密工作部门确定应当保守的国家秘密事项。

需要说明的是在各党政机关的秘密事项中，凡符合国家秘密诸要素的，均属于国家秘密。

（二）国家秘密等级及标准

我国国家秘密的密级分为3个等级；绝密级、机密级、秘密级。

区分这三个等级的原则标准是：

（1）“ 绝密 ”——是最重要的国家秘密，泄露后会使国家的安全和利益遭受特别严重的损害。

（2）“ 机密 ”——是重要的国家秘密，泄露后会使国家的安全和利益遭受严重的损害。

（3）“ 秘密 ”——是一般的国家秘密，泄露后会使国家安全和利益遭受损害。

从以上密级划分的标准可以看出，以上3个等级的密级是以泄露后所产生的危害程度来划分的。

绝密级——特别严重的损害后果。

机密级——严重的损害后果。

秘密级——损害后果。

秘密事项的密级一旦确定之后，要严格按照确定的密级进行管理和控制知悉范围。这是保密工作的基本要求。

国家秘密的保密期限：绝密不超过30年，机密不超过20年，秘密不超过10年。

（三）工作秘密的含义及其特征要素

我们部分部门或单位虽然不直接产生或不涉及国家秘密，但在具体工作中存在一些不宜公开的工作事项，这就是所谓的工作秘密。工作秘密是在国家公务活动中产生的，不属于国家秘密而又不宜对外公开的秘密事项。它有三个特征要素：

（1）工作秘密是各级国家机关产生的事项；

（2）工作秘密是涉及国家机关的公务活动和内部管理的事项；

（3）工作秘密是不属于国家秘密，又不宜公开的事项。

工作秘密未经批准，不得擅自扩散。

（四）保密工作基本要求

保密工作就是从国家的安全和利益出发，将国家秘密控制在一定的范围和时间内，防止被非法泄露和利用，使其自身价值得到充分有效的实现所采取的一切必要的手段和措施。简言之，是指与国家的安全和利益密切相关的保守国家秘密的一切活动。它包括保密立法，保密宣传教育，建立健全保密规章制度，研制、开发和应用先进的防窃密、泄密的技术设备，依法进行保密检查监督，追查处理泄密事件，以及开展保密工作的理论研究等活动。

新修订的《保密法》第四条明确规定，“保守国家秘密的工作，实行积极防范、突出重点、依法管理的方针，既确保国家秘密安全，又便利信息资源合理利用。法律、行政法规规定公开的事项，应当依法公开。”这一表述，集中阐述了新时期党的保密工作方针，高屋建瓴，内容丰富，特色鲜明，为我们做好新形势下的保密工作提供了指南。

所谓“积极防范”是保密工作实践经验和特点规律的科学总结。保密工作是国家行政管理的重要组成部分，确保国家秘密安全是其核心任务。保密工作实行积极防范的方针，是由保密工作的本质特性所决定。“积极防范”强调的是主动的、事先的防范，即以防止窃密泄密为出发点和着力点，主动把保密工作做在前面，把保密措施落实在前面，努力构筑人防、物防、技防相结合的综合防范体系，及时发现和消除泄密隐患，堵塞泄密漏洞，从源头上防止各类泄密事件发生，确保国家秘密安全。保密工作的本质特征决定着保密工作必须以防为主，防患未然，把工作重点放在预防上，立足于不泄密。我们在日常工作中，积极防范应该做到：（1）领导重视并把保密工作纳入议事日程，使其与业务工作同步进行；（2）建立健全保密规章制度并严格执行，经常督促检查，堵塞泄密漏洞；（3）坚持经常性的保密宣传教育；（4）严格保密纪律，及时查处泄密事件；（5）积极开发和利用先进的保密技术；（6）及时总结经验，提高保密工作的整体水平。

所谓“突出重点”是抓好工作的一个重要方法，也是保密工作的基本工作方针。做好保密工作必须正确处理重点与一般的关系，通过抓好重点，确保核心秘密安全，同时兼顾一般，促进保密工作协调发展。突出重点，就是要把落实重点领域和重要方面的保密工作摆在突出位置，对绝密级国家秘密、绝密级信息系统、保密要害部门部位、核心涉密人员，必须采取更严格的保密管理措施。在具体工作中要做到：一是按国家秘密的密级划分，绝密是重点，应当采取比对机密、秘密级的国家秘密更为严格的保密措施；二是对国家秘密相对集中的部门、部位应当加强防范工作；三是对于接触国家秘密较多的领导和经管国家秘密事项的专职人员，应当有更严格的要求。

所谓“依法管理”是贯彻依法治国的基本方略的必然要求。坚持依法管理，必须做到有法可依，有法必依，执法必严，违法必究。有法可依，要求建立完备的保密法律制度，将保密工作的各个方面纳入法制轨道，增强保密法律体系的完整性、权威性、有效性；有法必依，要求机关、单位严格按照有关法律法规管理涉密人员、涉密载体、涉密信息系统和涉密活动等；执法必严，要求保密行政管理部门按照有关法律法规，认真履行监督管理职责；违法必究，要求对违反保密法律法规的行为依法查处，严肃追究法律责任。

“既确保国家秘密安全又便利信息资源合理利用”，明确要求在确保国家秘密安全的同时，应当充分遵循信息化条件下信息资源利用和管理的客观规律，建立科学有效的保密管理制度，促进信息资源的合理利用。需要指出的是，信息资源的合理利用并不等同于信息公开，它既包括依法解密和依法公开信息，也包括依法降低密级、缩短保密期限、扩大知悉和接触范围等。

“法律、行政法规规定公开的事项应当依法公开”，充分体现了对保障公民知情权、参与权和监督权的高度重视。依法公开，一是指法律法规要求公开的必须公开，不得以保密为由不予公开或者拒绝公开；二是指公开前必须依法进行保密审查，公开事项不得涉及国家秘密；三是指公开的程序和方式必须符合法律规定。

保密工作方针是学习领会保密法的总钥匙，更是指导保密工作理论和实践的科学指南，既要做好字句上的解读，更要联系保密工作实际，全面加深理解，坚决贯彻执行。

保密工作始终伴随着，颠覆与反颠覆、渗透与反渗透、策反与反策反、窃密与反窃密的矛盾斗争。当前无论是国际还是国内，保密工作都面临着相当严峻的形势。仅2015年中央保密委通报查处的重大失泄密事件中，三分之一的失泄密事件是向境外提供国家秘密或出卖情报的，有几十起是发生在党政军机关和国防军工科研生产单位的，其中最突出的是涉密计算机和互联网泄密案，占总数的42%，还有部分发生在涉密文件流转和销毁环节。所以，保密意识淡薄、保密知识匮乏，保密制度执行不力、监管不严造成的失泄密问题和所面临的安全隐患形势十分严峻。

当前保密工作严峻形势体现在三个方面：

严峻形势之一：境内外敌对势力加紧对我进行情报窃密活动。近年来，境内外各种敌对势力为了达到对我遏制、分裂、颠覆的目的，对我实施全方位的情报窃密战略，窃密活动日益猖獗。境外敌对势力从未放弃过对我进行“西化”、“分化”的战略图谋，利用各种手段，窃取我政治、经济、科技、军事等方面的情报，策反我党政领导机关核心要害部门的知密人员，竭力在我们内部寻找代理人，加紧渗透颠覆活动，窃密与反窃密的斗争非常激烈。境内外“民运”“台独”“藏独”“东突”以及“法轮功”邪教组织等敌对势力，无时不在对我进行捣乱、破坏和分裂活动。特别是台湾当局为了进行“台独”分裂活动，愈加不择手段地进行渗透、策反和窃密，除在我境内大肆活动外，还在50多个国家建立了100多个情报站，专门策反出国、驻外人员。西方国家和台湾间谍情报机关、非政府组织以旅游、考察、扶贫、支教等为借口，多方搜集、刺探我政治、经济、军事及民族、宗教等方面的情报；境外宗教势力以赈灾、助学等方式向我贫困地区渗透，并从我出国留学人员中物建培养新生代；“法轮功”等邪教组织的非法活动突出，形式趋于隐蔽化、手段趋向高技术化。比如；2015年，四川省国家安全机关开展了代号为“扫雷”的专项行动，一举破获4起涉嫌危害国家安全的网上间谍案。4名嫌疑人均供职于同一国防军工单位，互不认识，有的通过手机q寻找兼职，有的在网上投简历跳槽，还有的熟人介绍，分别被境外间谍情报机构发展利用，踏上了对外偷卖所在单位涉密信息的不归路。

主要表现在：一是窃密主体增多。除间谍情报机关某某，以新闻、商务机构和非政府组织为掩护的窃密活动明显增多，而且更具隐蔽性。二是窃密领域扩大。过去主要是直接指向我政治、经济、军事、科技等方面，现在扩大到我民情、社情和能源、环保等多个领域。三是窃密方式多样。不仅以思想渗透、金钱美色利诱等手段拉拢策反我内部人员，还以商贸洽谈、学术交流、社会调查为幌子，广泛搜集窃取我各种情报。四是窃密手段现代化。敌对势力投入大量的人力、物力和财力发展高科技窃密技术，窃密器材越来越向高效率、多功能、超微型、易某某、善隐蔽方向发展，特别是利用网络技术和间谍卫星窃密，保密防范的难度越来越大。五是窃密目标指向我掌握核心秘密的人员。境内外敌对势力为了窃取我党和国家核心秘密，千方百计向我党政军领导机关和军工科研生产单位渗透，策反我内部人员，而且策反的对象指向我重要岗位的核心涉密人员。近年来，国家安全机关破获的间谍窃密案件中，涉及我党政军机关多名高级别的领导干部，令人触目惊心。

严峻形势和挑战之二：市场经济的发展给保密管理提出了新课题。我国社会主义市场经济的建设，极大地推进了生产力的发展，丰富了人们的物质文化生活，综合国力明显增强。但是，在市场经济条件下，随着利益关系的调整变化，一些人的价值观、利益观也发生了很大变化，给保密管理提出了许多新课题。突出表现在四个方面：一是一些人见利忘义，使国家秘密遭受损害。一些人为了单位和个人的利益，不惜践踏国家保密法规，以牺牲国家利益谋取单位和个人的利益；一些人利益受到冲击，思想观念发生变化，理想信念发生动摇，个别人为了一己私利，甚至出卖国

家利益，沦为国家和民族的罪人。二是人员流动加剧，给保密管理增加了新的难度。随着国际交往和人员交流日益增多，包括高科技人员在内的各类人员流动加快，一些涉密人员离职跳槽到外资或合资企业，有的甚至举家移居海外。而相关的法律法规和管理制度不适应，管理和监控能力下降，给国家秘密安全造成巨大危害，其中有些人成为间谍情报机关和敌对势力猎取我国家秘密的目标。三是新的经济成分、社会组织的出现，使涉密主体多元化。越来越多的非公有制经济单位和民营企业进入涉密领域，原有密管理体制出现盲点，新的体制又没有完全建立起采，给保密管理带来了新的困难。四是在市场经济体制下，各行业、各部门的管理方式、工作方式都发生了很大变化，给国家秘密的管理也带来了新的变化。长期以来，以行政关系为基础的保密管理方式，以内部管理为主要手段的保密管理体制，在市场经济条件下出现了某些不适应，保密管理部门对各类涉密信息及其载体的控制能力受到削弱。

严峻形势和挑战之三：以信息技术为代表的高技术发展加大了保密工作的难度。当前，我国正处于“ 互联网+ ”跨越式发展时代，大力推进信息化，以信息化带动工业化，以工业化促进信息化，走新型工业化道路，是全面建设小康社会、加快社会主义现代化建设的必然选择。同时，也要看到，信息化建设给国家信息安全带来了严峻挑战，给保密工作提出了新的更高的要求。

（一）国家秘密的存在形态和运行方式发生重大变化，泄密渠道明显增多。随着现代信息技术的迅猛发展和广泛应用，信息的存载和传输方式出现电子化、网络化，国家秘密信息的产生、传输、存储和处理方式日益多样，除纸介质外，还包括声、光、电、磁等。这些变化，在保密观念、保密技术和保密制度等方面都给我们做好保密工作带来了巨大的冲击。

1.国家秘密存储介质多样化、轻便化。由于计算机在处理文字信息方面有着无可比拟的优势，国家秘密信息越来越多地通过计算机来存储和处理。除纸质文件外，出现了以“ 三盘一机 ”（光盘、优盘、硬盘和计算机）为代表的新型涉密载体。这些新型载体具有体积小、容量大、携带方便、泄密的风险高、危害重等特点。比如，假设每份电子文件占用200k硬盘空间，1块容量为100g的硬盘就能存储50万份文件。一旦丢失或被窃，危害将十分巨大。

2.国家秘密信息的存载与保护方式数据化、系统化。大量的国家秘密信息进入计算机信息系统，涉密部门和单位的日常工作愈来愈严重地依赖信息系统，一旦信息系统出现问题，就会导致灾难性的后果。与此相适应，信息安全概念已经从单纯的信息内容的保密性，扩展到信息和信息系统的完整性和可用性。也就是说，国家秘密信息安全更多地表现为整个信息系统的安全，而远不止单个信息的安全。保密工作不仅要“ 保某某 ”，而且要“ 保某某 ”，难度远远超过对纸质文件的管理。

3.国家秘密信息泄露渠道增多，形式隐蔽，隐患严重。当前较为突出的，主要有以下几种情况：一是涉密笔记本电脑泄密。笔记本电脑携带方便，使用普遍，泄密问题十分突出。一些工作人员携带涉密笔记本电脑出差，丢失或被窃的事件不断发生。同时，使用涉密笔记本电脑上互联网的问题也比较突出。二是数字复印机泄密。新一代数字复印机配置了内存或大容量硬盘，有的容量高达几百亿字节，可以存储十几年复印过的所有文件内容，如管理不当，极易造成泄密。在美国，政府曾发过一个文件，就是禁止政府部门使用日本“ 佳能 ”复印机，主要目的就是为了防止数字复印机带来的泄密问题。三是多功能一体机泄密。该设备集打印、复印、扫描、传真等功能于一体，在复印、扫描涉密信息时，很可能通过连接的普通电话将涉密信息传出去。如果同时还连接涉密信息系统，物理隔离就形同虚设。四是无线局域网泄密。无线上网使用的是开放式无线信道，传输信号暴露在空中，任何具有接收功能的设备都可能获取信息。同时，一台具有无线上网功能的计算机，若没有对其接入方式进行设定，就可以在用户不知情的情况下，与同样具有无线上网功能的计算机自行连接。如果附近有无线局域网接入点，还会自动寻找并建立连接。此外，

使用无线键盘、无线鼠标处理涉密信息，传输的信号也很容易被接收还原。五是移动存储介质交叉使用泄密。在涉密信息系统与互联网之间交叉使用移动存储介质，涉密信息就很可能因木马病毒在不知不觉间传输到互联网上。六是手机泄密。手机作为通话和接发信息的工具，尤其是现在的智能手机已经成为泄密的重要渠道。手机的定位功能还容易暴露涉密人员和涉密活动的位置，同时，如果手机被植入了特殊功能程序，还可实现遥控操作，使关机或待机的手机转为通话状态，在无振铃、无显示的情况下，将周围的声音发射出去，手机就变成了窃听器。由于手机携带方便，使用灵活，功能多样，信息繁杂，核心技术又掌握在国外厂商手中，安全可控性很低，加上使用者的保密意识淡薄等原因，管不住、管不实、管不好的问题比较突出。

（二）情报窃密技术先进，手段多样。近年来，境内外敌对势力针对我国的情报窃密活动更加激烈复杂，他们在运用传统窃密手段的同时，还利用高技术优势，大肆窃取、刺探、搜集我政治、经济、军事、外交等方面的情报。

1.对我通信及电磁信号和重要目标设施进行侦察监视。境外情报机构建立多种侦察平台，对我通信及电磁信号、重要目标设施等进行多层次、立体式、全方位、全天候的侦察监视。他们还利用移动通信系统的定位功能和语音识别、信息筛选、号码锁定等技术，有重点地对手机通信实施监控，监视和掌握我重要涉密人员的活动，侦测我党政军领导机关和重要军事设施的具体位置。如：近期，美国的“ 萨德系统 ”在韩国部署，虽然美韩一直将朝鲜威胁作为部署“ 萨德系统 ”的借口，但其针对中国的意图非常明显，会严重威胁到中国安全。

2.通过计算机信息网络攻击入侵我涉密信息系统。西方国家大都组建了专业的“ 黑客部队 ”。如，美国组建了专门负责网络作战的“ 司令部 ”，将网络部队正式纳入美军的作战序列；英国军情六处组建了一支由数百名计算机精英组成的黑客部队；日本防卫省组建了一支约5000人的网络作战部队，专门从事网络系统的攻防。这些黑客部队利用网络的漏洞，通过“ 后门程序 ”、“ 网络炸弹 ”、“ 僵尸网络 ”等手段攻击他国计算机信息系统，窃取秘密信息。据有关部门监测统计，这两年来我境内与互联网联接的用户，有60%以上受到过来自境外的入侵攻击。

3.对我重点涉密单位进行窃听、窃照。激光窃听器可以在1000米之内，窃听对面建筑物内的谈话，拍摄建筑物内的情况。计算机工作时产生的电磁泄漏信号，可以在一定范围内被接收还原，造成泄密。近年来，在我驻外使领馆发现大量窃密装置，甚至在我使领馆保密会议室内都发现了间谍机关安装的窃密装置。最近，我驻外某机构还发现，在当地购买的碎纸机内也安装有窃密装置，使用该碎纸机粉碎文件时，文件内容会被窃照，并转换成电磁信号发射出去。

（三）保密技术防护薄弱，管理制度不落实，泄密事件时有发生。总的说来，我国信息系统安全防范体系还在建设中，制度保障能力、基础支撑能力和技术对抗能力还相对比较薄弱，泄密隐患还十分严重。主要表现在：

1.计算机信息系统安全基础薄弱。最根本的是技术基础薄弱。目前，我们使用的通用计算机cpu芯片、操作系统主要是美国生产的，所使用的高端网络设备几乎全是国外产品，网络安全协议也都是国外制定的。核心技术掌握在他人手中，难以做到心中有数。比如，我国民航空中调度和金融、证券行业计算机信息系统的硬件设备、操作系统、数据库系统等，绝大多数是国外技术和产品。从不断披露的软硬件“ 后门 ”看，别有用心者完全可以通过远程控制窃取我秘密信息、瘫痪信息系统。一旦遇到紧急状况，必将受制于人，付出惨重代价。另外，在基础设施和物理安全方面也存在一些突出问题。这是一个很大的隐忧。

2.涉密信息系统保密管理薄弱。首先是有些部门单位不能做到涉密信息系统与保密设施同步规划

、同步建设。从近年对我县部门单位计算机信息系统保密检查的情况看，个别部门的涉密信息系统未经安全>>>>>>内容过长，仅展示头部和尾部部分文字预览，全文请查看图片预览。