高校师生保密知识读本

前 言

在高等学校中普及保密教育，不仅关系着国家安全与利益，关系着学校稳定与发展，也关系着高校师生自身成长与前途。为了使广大师生增强保密意识、了解保密常识，在教育部保密委员会办公室的指导下编写了本《读本》。

一方面，高校是我国高层次人才培养、科学研究、技术开发和服务国家战略的重要基地。高校师生发表论文、出版专著、学术交流和对外合作等活动非常频繁，保密管理工作难度大，面临的挑战越来越严峻。另一方面，高校培养的毕业生作为党和国家的宝贵人才资源，成为国家治理、资源管理、科学研究、工程实现、创新创业的生力军，其中很多职业和岗位都有保守国家秘密和其他秘密的要求，在学生时代加强保密意识的培养显得尤为急迫和重要。

一些境外组织利用网络聊天工具、校园论坛、招聘网站等渠道，打着“学术交流”“科研资助”“兼职就业”“招聘调研员”等幌子，以金钱等利益诱使极个别人收集情报、窃取国家秘密的事件时有发生。我们必须增强保密意识，提高防间谍、反窃密的警惕性，了解保密知识，筑牢保密防线，为维护国家安全和利益尽到自己的责任和义务。

本《读本》共 10 讲，38 个知识条目并选配了相应的案例，由北京交通大学国家保密学院韩臻、毕颖、杜晔、邵丽萍、李静、张大伟、周琼编写，韩臻负责全书统稿。参与《读本》编写工作的还有殷小彤、张汉姝、

崔永彪等。《读本》的编写还得到了国家保密局有关部门、单位的大力支持，征求并获得了相关单位和专家的意见与指导，引用或参考了相关资料和文献，在此表示衷心的感谢！

由于编者水平有限，《读本》可能有疏漏和不妥之处，敬请大家批评指正。

目 录

第 1 讲　保密的基本概念

1.1 保密的含义

保密，顾名思义，就是保守秘密。这里所称的秘密是指需要隐蔽和保护而不为他人所知的事物和信息。秘密是一种客观存在的社会现象，根据涉及的利益不同，大体上可以分为国家秘密、工作秘密、商业秘密和个人隐私等四类。保密是不让秘密泄露、保护其隐秘性的行为。保密行为基于人和社会组织的一种安全意识，对需要保护的事物和信息采取隐蔽措施，使之不被他人知悉、不被公之于众、不被泄露、不被他人窃取。

对保密的概念及其重要性的认识古已有之。孔子言：“君不密则失臣，臣不密则失身，几事不密则害成。”（春秋·子夏《易传·系辞上》）。

纵观古今中外，有很多事例表明保密与否直接关系到一场战役的胜败，左右整个战局的走向，甚至影响一个国家或政权的生死存亡。例如，二战时期，英国破译了德国的恩尼格玛密码，使得盟军能够预先知晓敌方大量的军事秘密，逐渐掌握了战争的主动权；美国对日本的通信破译也十分成功，在击落山本五十六座机和中途岛之战等关键战役中赢得了先机。盟军在保密领域的明显优势大大加速了战争进程，成为世界取得反法西斯战争胜利的重要基础之一。

党中央历来非常重视保密工作，从斗争实践中不断汲取经验教训，形成了优良的保密传统，为中国共产党领导人民走向胜利提供了至关重要的基础保障作用。

1.2 国家秘密及标志

《中华人民共和国保守国家秘密法（2010年修订）》（以下简称《保密法》）第二条明确规定:“国家秘密是关系国家安全和利益，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。”

依据该规定，国家秘密必须具备三个要素，缺一不可。

关系国家安全和利益，是构成国家秘密的实质要素，体现了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。国家安全和利益，主要包括国家领土完整、主权独立不受侵犯，国家经济秩序、社会秩序不受破坏，公民生命、生活不受侵害，民族文化价值和传统不受破坏等。在我国，国家安全和利益与广大人民群众的根本利益是一致的。“关系国家安全和利益”，是指某一事项一旦泄露会使国家安全和利益受到损害，主要包括危害国家防御能力，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，损害国家经济利益和科技优势，妨碍国家外交、外事活动正常进行，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等。

依照法定程序确定，是构成国家秘密的程序要素，体现了国家秘密的法定属性。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。“法定程序”由保密法律法规规定的定密依据、权限、方法和步骤构成。“依照法定程序”，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。

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，体现了国家秘密的限定属性。“在一定时间内”表明国家秘密有一个从产生到解除的过程，有明确的期限。“只限一定范围的人员知悉”表明国家秘密应当而且能够限定在一个可控制的范围内。机关、单位在确定国家秘密密级的同时应当确定其保密期限及其知悉范围，并在保密期限内采取严格保密措施，使之不超出限定的知悉范围。保密期限和知悉范围具有可控可查的限定边界。

国家秘密分为绝密、机密、秘密三个密级。国家秘密标志为：密级★保密期限、密级★解密时间、密级★解密条件。国家秘密标志是法定的文字符号标识，用以标明所标识的物品承载的内容属于国家秘密，并明确了其密级和保密期限。**例如：某文件首页左上角标有“秘密★10年”，就标明该文件属于秘密级国家秘密，保密期限10年。对该文件的阅读、流转、保存和销毁等必须按照相关保密规定进行管理。**

我们身边就有国家秘密。例如，**印制人民币所特有的防伪材料、防伪技术、防伪工艺等都是密级较高的国家秘密。《中华人民共和国人民币管理条例》明确规定：“印制人民币的特殊材料、技术、工艺、专用设备等重要事项属于国家秘密。”其相关事项和资料都会按确定的密级标记国家秘密标志，窃取或破解这些秘密的行为都是违法的。但人民币本身不是国家秘密，其发行时间、面额、图案、式样、规格、主色调、主要特征等是予以公开的。**

又如，高考、研究生入学考试试卷在开考前也属于国家秘密。

1.3 国家秘密的基本范围

《保密法》第九条规定：“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前款规定的，属于国家秘密。”

为规范准确定密，国家秘密及其密级的具体范围（简称保密事项范围）对国家秘密范围做了更为具体的界定和描述。保密事项范围是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，军事方面的保密事项范围由中央军事委员会规定。保密事项范围一般名称为“××工作国家秘密范围的规定”，包括正文和目录。其中，正文以条款形式规定保密事项范围的制定依据、本行业本领域国家秘密的基本范围、与其他保密事项范围的关系等内容；附件“××工作国家秘密目录”以表格形式列明国家秘密具体事项及其密级、保密期限、产生层级、知悉范围等内容。**例如，教育部和国家保密局 2018 年修订下发了《教育工作国家秘密范围的规定》。**

科学技术部和国家保密局2015年公布的《科学技术保密规定》规定：

关系国家安全和利益，泄露后可能削弱国家防御和治安能力，或者降低国家科学技术国际竞争力，或者制约国民经济和社会长远发展，或者损害国家声誉、权益和对外关系的科学技术事项，包括科学技术规划、计划、项目和成果等，应确定为科学技术中的国家秘密。主要有：不宜公开的国家科学技术发展战略、方针、政策、专项计划；涉密项目研制目标、路线和过程；敏感领域资源、物种、物品、数据和信息；关键技术诀窍、参数和工艺；科学技术成果涉密应用方向；其他泄露后会损害国家安全和利益的核心信息。同时规定：对于国内外已经公开的，或者难以采取有效措施控制知悉范围的，或者无国际竞争力且不涉及国家防御和治安能力的科学技术事项，以及已经流传或者受自然条件制约的传统工艺，不得确定为国家秘密。

1.4 保密的极端重要性

习近平总书记指出：“实现中华民族伟大复兴的中国梦，保证人民安居乐业，国家安全是头等大事。” 坚持总体国家安全观，必须坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，完善国家安全制度体系，加强国家安全能力建设，坚决维护国家主权、安全、发展利益。

国家安全是安邦定国的重要基石，国家安全和利益是国家生存和发展的必要保证，维护国家安全和利益是保密的目标。国家秘密是国家安全和利益的一种表现形式，是国家的重要战略资源。国家秘密一旦被泄露，必将危害国家安全，直接损害国家和人民的根本利益。保守国家秘密是一种

国家行为，也是一种国家责任，保密能力是国家能力的重要体现和保障。同时，国家秘密与人民群众的根本利益息息相关，保障国家秘密安全，从本质上讲是全国各族人民根本利益所在，是为了保障公民的正当权益。

当前，国际国内形势正在发生新的深刻复杂变化，世界处于百年未有之大变局，保密形势十分严峻，国家秘密安全面临新的挑战，保密工作是维护国家政治、经济、国防、外交、科技等领域安全的重要基础，保密的重要性和价值更加突出。

党的十八大以来，以习近平同志为核心的党中央高度重视保密工作，作出了加强和改进保密工作的新决策、新部署，提出了坚持党管保密、加强依法治密、加大创新力度、做好综合防范等一系列重大举措。

毛泽东同志说：“必须十分注意保守秘密，九分不行，九分九也不行，非十分不可。”他用通俗易懂的语言，阐明了保守国家秘密的极端重要性。

国防领域保密是保密工作的重中之重，如果秘密被窃取、出卖，造成的损失往往无法挽回。例如，被境外情报机构间谍策反的某军工集团研究所保卫干警刘某，伙同为所领导打扫办公室的工勤人员龙某，大肆窃取该所的军事技术情报并出卖。国家安全机关破获了该间谍窃密案，查获的文件资料86份共3288页，其中属于绝密级国家秘密1份、机密级16份、秘密级26份、情报38份。案发时刘某已三次将窃取的国家秘密送往境外，导致我方重要部署泄露，巨大投入被打了水漂，损失无法挽回。刘某和龙某被依法判处死刑。

关系到国家安全和利益的科技、经济和商务等活动，也越来越要注重保密，如果秘密被窃，将造成核心竞争力的丧失和极大的经济损失。例如，国外某公司上海办事处胡某等四人因刺探窃取中国国家秘密被刑事拘留，

之后以涉嫌侵犯商业秘密罪和非国家工作人员受贿罪被正式批捕。该案中相关秘密的泄露使中国企业在铁矿石进口谈判中处于不利地位，给中国钢铁行业带来了巨额经济损失。经法院审理，胡某被判处有期徒刑十年，其余三人分别被判处有期徒刑十四年、八年、七年。

做好保密工作是很多重要工作顺利进行的保障，如果发生泄密事件，工作就不能正常进行。例如，因某大学医学院口腔修复学教授王某和时任国家医学考试中心试题开发一处副处长孟某合谋故意泄露考题（启用前属于机密级国家秘密），致使原定进行的国家医师资格考试延期举行，造成恶劣的政治和社会影响及重大的经济损失。因故意泄露国家秘密罪，王某和孟某分别被判处有期徒刑三年。

在社会活动和治理中也有不少必须保密的情况，如果秘密泄露，会给相关工作带来极大被动，甚至影响社会稳定和安全。例如，2011 年 10 月 5 日，13 名中国船员在湄公河泰国水域被枪杀，是举世震惊的惨案。经中老缅三国警方 6 个多月的艰苦努力，先后抓获了糯康等一批武装贩毒集团湄公河惨案主犯。专案组成员，民警张某在办案过程中收受贿赂 5000 余元，向境外糯康势力泄露了案件侦办的一些秘密，增加了破案的难度。案发后，张某被判处有期徒刑四年。

1.5 保密的严峻形势

随着经济全球化和中华民族的复兴，我国已形成全方位对外开放的格局。国家间综合国力的竞争日趋激烈，利益博弈风云激荡，各种安全问题凸显，维护国家安全和发展利益的任务愈加复杂和艰巨，保密领域首当其冲，必然面临巨大挑战。我们必须坚定理想信念、忠诚爱国，提高警惕，不能有丝毫的懈怠和侥幸，更不能有贪念。

从外部看，境外势力对我实施的全方位信息监控和情报战略没有改变，对我窃密活动持续升级的基本态势没有改变。从内部看，我国多种所有制经济并存，对外开放进一步扩大，涉密领域不断延伸和扩展，涉密主体多元化，涉密人员流动复杂，保密管理难度持续加大。除了极个别丧失理想信念、资敌卖密的犯罪分子之外，一些人员保密意识淡薄、保密常识不知不会、不遵守保密规定，导致国家秘密面临过失泄密的巨大风险。

境外情报机构对我国各类信息情报特别是国家秘密的收集、刺探、收买等活动无孔不入、花样繁多，对我渗透策反和情报窃密活动猖獗。例如，2020年4月15日第五个全民国家安全教育日，国家安全部新闻办又对外披露了几起典型案件。其中，张某间谍案是一起危害军事安全、科技安全的典型案件。张某，在某国防军工研究所工作，案发前任高级工程师，研究领域涉及重要军事武器装备和尖端武器。张某在公派至某西方国家学习期间，该国情报人员隐蔽身份，经相关学者介绍，通过感情拉拢和金钱诱惑等方式与张某接触。随后，境外情报人员表明身份，将张某策反。张某向对方提供了我国军工科研院所、军工研究领域及相关武器装备等情况，收取对方报酬。张某回国后，继续利用工作便利，搜集了一大批我重要武器装备研究和生产等情报，并按照境外情报人员要求，计划在再次赴外参加学术研讨会时传递情报。国家安全机关提前掌握了张某出境传递情报的线索，及时实施抓捕，避免了危害扩大。案发后，张某被判处有期徒刑十五年。

又如，在校大学生庄某在某QQ群中寻求兼职。一个群成员主动申请添加庄为QQ好友，并向其提供“某军港附近地图信息采集和沿街商铺拍摄”的兼职工作。庄某按对方要求，将个人简历、定位信息和微信收款码通过QQ发送给对方，先后8次前往小区楼顶制高点、公园及医院附近，拍摄军

事目标及附近街道店铺、路况等，每次拍摄 100—200 张照片，通过邮箱发送给对方。庄某还应对方要求，通过网上购买长焦镜头观测及租船出海抵近观察等方式，先后 10 次赴某海军舰队实施观察和情报搜集。境外情报机关还对庄某进行了安全培训，要求以“观察记录为主、拍照为辅”的方式搜报军舰舷号。庄某因为境外非法提供国家秘密罪被判处有期徒刑 5 年 6 个月，剥夺政治权利 1 年。

再如，有关部门发现，某市某局人事科干部王某的工作电脑中除了日常办公文档，还有通过某通信系统接收，违规私自保存的 42 份标注密级的地形图。经鉴定，这些地图全部属于国家涉密测绘图，其中 31 份为机密级，11 份为秘密级，已被电脑中隐藏的窃密木马程序全部发往境外，对国防军工单位的安全带来很大隐患。王某因过失泄露国家秘密罪被立案查处，相关领导干部，因落实保密责任不到位，保密安全意识淡薄，也分别受到了处分。

信息化发展既促进了保密能力的提升，同时也对保密工作带来了持续的严峻挑战。网络和信息技术日新月异，包括国家秘密在内的信息存储和处理日益数字化、网络化，由此带来更加复杂多样的网络安全和信息保密问题，泄密渠道增多、窃密手段更加隐蔽。我国面临的计算机网络窃密风险一直居高不下。据统计，90%以上的窃密泄密事件涉及计算机和网络。

例如，2018 年 12 月《焦点访谈》播出的《网上谍影》就介绍了三起网络窃密案例。其中的一个案子是：某网络科技公司提供电子邮件系统安全产品，客户中有很多涉密单位。该公司安全防范意识淡薄，把客户的地理位置、网管人员身份、远程登录方式和账号密码等敏感信息储存在内网服务器中，并允许在外的员工通过一个 VPN 账号能随时从外网登录内网查询信息，为境外情报机构网络窃密打开了方便之门。经查，该公司的核心

应用服务器先后被三家境外情报机构实施多次网络攻击，大量敏感数据资料被窃取。事后，该公司及相关责任人受到了相应的处罚。

安全保密问题的综合性、复杂性、多变性明显加剧，传统安全威胁和非传统安全威胁相互交织，国家安全面临的威胁日益多样化，保密与窃密的斗争日趋激烈。别有用心的境外组织或人员，利用一些企事业单位和科研院所对外合作交流的迫切心情，挖空心思窃取我国家秘密和商业秘密，特别是在气象资源、矿产资源、海洋环境、测绘勘探、生物资源等领域，严重危害着我国家安全和利益。

例如，2018 年 10 月，科技部公布了一批行政处罚决定书，涉及六家机构违规采集、收集、买卖、出口、出境人类遗传资源的三起事件。其中一起涉及某知名基因测序公司和某重点大学附属医院，他们未经许可，在与某国外知名大学开展国际合作研究期间将部分人类遗传资源信息违规从网上传递出境。为进一步支持合理利用人类遗传资源开展科学研究、发展生物医药产业、提高诊疗技术，增强我国生物安全保障能力，提升人民健康保障水平，2019 年 5 月国务院颁布了《中华人民共和国人类遗传资源管理条例》（自 2019 年 7 月 1 日起施行）。其中，对采集、保藏、利用、对外提供我国人类遗传资源等方面的事项提出了更加明确的规定，以防止非法泄露。

1.6 保守国家秘密是公民的义务

国家秘密虽然只限知悉范围内的少数人员知悉，但保守国家秘密是我们每个公民的责任和义务。《中华人民共和国宪法（2018 年修订）》（以下简称《宪法》）第二章第五十三条明确规定：“中华人民共和国公民必须遵守宪法和法律，保守国家秘密，爱护公共财产，遵守劳动纪律，遵守公

共秩序，尊重社会公德。”《保密法》第三条规定：“国家秘密受法律保护。一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。任何危害国家秘密安全的行为，都必须受到法律追究。”

国家秘密知悉范围内的人员，必须严格遵守各项保密规定，保护所知悉、经管的国家秘密。国家秘密知悉范围外的普通人员，也必须履行法律义务，不得非法获取国家秘密，在国家秘密安全受到威胁时，应当采取保护措施并及时报告。任何泄露国家秘密的行为都将受到严肃的处罚。

例如，李某，研究生毕业后在某银行工作，在被上级单位借调工作期间，她明知文件首页标有“机密”标志的情况下，用手机将尚处于内部征求意见阶段的《关于规范金融机构资产管理业务的指导意见》及起草说明中的 36 张页面拍照后通过微信发给某银行经理郑某。郑某随后将文件照片转发给了其他人，导致该文件在多个金融行业微信群、微信公众号、微博及博客中不断转发，最终造成涉密信息在互联网上被大范围公开传播。李某违反保密规定，情节严重，其行为已构成故意泄露国家秘密罪，但鉴于其能自愿认罪，酌情给予了从轻处罚。最终她被判处有期徒刑一年，缓刑一年，个人前途毁于一旦。

又如，有关部门在工作中发现，国内某些知名数据库网站刊登了 1 篇内容敏感的论文。经鉴定，论文内容涉及秘密级国家秘密。论文作者是某大学研究生张某，其在帮助表弟齐某解决某涉密工程研发的技术难题时，擅自拷贝了部分涉密资料。之后，张某在撰写毕业论文时，经征求齐某同意后将上述涉密资料加工整理写入了学位论文。随后，论文刊登在了这些数据库网站上，造成泄密。事件发生后，齐某被党内警告处分，张某被批评教育。

对待保密工作，切莫存有侥幸心理。很多泄密事件都是因为侥幸、贪图方便造成的。所以，高校师生不仅要注重专业知识的学习和运用，也要学习《保密法》等保密法规和保密知识，绷紧保密这根弦。

例如，微信使用非常广泛，很多涉密人员也在使用，随之而来在微信上违规泄露国家秘密的行为也频繁发生。某天，某市市委某部门印发了部署相关敏感工作的涉密文件，下属某乡镇干部洪某领取文件后，认为事情紧急，又值深夜，就违反保密规定将该文件拍照后发至乡政府微信群，群成员杨某随之转发到了其他微信群，最后该涉密文件被数次转发到了多个微信群和微博上，造成大范围的泄密。事后，洪某和杨某都受到党纪政纪处分。

普通人在平时也要履行保守国家秘密的义务。例如在马路、公交车等公共场所看到遗失的涉密载体时，应立即拾起并及时交给公安民警；发现有人在军事管理区、军事禁区周围拍照，要立刻告诉站岗的哨兵或报警；当发现有危害国家安全的行为和线索时，要及时拨打国家安全机关举报电话 12339 举报；在网上发现有刊登、传递、存储国家秘密信息的，要及时拨打互联网泄密举报电话 010-55601919。对保守国家秘密有功的行为，有关部门会给予表扬和奖励。

例如，某高校的大二学生张某，警惕性很高，主动协助国家安全机关消除了间谍窃密的隐患。有一天，张某在登录QQ时发现有一封来自境外的电子邮件，他很好奇，这个陌生人为什么要给他发信息？就试着联系对方，对方随之给了回复。邮件来回几次后，张某就和这位所谓的境外友人互加了QQ好友。聊天时，对方自称叫王某，是某国一民间研究中心的成员，喜欢研究中国的政治、文化、军事，需要张某帮忙提供一些参考资料。张某本身也是军事爱好者，经常浏览各大军事网站、论坛，对境外间谍活动

有所了解，他在和王某聊天时，多留了个心眼，故意把自己说成是退役军人。一听是军人，这位“境外友人”的兴趣就更大了，王某随后给张某发来了一个聊天室链接，并强调可以给张某很高的酬劳，前提是必须提供一些涉及军事政治等方面的信息。到这时，张某确定，这位所谓的“境外友人”一定是境外间谍人员。张某就一边不动声色稳住对方，一边拨打了国家安全机关举报电话 12339。根据张某提供的线索，侦察员立即跟进查证，发现这个叫王某的人根本不在某国，他所说的某研究中心也不存在！在和张某联系期间，王某还以同样的身份与其他省市大学生联系，他的真实身份，是境外间谍人员！张某因此受到了表扬和奖励。

又如，出租车司机王某发现几名外国人随身携带不明设备在军事禁区附近逗留，就拨打“12339”反映情况。经国家安全机关调查发现这几名外国人有境外情报机构背景，欲通过地下探测设备刺探我军事秘密。王某因此获得了奖励。

而对于极个别经不起利诱，丧失理想信念，被拉拢策反，甚至主动出卖国家秘密的犯罪分子，必将受到法律的严厉制裁。

例如，黄宇，高校毕业后进入某涉密研究所工作。由于黄宇能力平平，工作态度也不端正，业绩靠后，按单位规定，他被解职。黄宇对自己被解职心怀不满，竟然主动勾搭某境外情报机构出卖国家秘密。至案发，黄宇共获取了 70 余万美元的赃款，出卖了 15 万余份资料，其中绝密级国家秘密 90 项、机密级 292 项、秘密级 1674 项，对我国党政军以及金融等多个部门的密码通信安全造成难以估量的危害和损失。黄宇还蛊惑同在涉密单位工作的妻子唐某违规把涉密资料备份带回家，乘机窃取；利用在同一单位担任总工程师的姐夫谭某使用私人电脑存储涉密资料的违规行为，趁姐夫不备，用间谍 U 盘偷偷拷贝了电脑里的涉密文档。黄宇因犯间谍罪被依法判处死刑，剥夺政治权利终身。其妻子唐某、姐夫谭某也因过失泄露国

家秘密罪被分别判处五年、三年有期徒刑。

又如，陈某，曾是某军工科研院所下属公司的一名网络管理员。该单位从事我国重要装备部件研发，属于核心涉密单位。有一天，陈某在公司门口“偶遇”了一名自称彼得的外国人，说作为技术专家想购买一些技术资料。在高额报酬的诱惑下，陈某开始向彼得提供情报信息。凭借从事网络管理的工作便利和权限，陈某窃取了大量的涉密文件和内部资料提供给彼得。陈某也意识到彼得并非普通的技术专家，而是一名间谍，心生恐惧的陈某提出了终止合作，但彼得却看透了他的性格和心理弱点，以陈某此前提供的情报为把柄，要挟恐吓他继续提供情报。在彼得紧逼下，陈某继续通过内网窃取了大量涉密材料。终日生活在恐惧中的陈某从单位辞职以图终止自己窃取情报的行为。经查，陈某共窃取并向境外间谍提供文件共5500多份，其中机密级国家秘密146份、秘密级1753份。陈某被判处无期徒刑，剥夺政治权利终身。

面对复杂的社会环境，高校师生要重视学习保密知识，增强保密和防间谍意识。不要以为现在是和平时期，间谍只是电影电视剧中才会有，或者只会出现在保密单位，普通人遇不到。被策反的很多案例中，当事人一开始都以为只是和对方简单的吃顿饭、聊聊天、交个朋友、相互帮个忙、拍个照片、邮寄个资料，不会有大问题，而都是被一步一步地引入陷阱，触碰出卖国家秘密的红线。境外情报机构在网络上以求职招聘、学术研究、商务合作、交友婚恋等各种名义为掩护，巧言令色，欺骗、勾联我社会人员甚至在校学生窃取出卖国家秘密的案子绝非个例。

例如，刚入学某高校的李某，有一天收到了一个来自陌生人的QQ好友邀请。对方自称陈某，生活在国外，最近在做军民融合项目调研，希望李某能够提供一些国内的相关信息，事成之后将支付丰厚的报酬。为了挣

钱，李某专门跑到学校图书室，收集相关资料，第一次收到了对方 1000 元钱。随后，他又按对方要求拍了《海军杂志》，还有七十周年国庆阅兵的相关信息，包括自己拍摄和网上收集的一些照片，又收到 400 元钱。李某竟丝毫没有意识到自己已经走上了出卖情报的危险歧路。所幸，他向境外传送照片的一举一动，早已被有关部门锁定。执法人员问讯了李某，李某竟然还声称：他拍的这些杂志，全部是公开发行的，怎么会涉密呢？幸亏有关部门及时查获，切断了李某与对方的联系，否则很有可能会被对方引诱进入收集出卖国家秘密和情报的犯罪深渊，后果不堪设想。

又如，李某，19 岁，在一家网吧上网时发现一个 QQ 网名“风骚小女人”的人申请加他为好友，并附言“你想发财吗？有份好工作等着你”。李某将对方加为好友并在发财梦的驱使下，收取对方汇款购置数码相机和摩托车，并发展某中学高二、高三学生 4 人为下线，按对方要求偷拍某军用机场飞机和设施，发送相关照片数百张换取“报酬”。国家安全机关侦破了此案，李某因非法获取国家秘密，被判处有期徒刑 3 年。

境外情报机构还以我驻外机构、中资企业、留学群体、出境团组为目标，采取诱蚀收买、圈套把柄、恶意执法、暴力胁迫、柔性强制等手段实施策反，严重危害我国公民人身安全。如遇此类情况，应该立即向我国驻外机构或国家安全机关报告，有关机构会依法处理，保护我国公民的安全。万一被人拉拢、利诱、威逼或者不慎落入圈套，也要做到悬崖勒马，及时坦白报告，一定要相信组织，使自己得到挽救。《中华人民共和国反间谍法（2014 年）》第二十八条规定：“在境外受胁迫或者受诱骗参加敌对组织、间谍组织，从事危害中华人民共和国国家安全的活动，及时向中华人民共和国驻外机构如实说明情况，或者入境后直接或者通过所在单位及时向国家安全机关、公安机关如实说明情况，并有悔改表现的，可以不予追

究。”

例如，某高科技企业驻某国分公司负责人李某主动向国家安全机关报告了境外情报机构对其骚扰的情况。该国情报机构长期将该企业驻当地分公司作为重点工作目标，曾将李某的前任抓捕审查4个月，但胁迫策反未果。李某接任后，对方通过严密监控，陆续掌握了他贿赂当地政府官员、在当地进行个人投资等情况，择机抓捕了李某，并以上述把柄胁迫他办理了充当间谍的手续。此后，对方多次布置李某刺探我驻外使馆、中资机构等情况。起初，李某出于个人利益考虑，未向公司报告，并向对方提供了部分情况。后来，李某逐渐认识到此事的严重后果，主动向国家安全机关作了报告。鉴于李某如实说明了被境外情报机构胁迫策反的经过，且有悔改表现，根据相关法规，他被免于追究刑事责任。

第 2 讲　保密工作方针和优良传统

2.1 保密工作的领导体制和管理体制

坚持党管保密是我国保密工作的政治优势和组织优势，是由我国基本制度所决定的，既是巩固党的执政地位、加强党的执政能力建设的重要内容，也是做好新时代保密工作的根本。

中共中央保密委员会是党中央统一领导全国保密工作的领导机构，各级党的保密委员会是党管保密的专门组织。下级保密委员会接受上级保密委员会的指导和监督。这是我国保密工作的领导体制。

中央和地方各级保密委员会下设办公室，与本级保密行政管理部门是“一个机构，两块牌子”，保密行政管理部门一般名称为“××国家保密局”。国家保密行政管理部门主管全国的保密工作，县级以上地方各级保密行政部门主管本行政区域的保密工作。机关、单位设立保密工作机构(例如：保密办、保密处)，或指定人员专门负责本机关、单位的保密工作。中央和国家机关在其职权范围内，管理或者指导本系统的保密工作。这是我国保密工作的管理体制。

中国共产党成立以来革命和建设的实践证明，保密工作的发展进步，都是在党中央的领导和指引下，由中共中央保密委员会部署实现的。我们必须始终不渝地坚持党管保密的原则，贯彻落实好中央领导同志关于保密工作的一系列重要指示精神，深入领会执行好中央关于保密工作的各项方针政策。

2.2 保密工作方针

保密工作方针，是指党和国家确定的关于保密工作的指导性原则和基本要求，对保密工作的开展以及落实保密方面的重大政策性问题具有重要的指导意义。

《保密法》第四条规定：“保守国家秘密的工作（以下简称保密工作），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。”

保护国家秘密，首先要以预防为主，做到未雨绸缪，防患于未然。“积极防范”就是以防止窃密泄密为目标，积极主动、关口前移，把保密工作落实在前面，前置保密措施，构筑人防、物防、技防的综合保密防范体系，及时发现和消除泄密隐患，堵住漏洞，从源头上防止窃密泄密事件发生，确保国家秘密安全。

国家秘密涉及的领域和范围广，必须分层分级分类管理和保护。“突出重点”就是要在全面管理好国家秘密的基础上，针对不同等级的管理对象，切实抓好重点领域和重要方面的保密工作，管住核心、管住要害、管住源头，确保核心秘密安全。

保密工作实现依法管理，是依法治国基本方略在保密工作中的运用和体现。“依法管理”就是要建立完备的保密法律制度，保密工作的方方面面都有法可依，保密行政管理部门必须依法行政、严格执法，认真监督、查处违反保密法律法规的行为并严肃追究法律责任。

在确保国家秘密安全的前提下，应当充分发挥信息资源共享和利用的优势。“既确保国家秘密安全，又便利信息资源合理利用”就是要“该保

则保”“该放则放”，做到依法保密、依法公开，处理好国家秘密保护和信息资源利用之间的平衡关系。

2.3 中国共产党的优良保密传统

习近平总书记强调：“历史是最好的教科书。学习党史、国史，是坚持和发展中国特色社会主义、把党和国家各项事业继续推向前进的必修课。”党的保密工作历史，是党史的重要组成部分。高校师生了解党的保密工作历史，继承和发扬党的保密工作优良传统，对进一步做好新时代保密工作，维护国家安全和利益，具有非常重要的意义。

从中国共产党创立到中华人民共和国成立，中国共产党领导中国人民所走过的道路极其曲折和艰难，为赢得革命胜利和民族解放付出了巨大代价。革命战争年代党的保密工作历史，是用革命先烈的鲜血写成的，经过历史的凝聚和锤炼，形成了坚定的理想信念、强烈的忧患意识、严格的纪律约束、紧紧地依靠人民、持续的技术对抗、领导的率先垂范等六个方面的保密工作光荣传统和优良作风，历久弥新，促人奋进。

（1）坚定的理想信念

理想信念是马克思主义政党团结奋斗的精神旗帜，是中国共产党人的安身立命之本，是中国共产党人的命脉和灵魂，也是党的保密工作优良传统的本源。革命战争年代，无数革命先烈在极其严酷恶劣的环境下，怀着对党绝对忠诚和革命事业必胜的理想信念，宁可牺牲生命，也要保守党的秘密。这些英雄壮举体现了共产党人的高贵品德，闪耀着党的保密工作优良传统的光辉。

例如，麻植（1905-1927 年），浙江青田人，1924 年考入黄埔军校，

同年8月加入中国共产党。1927年4月12日，蒋介石在上海发动反革命政变，大肆逮捕、屠杀共产党员和革命群众。4月15日，广东军阀在广州发动政变，全城搜捕共产党员和进步人士，麻植和同志们迅速撤离到南海县里水乡。安顿好同志们之后，麻植立刻返回广州去销毁其住处保存着的秘密文件。敌人的脚步声越来越近，他和留守的女交通员黄玉兰坚守在火炉旁，看着一件件文件化成灰烬。就在这时，敌人破门而入，他为保守党的秘密而被捕。没有得到文件的敌人恼羞成怒，试图从麻植口中得到党组织的秘密，连夜对他进行审讯。严刑拷打之下，他始终沉默，绝不泄露党的秘密。4月29日下午，麻植在广州黄花岗英勇就义，年仅22岁。1988年，邓颖超写信给浙江省青田县党史办：“半个多世纪以来，我常常怀念起麻植烈士，……。”

习近平总书记指出，理想信念是共产党人精神上的“钙”，理想信念坚定，骨头就硬，没有理想信念，或理想信念不坚定，精神上就会“缺钙”，就会得“软骨病”。理想信念动摇是最危险的动摇，理想信念滑坡是最危险的滑坡。在新的形势下，坚定理想信念、对党忠诚仍然是我们保守党和国家秘密的根本。

（2）强烈的忧患意识

自中国共产党成立以来，苦难的民族遭遇，严酷的斗争环境，激发了共产党人强烈的忧患意识，为做好保密工作磨练出了高度的警觉性。第一次国共合作期间，党的保密工作曾经有过惨痛的教训。我们党的一些同志，甚至是党的高级领导干部，对国民党右派缺乏应有的警惕，分不清敌友，将党员身份和党的核心秘密对国民党和盘托出。当第一次国共合作失败，国民党右派分子向共产党举起屠刀的时候，我们党几乎毫无防备，损失惨

重。八七会议之后，我们党痛定思痛，十天之内中央连续发出了《中央通告第三号-建立党内交通网》等六个关于加强保密工作的通告，决定建立党的秘密机关，特别强调要运用“精细的技术”来开展保密工作。第二次国共合作，我们党吸取血的教训，始终保持高度警惕，采取的方针正确，制定的策略得当，严格把握保密与公开的尺度，既保住了党和军队的秘密，又推动了抗日民族统一战线的形成，为夺取抗战胜利奠定了重要基础。我们党正是依靠牢固树立忧患意识，始终把保密当作关系党的生死存亡的大事，才领导人民取得了革命胜利，走到了今天的辉煌。当今世界各种利益纷争错综复杂，强烈的忧患意识和高度的警惕性，依然是我们做好保密工作的前提。

例如，中共中央政治局于 1927 年 8 月 7 日在汉口召开的紧急会议，简称“八七会议”，是在极端秘密的情况下举行的。首先，是会址的选定。会议地点选在汉口德国租界内一个俄国人居住的洋房楼上。这座洋房前临僻静街道，后通幽曲小巷，且屋顶凉台与邻屋相连，一旦发生紧急情况，方便与会人员迅速撤离。其次，是会议通知的发出慎之又慎。在当时的局势下，稍有疏忽，后果不堪设想。因此，八七会议通知的发出是非常审慎的，特别选派了熟悉武汉街道的同志亲手送达，并反复交待哪个代表从前门进，哪个代表从后门进。再次，是代表吃住的安排。从安全的角度考虑，一切从严、从简、从快，代表们用以充饥的面包和稀饭，都是由房子的女主人卓莫娃操办的。8 月上旬的武汉，是酷暑季节，但因为形势险恶，开会的地方代表们只能进不能出，睡的是地铺，门也不能开，如同在烤箱里。为了防止中暑，与会者每人发给一包仁丹，这是当时力所能及的防暑措施。会议虽然只开了一天，但会议的保密措施十分严谨，工作特别细致，全程保持了高度的警觉，从而保障了八七会议在敌人眼皮子底下的顺利进行。

（3）严格的纪律约束

没有铁的保密纪律，就没有党的秘密安全。党的二大通过了第一个党章，规定了党的纪律，**“凡党员泄露本党秘密者，该地方执行委员会必须开除之”**。这一规定是党的保密纪律和制度的源头，严格执行党的保密纪律成为党的传统和一贯作风。革命战争年代，严守党的秘密就是共产党人不可逾越的一道政治红线。

习近平总书记在十八届中央纪委三次全会上指出，遵守党的纪律是无条件的，要说到做到，有纪必执，有违必查，不能把纪律作为一个软约束或是束之高阁的一纸空文。

人不以规矩则废，党不以规矩则乱，守纪律、讲规矩、严守党的秘密，是一个严肃的政治原则问题。2015 年，党中央在县处级以上领导干部中开展的“三严三实”专题教育，就包括严格执行党的保密纪律的要求。各级党的组织、国家机关和涉密单位，要敢抓敢管，把严守保密纪律、保密法规和保密规矩作为领导干部和涉密人员的基本行为准则，使党的保密纪律和国家保密法规制度真正成为带电的高压线。

例如，1927 年 4 月 12 日，蒋介石在上海发动了震惊中外的四一二反革命政变。之后，四川、江苏、浙江、福建、广西、广东、湖北等省，相继发生共产党人和革命群众被屠杀的惨案，党的创始人和领导者李大钊等 20 人在北京牺牲。在这极端危急的关头，中共中央为挽救革命形势，决定在南昌举行武装起义。这次起义的组织工作必须高度保密，容不得一丝一毫的泄漏，担任前敌委员会书记、领导起义的周恩来严格执行党的保密纪律，对他相濡以沫的妻子邓颖超也不曾说。邓颖超在《一个严格遵守保密纪律的共产党员》一文中回忆说：“恩来同志，七月十九日，要离开武汉

的时候，在晚饭前后才告诉我，他当晚就要动身去九江。去干啥，呆多久，什么也没有讲。我对保密已成习惯，什么也没有问。当时，大敌当前，大家都满腔仇恨。我们只是在无言中紧紧地握手告别。这次分别后，不知何日相会？在白色恐怖的岁月里，无论是同志间，夫妇间，每次的生离，实意味着死别呀！后来还是看了国民党的报纸，才知道发生了南昌起义。”

（4）紧紧地依靠人民

我们党来自人民、植根人民、服务人民，党的根基在人民、血脉在人民、力量在人民。失去了人民的拥护和支持，党的事业就无从谈起。土地革命战争时期，国民党军队对中央苏区实行严密封锁和一次又一次疯狂“围剿”，中央红军能够取得四次反“围剿”的重大胜利，很重要的一条就是紧紧依靠苏区人民严守红军和中央机关的秘密；抗日战争时期，沦陷区人民面对日寇穷凶极恶、惨无人道的一次又一次“扫荡”，主动为八路军、新四军保守秘密，使敌人成了“瞎子”“聋子”；解放战争期间，胡宗南大举进攻陕甘宁边区，党中央撤离延安，转战陕北，隐蔽在人民群众之中，就是依靠边区人民保守秘密，确保了安全。历史证明并且还将证明，人民群众永远是我们党的保密屏障，是我们做好保密工作的基础。

例如，1942 年 8 月，新四军十四旅四十一团政委罗通率 7 个连组成鄂南抗日游击队掩护新四军主力北撤。罗通不幸染上了恶疾，由于当时条件艰苦，他的病情日益加重。鄂南地方武装军事部长雷同焦急万分，经过慎重考虑决定把罗通送到附近的维持会长黄子英家养病！

黄子英表面上当着日本人的维持会长，暗地里却帮助共产党抗日。他虽只是咸宁曹家井村一个普普通通的农民，但具有强烈的爱国思想，颇具正义感和同情心，还曾掩护过雷同。接到罗通时，黄子英坚定地对雷同说：

“你放心，我以全家性命担保，一定把你朋友照顾好！”

一天晌午，几个日军突然闯入黄子英家。原来，他们听说有一位新四军在这一带养病，便派出大批人马拉网式搜查。黄子英临阵不乱，一边赔着笑脸，一边递上香烟，信誓旦旦地说：“鄙人维持的地方，都是大大的良民，如若查出新四军，但凭皇军处罚。”有了维持会长的保证，日军将信将疑地离开了。当晚，黄子英就把罗通等人悄悄转移到家南边500米处后山的地窖里。第二天，日军果然又包围了曹家井，逼着黄子英把村民集中起来训话：“谁要是交出新四军或说出新四军的下落，皇军大大有赏，要是从谁家搜出来，就统统杀头。”乡亲们默不作声，日军又把村子搜了个遍，一无所获，抢夺了一些村民的财物后扬长而去。

日军离开后，黄子英又把罗通接回家中细心照料。罗通渐渐康复，临别前，罗通紧紧握住黄子英的手，激动地说：“是咸宁人民给了我第二次生命，我会永远记住咸宁人民的恩情！”

（5）持续的技术对抗

我党在大革命时期就提出了“保密技术工作”的概念。那时保密技术非常原始，主要是采用密写技术，通信联络采用代号、隐语。1928年，中央开始培养无线电和密码通信人才。1930年1月，中央在上海第一次秘密开通对香港的地下电台联络。1931年，周恩来亲自编制了第一本密码，称“豪密”，党的密码通信从此诞生。在长征中，在抗日战争和解放战争时期，党中央及中央军委与各地的联系和作战指挥，主要是靠密码通信。我党我军依靠保密技术与反动势力对抗，取得了骄人战绩。

例如，1947年7月，为了应对复杂严峻的形势，与敌人展开技术对抗，确保密码通信安全，周恩来在陕北连续召开机要通信会议，研究改进密码电台和通信保密问题，决定在山西临县孙家沟建立军委通信总台，在河北

平山建立固定辅助通信基地，建立了与全国各根据地、各战区及国统区秘密联络的后方大功率电台，负责收转中央与各地来往电报；给前委配备了4部15瓦小型移动电台，跟随毛泽东、周恩来、任弼时工作；各野战军和各根据地军队均配置与中央和中央军委进行通信联络的小型移动电台；总前委与前线部队之间往来密电，一律由军委通信总台接转，上下两级移动小型电台一般情况下不直接发生联系；跟随毛泽东和总前委工作的小型移动电台，不断变换，交替使用，随时改变发报位置，情况紧急时，间断关闭电台，转入“静默”状态，以确保位置不被泄露。

胡宗南进攻延安时，决定使用美国最新侦测设备侦测我总前委电台位置，以摸清毛泽东、周恩来的行踪，实施斩首行动。我潜伏人员熊向晖第一时间将有关计划完整地密报了中央，包括集中侦测时间和方位等。中央立即决定关闭所有电台，密码通信“静默三天”。这一措施，彻底粉碎了敌人的偷袭阴谋。

当今世界，科学技术特别是信息技术迅猛发展，国家秘密的存储、处理方式发生了根本性变化，网络进入各级党政机关和涉密单位。我们必须懂得，网络信息是跨国流动的，没有网络安全，就没有国家安全，没有信息化，就没有现代化。我们必须在享用信息化便利的同时，继承和发扬党的保密工作优良传统，切实加强保密技术研发和应用，不断提升技术抗衡能力，采用先进技术防护手段，精细地保护好党和国家秘密。

（6）领导的率先垂范

我们党的许多领导人既是党的保密工作创始人，更是执行保密规定的模范。毛泽东、朱德、周恩来、邓小平等老一辈无产阶级革命家在保密工作方面都是全党的楷模，为我们树立了永远的学习榜样。

今天，保密工作形势发生了深刻变化，在实现中国梦的伟大历史进程中，保密依然是绝对重要的头等大事，各级领导的率先垂范对于做好保密工作至关重要。党政领导干部保密工作责任制对各级党政领导干部在保密工作中的责任作了明确规定，是我们继承和发扬党的保密工作优良传统的制度保障。

例如，1941 年春，中办机要处一位同志给毛泽东送去一份秘密电报。电报稿没有用信封封装，而是从这位同志上衣口袋里掏出来的，这个细节引起了毛泽东的注意。他严肃地对这位同志说：“秘密文件放在衣兜里传递，是很不利于保密的。”他边说边从办公桌上抽出一张毛边纸，题写了“保守机密，慎之又慎”几个大字。这位同志回到机要处，特别慎重地将毛泽东题词送交机要处负责人李质忠，并汇报了经过。机要处立即将这幅题词工整地贴在当时办公的窑洞里，并作为机要保密工作的“座右铭”。从此之后，“保守机密，慎之又慎”，成为一代又一代保密工作者恪守不渝的保密箴言。

2.4 入党誓言中熔入的保密承诺

保守秘密是党的优良传统之一，中国共产党对保守党的秘密的重视充分体现在历届的党章里，并熔入了入党誓言中。

土地革命时期虽然没有统一入党誓词，但各地党组织都规定在入党时要宣誓，使用的誓词主要有：“努力革命，阶级斗争；服从组织，牺牲个人；严守秘密，永不叛党。”“我自愿加入中国共产党，服从党的纪律，为共产主义奋斗终生，严守秘密，誓不叛党。”“中华民国×年×月×日在×地以至诚加入中国共产党，愿永久遵守下列誓词：一、遵守党纲党章和纪律；二、绝对忠实为党工作永不叛党；三、保守党的秘密；四、服从党的一切决议；五、经常参加支部生活和活动；六、按时缴纳党费。如有

违上列各项愿受党的严厉纪律制裁。”

抗日战争时期，中组部起草发布了标准的入党誓词：“我宣誓：一、终身为共产主义事业奋斗；二、党的利益高于一切；三、遵守党的纪律；四、不怕困难，永远为党工作；五、要作群众的模范；六、保守党的秘密；七、对党有信心；八、百折不挠，永不叛党。谨誓。”

解放战争时期，各地党组织大都继续采用之前的入党誓词，也有一些根据当时的情况进行了补充，典型的有中共冀南区党委组织部印制的入党志愿书内的入党誓词为：“我自愿立誓参加共产党，永远跟着共产党毛主席走，一心一意为人民服务，个人利益服从党的利益，坚决执行党的决议，遵守党的纪律，保守党的秘密，遵守民主政府的法令、群众的决议，在任何情况下不动摇，不妥协，不怕困难与牺牲，为新民主主义和共产主义的实现而奋斗到底。”中共东北局宣传部编印的《共产党员课本》中收录的入党誓词：“我决心加入中国共产党，诚心诚意为工农劳苦群众服务，为新民主主义和共产主义事业干到底，自入党以后，努力工作，实事求是，服从组织，牺牲个人，执行命令，遵守纪律，保守秘密，永不叛党，如有违背，愿受党纪严厉制裁，谨此宣誓。”

新中国成立初期，入党仪式及誓词在党章中没有明文规定，中组部指示各级党组织应根据党章的内容在新党员入党志愿书中写出誓词，并在支部大会上声明。被广泛使用的誓词是：“我志愿加入中国共产党，拥护党纲党章，执行党的决议，遵守党的纪律，保守党的秘密，随时准备牺牲个人的一切，为全人类彻底解放奋斗终身。”

1982 年 9 月，党的十二大通过的《中国共产党章程》，正式载入了入党誓词并沿用至今，其第一章第六条明确规定：“预备党员必须面向党旗进行入党宣誓。誓词如下：我志愿加入中国共产党，拥护党的纲领，遵守

党的章程，履行党员义务，执行党的决定，严守党的纪律，保守党的秘密，对党忠诚，积极工作，为共产主义奋斗终身，随时准备为党和人民牺牲一切，永不叛党。”

第3讲　保守国家秘密的法律制度

3.1 我国保密法律制度体系

保密法律制度是中国特色社会主义法律制度的重要组成部分。我国保密法律制度体系经过多年的建设，构建了以《宪法》为依据，以《保密法》为核心，以保密法实施条例及相关保密法规、规章和标准为配套的保密法律制度体系。保密工作总体上实现了有法可依、有章可循，为推进保密依法行政和治理方式创新奠定了坚实基础。

我国现行保密法律制度体系，主要由以下七个部分构成。

（1）宪法。《宪法》第五十三条明确规定了保守国家秘密是一项宪法性义务。

（2）保密法律。保密法律是指全国人大常委会制定的专门的保密法律和全国人大及其常委会制定的有关法律中涉及保密的法律条款。《保密法》是我国保密法律体系的主干，是我国调整保密法律关系的专门性、综合性法律。除了专门的《保密法》之外，我国的《刑法》《国家安全法》《反间谍法》《网络安全法》《密码法》《公务员法》《出境入境管理法》《统计法》和《档案法》等法律中涉及国家秘密的条款，也属于保密法律体系的重要内容。例如，《刑法》对故意泄露国家秘密罪，过失泄露国家秘密罪，非法获取国家秘密罪，非法持有国家绝密、机密文件、资料、物品罪，为境外窃取、刺探、收买、非法提供国家秘密罪的规定等。又如《出境入境管理法》中，关于“对查获的违禁物品，涉及国家秘密的文件、资料以及用于实施违反出境入境管理活动的工具等，公安机关应当予以扣押，并依

照相关法律、行政法规规定处理”的有关规定等。

（3）保密法规。保密法规是对《保密法》及其有关保密法律规定的具体化，保密法规包括保密行政法规和地方性保密法规。保密行政法规主要包括国务院颁布的条例、办法和细则中有关保密条款的规定，如《中华人民共和国保守国家秘密法实施条例》《中华人民共和国政府信息公开条例》。地方性保密法规包括省、自治区、直辖市以及设区的市人民代表大会及其常务委员会制定的保密法实施细则，或在其他地方性法规中规定的保密管理制度等。

（4）保密规章。保密规章主要由国家保密行政管理部门、中央和国家有关机关和省、自治区、直辖市以及设区的市的人民政府制定的保密规章、保密规范性文件，也包括其他规章中的保密条款和法律授权部门对保密法律规定的解释。保密规章一般具有行业或地域特点，具有较强的实用性和可操作性。例如，1992年国家保密局、中央对外宣传小组、新闻出版署、广播电影电视部颁布的《新闻出版保密规定》，2014年国家保密局颁布的《国家秘密定密管理暂行规定》，2015年科学技术部、国家保密局颁布的《科学技术保密规定》，2017年国家保密局颁布的《泄密案件查处办法》，2018年科学技术部印发的《国家科学技术秘密定密管理办法》等。

（5）相关司法解释。最高司法机关在司法实践中，对相关罪名的具体适用标准作出了详细的司法解释，指导司法实践。例如，《最高人民检察院关于渎职侵权犯罪案件立案标准的规定》对于故意泄露国家秘密和过失泄露国家秘密应予立案的规定；《最高人民法院关于审理为境外窃取、刺探、收买、非法提供国家秘密、情报案件具体应用法律若干问题的解释》

对人民法院审理相关案件，如何适用《刑法》作出了规定。

（6）国家保密标准。国家保密标准是一类特殊的强制性国家标准，由国家保密行政管理部门归口组织制定、发布、管理。国家保密标准主要涵盖涉密网络、涉密专用计算机、电磁泄漏防护、安全保密产品等多个领域，涉及技术标准、管理标准和测评与检查标准等，适用于全国各行各业、各单位对国家秘密的保护工作，在国家秘密产生、处理、传输、存储和销毁的全过程中都应严格执行。

（7）国际公约或政府间协定的相关规定。在国际交往中，根据国际公约和有关政府间协定的规定，在我国承担公约义务的范围内，我国政府也会承担相关保守秘密的义务。

3.2《保密法》的主要内容

新中国成立之始，党中央就作出了一系列加强保密工作的决定。1951年6月，中央人民政府政务院令发布了我国第一部保密法规《中华人民共和国保守国家机密暂行条例》。1988年9月，全国人大常委会审议通过《中华人民共和国保守国家秘密法》，2010年4月做了修订。修订后的《保密法》自2010年10月1日起施行。2014年1月，国务院颁布了《中华人民共和国保守国家秘密法实施条例》，自2014年3月1日起施行。

现行的《保密法》共六章五十三条，对国家秘密的范围和密级，保密制度，监督管理和法律责任等作出了明确规定。

第一章“总则”，共八条，主要明确了立法宗旨，适用范围，国家秘密概念，保密工作方针，保密工作管理制度，机关、单位保密工作职责以及保密奖励制度等。其中第一条规定了《保密法》的宗旨：“为了保守国

家秘密，维护国家安全和利益，保障改革开放和社会主义建设事业的顺利进行，制定本法。”

第二章“国家秘密的范围和密级”，共十二条，主要规定涉密事项范围和密级范围，定密工作体制，定密责任和权限，定密工作内容和流程，国家秘密的变更和解除，以及不明确或者有争议事项的确定等。

第三章“保密制度”，共二十条，主要规定国家秘密载体、涉密信息系统、信息发布、涉密采购、对外交往和合作、涉密会议活动、保密要害部门部位、军事禁区与涉密场所、从事涉密业务的企业事业单位、涉密人员等方面的保密管理制度，并针对危害国家秘密安全的行为作出禁止性规定。

第四章“监督管理”，共七条，主要规定保密行政管理部门制定保密规章和标准，宣传教育，保密检查，保密技术防护，泄密案件查处，定密监督，密级鉴定和处分监督等职责。

第五章为“法律责任”，共四条，主要规定严重违规行为的法律责任，机关、单位发生重大泄密案件和定密不当的法律责任，互联网及其他公共信息网络运营商、服务商的法律责任，以及保密行政管理部门工作人员的法律责任。

第六章“附则”，共两条，是关于军事保密法规和本法施行日期的规定。

3.3《保密法》确定的主要制度

《保密法》及其实施条例适应中国特色社会主义建设新形势、依法治国新要求、信息技术新发展、信息公开新需要，针对保密工作新情况新问

题，从定密、计算机网络、涉密人员、保密资质、信息公开保密审查、涉外保密等方面作出了全面的制度性规定。《保密法》确定的制度主要包括以下几个方面。

（1）保密工作责任制度。《保密法》第七条规定，机关、单位应当实行保密工作责任制。保密工作责任制主要包括：领导干部保密工作责任制，机关、单位保密工作责任制，涉密人员保密工作责任制，保密行政管理部门保密工作责任制等。

（2）定密制度。定密是指机关、单位依法确定、变更和解除国家秘密的活动，是保密工作的源头。《保密法》就定密专门确立了定密责任人制度、定期审核制度等，规范了定密程序和要求。

（3）涉密人员管理制度。《保密法》按照责任与权益相一致的原则，确立了涉密人员管理制度。主要内容包括：分类管理制度、上岗审查培训制度、出境管理制度、脱密期管理制度、涉密人员合法权益受法律保护等。

（4）涉密载体保护制度。《保密法》就国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁等作出了规定。

（5）涉密信息系统保护制度。《保密法》就涉密信息系统保护规定了一系列保密措施，按照涉密程度实行分级保护，加强技术防护，针对信息系统和信息设备使用过程中存在的安全保密问题作出了严格规定。

（6）信息公开发布保密审查制度。公开发布信息应当遵守保密规定。坚持“谁公开、谁审查”以及事前审查和依法审查的原则。

（7）涉外保密审批制度。《保密法》规定了机关、单位对外交往与

合作中需要提供国家秘密事项，或者任用、聘用的境外人员因工作需要知悉国家秘密的，应当报国务院有关主管部门或者省、自治区、直辖市人民政府有关主管部门批准，并与对方签订保密协议。

（8）涉密会议、活动保密制度。《保密法》对举办会议或者其他活动涉及国家秘密的，要求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。

（9）保密要害部门部位保密制度。《保密法》规定了机关、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，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。

（10）企业事业单位从事涉密业务保密审查制度。《保密法》规定，从事国家秘密载体制作、复制、维修、销毁，涉密信息系统集成，或者武器装备科研生产等涉及国家秘密业务的企业事业单位，应当取得相应保密资质。机关、单位委托企业事业单位从事上述涉密业务，应当与其签订保密协议，提出保密要求，采取保密措施。

（11）保密法律责任制度。保密法律责任是确保《保密法》有效实施的重要保障，《保密法》规定了十二种违法行为的责任，规定了机关、单位因违规发生重大泄密案件和定密不当时对直接责任人员的处分，规定了互联网及其他公共信息网络运营商、服务商的责任，规定了保密行政管理部门工作人员的违规责任。

第 4 讲　涉密人员和涉密载体的保密管理

4.1 涉密人员的保密要求

涉密人员，是指在涉密岗位工作的人员。涉密岗位，是指在日常工作中产生、经管或经常接触、知悉国家秘密事项的岗位。我国对涉密人员坚持以岗定人的原则，只要在涉密岗位工作的人员就应当确定为涉密人员。依据涉密岗位的分级，涉密人员分为核心涉密人员、重要涉密人员和一般涉密人员。

涉密人员是国家秘密产生、使用和管理的直接主体。涉密人员能否自觉履行保密责任和义务，管理和使用好国家秘密尤为重要。国家秘密能否得到有效保护，涉密人员具有决定性的作用。

高校是我国科研活动的重要阵地，不少学校承担着涉密的国家重大科研或军工项目，一些学生也在老师的指导下直接参与其中并接触到涉密事项，项目涉密事项的参与人员就应该被确定为涉密人员。

2016 年 11 月，国务院学位委员会、教育部、国家保密局印发的《涉密研究生与涉密学位论文管理办法》还专门给出了涉密研究生的解释，其第二条“本办法所称涉密研究生是指直接参与涉及国家秘密的教学、科研项目、任务等工作或者在教学、科研过程中接触、知悉、产生和处理较多国家秘密事项的在读研究生。在职攻读学位的研究生，已被确定为涉密人员，确因教学、科研需要，接触、知悉、产生和处理国家秘密的，依据涉密人员相关规定进行管理”，并规定“涉密研究生一般只能接触、知悉、

产生和处理秘密级国家秘密事项”。“培养单位确定涉密研究生，应在研究生开展涉密内容研究或涉密学位论文开题前，由研究生本人提出申请、导师确认，经培养单位按程序审查批准，签订保密协议。”

涉密人员的保密管理要求主要包括任前审查、上岗培训、在岗管理和离岗离职管理等，对此，《保密法》都作出了相关规定。

（1）任前审查。《保密法》第三十五条规定：“任用、聘用涉密人员应当按照有关规定进行审查。”用人单位的组织人事部门、保密工作机构应根据审查对象拟进入岗位涉密等级确定审查内容并开展调查。涉密人员有明确的禁用条件，有如下情况的人员不得任用、聘用为涉密人员：不具有中华人民共和国国籍或者获得国（境）外永久居留权、长期居留许可的，有犯罪记录的，曾被开除公职的，曾因严重违反保密规定被调离涉密岗位的，有吸毒、酗酒和赌博等不良嗜好的，等等。

涉密岗位用人审查不严是造成泄密事件的重大隐患，特别是对于临时借调或聘用人员，或者工勤人员等，只要其工作内容能够接触到国家秘密，就必须对其进行正式的保密审查和教育培训。

（2）上岗培训。《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。”涉密单位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，培训合格后还要签订保密承诺书才能上岗。

涉密人员未经保密教育培训，缺乏保密意识和保密常识造成的泄密事件屡有发生。例如，有一天，某单位工作人员陶某在加班过程中，由于急于传达某文件精神，将一份密码电报拍照上传至微信群中，后被大规模转发，造成了泄密事件。经了解，陶某入职不满1年，虽然已被确定为涉密人员并签订了保密承诺书，但尚未接受系统的保密教育培训，对涉密载体种类形式、泄密渠道等了解不够，第一次接触密码电报类文件，未注意到其标注的密级与保密期限，导致了过失泄密的后果。事后，有关部门给予陶某记大过处分，相关责任人也受到了相应的处分。

又如，有关部门在对某单位进行保密检查时发现，多名工作人员在连接互联网的非涉密计算机中违规存储处理多份涉密文件资料，部分人员还存在违规通过互联网电子邮箱传递涉密文件的情况。经查，该单位大量借调下属事业单位人员帮忙工作，其中许多岗位涉及制作、复制、收发、传递、保管国家秘密载体，但该单位几乎从不对这些人员进行必要的保密教育培训。事发后，有关部门给予该单位多名责任人党纪政纪处分。

（3）在岗管理。涉密人员在岗管理主要包括在岗教育培训、遵守保密规章制度、接受监督检查、重大事项报告、出境和从业限制、发表文章和著作的保密审查、以及权益保障。相关单位在与涉密人员签订任（聘）用合同或者劳动合同时，应当增加保密条款，对离职离岗脱密期管理要求进行约定。对于涉密研究生，规定每年应接受不少于4个学时的保密专题教育培训，导师是研究生在学期间保密管理的第一责任人。

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，严禁私自为境外机构、组织或者人员提供劳务、咨询和其他服务。涉密人员在岗期间对下列重大事项应当及时报告：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。

《保密法》第三十七条规定：“涉密人员出境应当经有关部门批准，有关机关认为涉密人员出境将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。”为了国家安全，也为了保护自己和家人，千万不要因为对法律无知而走上犯罪的道路。**例如，某单位重要涉密人员苗某，没有经过单位批准擅自携妻儿赴某西方国家滞留不归，并在其后加入了外国国籍。几年后，苗某在回国探访时被国家安全机关抓获。苗某因犯叛逃罪被判处有期徒刑两年。**

（4）离岗离职管理。离岗离职管理主要包括涉密载体清退、签订保密承诺书与脱密期管理。涉密人员离岗离职前，应清退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、涉密信息设备等纸介质、光、电、磁介质涉密载体。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。涉密人员离岗离职时，单位应与其签订离岗离职保密承诺书，进行保密提醒谈话，明确涉密人员离岗离职后应履行的保密义务以及违反保密承诺的法律责任。对于涉密研究生，规定“涉密研究生因毕业、涉密工作结束等原因不再接触国家秘密事项的，培养单位应对涉密研究生进行保密教育谈话，告知其承担保守国家秘密的法律义务，严格核查、督促清退所有涉密载体，掌握其就业、去向等相关情况，并与其签订保密协议”。

《保密法》第三十八条规定：“涉密人员离岗离职实行脱密期管理。

涉密人员在脱密期内，应当按照规定履行保密义务，不得违反规定就业，不得以任何方式泄露国家秘密。”**例如，某国有企业负责机要工作的合同制员工韩某因考上公务员，打电话向所在部门领导和组织人事部门告知离职事宜，并请他人代办离职手续，其本人则未按规定回企业进行涉密载体清退与交接。后该企业在清退文件时发现，韩某存放在保密柜中的2份秘密级文件下落不明。案发后，韩某受到行政警告处分。**

4.2 涉密载体的保密要求

涉密载体是国家秘密载体的简称，它是国家秘密的主要存在形式。涉密载体是以文字、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及其同形载体（例如影像胶片、缩微胶片等）、光介质、磁介质、半导体介质等各类物品。

涉密载体从制作、收发、传递、使用、复制、保存、维修到销毁，要全程做好保密管理。除了涉密载体之外，还有属于国家秘密的设备和产品（简称密品），其研制、生产、运输、使用、保存、维修和销毁，应当符合相关的保密规定。

（1）涉密载体制作与复制。制作与复制涉密载体，应在单位内部或在保密行政管理部门审查批准的定点单位进行。制作涉密载体，应标明密级和保密期限，注明发放范围、制作数量及编号；制作场所要符合保密要求，使用电子设备的应当采取电磁泄漏发射防护等措施；制作过程中形成的无需归档的材料应及时销毁。机密级、秘密级涉密载体的复制、摘录、引用、汇编应当按照规定报批，并履行登记手续，复制件加盖复制单位复印戳记，并视同原件管理，不得改变密级、保密期限和知悉范围。汇编涉

密文件资料形成的秘密载体，应当按其中的最高密级和最长保密期限管理。绝密级涉密载体，不得复制和摘抄，确有工作需要的，必须征得原定密机关、单位或其上级机关的批准。

一些工作人员保密纪律松散，对涉密载体管控不严，导致不该看的看了，不该抄的抄了，不该印的印了，不该改的改了，该保密的不保等违规事件屡禁不绝，成为泄密的严重隐患。**例如，某高校教授张某为研究课题到某机关档案室查看文件与资料。档案室管理员刘某违规把张某带入档案室的涉密库房，把最近几年与课题有关的文件（部分涉密）拿出来让张某查阅。张某在查阅过程中看到一份标着“机密”的文件对课题涉及问题的表述十分全面，就请刘某帮忙扫描。刘某扫描文件后删掉了密级标志，把扫描电子稿刻入光盘交给了张某。张某回校后把文件存进了自己连接互联网的笔记本电脑中，并在移动硬盘中留了一个备份。后来，该文件被张某的学生赵某刊登在自己的博客上，导致文件被大规模传播。事件发生后，张某和刘某受到了党纪政纪处分。**

（2）涉密载体收发与传递。涉密载体在收发过程中，应严格按照收发程序办理，履行清点、编号、登记和签收手续。传递涉密载体，应按规定通过机要交通、机要通信或者其他符合保密要求的方式进行，禁止通过普通邮政、快递等寄送，禁止委托无关人员捎带。指派专人传递时，应选择安全的交通工具和交通线路，并采取相应的安全保密措施。执行传递任务时，不能携带涉密载体进入无关场所或办理与任务无关的其他事情。

例如，某天，某市机要部门通知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

职但尚未接受保密教育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份机密级文件首页拍照，并实时在其亲友微信群中发布，造成泄密。事后，周某和赵某分别受到了相应的处分。

又如，某省地矿局下属的环境监测院专职安全员曹某有一天丢失了两份秘密级文件。经查，曹某到地矿局办公室领取了上述涉密文件，在换乘公交车时，疏忽大意，不慎将文件遗失。曹某发现文件丢失后，立即前往公交调度站寻找文件，自查无果后报告了所在单位。事件发生后，有关部门给予曹某党内严重警告处分并调离机要岗位，给予负有领导责任的院长办公室主任李某和党群办公室主任包某党内警告处分，并责成该院院长黎某、党委书记牛某作出书面检查。

（3）涉密载体使用。使用涉密载体有严格的保密规定，以防止涉密载体在使用过程中被非法扩散。阅读和使用涉密载体，要按规定办理登记、签收手续，在符合保密要求的办公场所进行，确需在办公场所以外阅读和使用的，应遵守有关保密规定。传阅涉密文件资料应当由经办人员负责，专夹传阅，登记文件份数、编号和阅读时间等，阅读者之间不能横传；阅读者不能擅自抽出、留存密件，未经批准不得抄录涉密内容。借阅、借用密件，要经过借出单位主管领导批准，不属于该项国家秘密知悉范围内的单位和人员，不能借予；归还所借密件时，要当面办理清点、销号、退还手续。传达国家秘密时，凡不准记录、录音、录像的，传达者应当事先声明。

例如，有关部门在工作中发现，某州委门户网站刊登多份涉嫌泄密的文件。经鉴定，涉案文件中有1份机密级、3份秘密级国家秘密。经查，

该州州委工作人员吕某在起草文件时，摘编了有关涉密文件内容，但未按规定标注密级，后被不知情人员当作非涉密文件上传到州委门户网站，造成泄密。事发后，有关部门给予吕某行政记过处分，给予负有领导责任的杨某党内警告、行政记过处分。

（4）涉密载体保存。保存涉密载体，应当选择安全保密的场所和部位，配备必要的保密设施和设备，并定期进行清查、核对，发现问题及时报告。离开办公场所，应当将涉密载体存放在保密设备里。按照规定应当清退的涉密载体，应及时如数清退，不得自行销毁。

例如，有关部门在工作中发现，1份标有某市信访局单位编号的涉密文件复印件在上访人员中流传，而该文件的原件却完好地保存在当地信访局，没有发生过丢失。经调查，当地上访人员吴某在信访局等待接访时，发现一间办公室未锁门且无人值守，办公桌上放有涉密文件。吴某阅读文件后认为内容对其有利，便将此件偷出，复印后放回原处，全程未被人发现。原来，该局办公室文秘姜某在案发当日按照领导布置将该文件送局长阅示，见局长一直在办公室与人谈话不便进入，就随手把文件放在了自己的办公室桌上，出门办其他事时忘了把文件放进保密柜，离开时也没有锁门，被吴某乘机窃取复印，导致泄密。事后，姜某受到了严厉的处分。

（5）携带涉密载体外出。携带涉密载体外出，要经过审批，并采取严格的保密措施，使涉密载体始终处于有效管控之下。严禁未经批准私自携带涉密载体外出。参加涉外活动，一般不得携带涉密载体，确需携带机密级、秘密级涉密载体的，须经单位负责人批准。

例如，某造船厂职工何某，曾擅自存储涉密文件至私人移动硬盘，并私自携带回家，在途中被抢。报案时，何某隐瞒实情，公安机关追回硬盘后，发现其中存有文件资料75份，其中机密级8份，秘密级63份。何某

因犯非法持有国家机密文件罪和过失泄露国家秘密罪，被判处有期徒刑一年零两个月。

（6）涉密载体维修。涉密载体维修应由本单位专门技术人员负责；确需外单位人员维修的，要在本单位内部进行，并指定专人全程现场监督，严禁维修人员读取或复制涉密信息；确需送外维修的，应送保密行政管理部门审查批准有维修资质的定点单位进行，并在送修前拆除信息存储部件。

例如，某单位规划处王某在自己的涉密计算机出现开机故障后，找到计算机管理员洪某，希望能让计算机供货商过来维修，但王某没有告诉洪某出故障的是涉密计算机。某外资品牌的计算机售后服务部派人上门维修发现该电脑硬盘已严重损坏，由于还在保修期内，便更换了一块新的硬盘，顺便带走了原来的硬盘，王某、洪某两人均未阻拦。最终，这块硬盘被寄到某国的客服总部。事后，王某、洪某因违反保密规定受到了严厉处分。

（7）涉密载体销毁。涉密载体需要销毁的，单位应当履行清点、登记、审批手续，并送交保密行政管理部门设立的销毁机构或指定的单位销毁。在送销前应存放在符合安全保密要求的专门场所，送销时应当分类封装、安全运送，并派专人现场监销。因工作需要，单位自行销毁少量涉密载体时应使用符合国家保密标准的销毁设备和方法。涉密载体销毁的登记、审批记录应当长期保存备查。

例如，有一次，公安部门在某大学食堂外一书摊上查获两捆文件，共计938份，其中机密级96份，秘密级339份。据摊主交待，这批文件是从某废品收购站买来的，准备转手倒卖。经核查，文件是某学院等单位作为废品卖给废品收购站的，其中该学院卖出的废品包括文件资料301份（

机密级95份、秘密级13份，非密文件193份），其余637份无法查实归属。事后，上级部门给予该学院党委、纪委通报批评，当事人李某被行政处分。

第 5 讲　使用信息设备的保密要求

5.1 使用计算机和网络的保密要求

就保密管理的角度，计算机分为涉密计算机和非涉密计算机两类。涉及存储、处理国家秘密的计算机应当确定为涉密计算机，非涉密计算机不得存储、处理国家秘密。涉密计算机按照存储、处理信息的最高密级分为绝密级、机密级和秘密级。计算机应严格实行分类分级的保密管理。

涉密计算机和涉密网络必须与互联网及其他公共信息网络物理隔离。使用计算机和网络时必须遵守“涉密不上网（指互联网等公共网络），上网不涉密”的基本要求。

涉密计算机应当按照其密级标注密级标识，并严格按照规定或标准设置开机口令和系统口令。应根据所在场所的实际情况对涉密计算机采取相应的电磁泄漏发射防护措施。

涉密计算机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、无线键盘等无线设备，不得擅自卸载、修改涉密计算机安全保密防护软件和设备，不得安装未经审核、特别是来历不明的软件，不得随意拷贝他人的文件资料，不得处理与工作无关的事务。

严禁使用非涉密计算机和非涉密移动存储介质存储、处理、传输涉密信息。移动存储介质不得在涉密计算机和非涉密计算机之间交叉使用，以防止涉密计算机被摆渡攻击植入木马等恶意软件。涉密场所中连接互联网的计算机不得安装和使用摄像头等音视频输入设备，以防止被窃听窃视。

违规将涉密计算机、涉密存储介质等涉密设备接入互联网及其他公共

信息网络造成泄密的事件时有发生。例如，某涉密单位工作人员邓某违规将涉密计算机接入互联网，被境外情报机构用窃密软件窃取了数十份涉密文件。邓某因过失泄露国家秘密罪被判处有期徒刑两年六个月。

又如，某计算机公司工程师张某违规将涉密计算机接入互联网，该机被境外情报机构植入木马并远程控制，导致 1019 份文件资料失控，其中机密级国家秘密 1 份。事发后，张某被开除，其所在部门副总经理、总经理和公司主管副总裁分别受到了撤职、党内警告和行政警告处分。

违规使用非涉密计算机、非涉密存储设备以及公共信息网络存储、处理、传递国家秘密信息的泄密事件频发。例如，有一天，一份涉密文件被刊登在某县中学的门户网站上，造成泄密。经查，该县教育局办公室主任马某为及时组织传达某会议精神，向县委某部门办公室主任周某索要有关文件。周某手中的文件来自其上级部门办公室主任洪某，洪某在明知该文件涉密的情况下，指示办公室副主任王某用QQ在线传给了周某。随后，周某用QQ邮箱传给了马某，马某将该涉密文件上传至县教育系统QQ群，被某中学办公室主任下载后发布在了学校的门户网站上。事发后，洪某、周某受到党内严重警告处分，王某受到党内警告处分，负有领导责任的领导被诫勉谈话、责令作出书面检查。

又如，有关部门在工作中发现，某县公共网上刊登一份涉密文件。经查，该县某单位工作人员任某曾以记录员身份参加了一个学习会议。为准确掌握学习内容、完善会议记录，任某在未履行借阅审批手续的情况下，向机要员刘某借了一份秘密级文件，并擅自将文件全文录入本人使用的连接互联网的计算机中。过后，任某又不慎将该文件作为非涉密文件上传至信息网络中心，被不知情工作人员发布在网站上。事发后，有关部门给予任某党内严重警告处分，刘某党内警告处分。

5.2 使用手机等通信设备的保密要求

不得使用普通电话机、传真机谈论或传输涉密信息。传真涉密信息，必须使用国家密码管理部门批准使用的加密传真机。加密传真机只能传输秘密级和机密级信息，绝密级信息应送当地机要部门译发。

使用普通手机，不得涉及国家秘密和其他敏感信息，不得连接涉密信息系统、涉密信息设备或其他涉密载体，不得利用涉密计算机充电，不得携带进入涉密场所或参加涉密会议，不得在涉密公务活动中开启和使用位置服务功能；不得使用境外机构、境外人员赠送的手机，不得使用未经国家电信管理部门进网许可的手机；在申请手机号码、注册手机邮箱或开通其他功能时，不得填写禁止公开的涉密单位名称和地址等信息。

智能手机等移动智能设备的使用越来越广泛，已成为隐患巨大的失泄密渠道，甚至是“定时炸弹”。智能手机在上网、接收彩信、扫二维码、领取红包、下载安装应用时，很容易被植入窃密木马等恶意软件，甚至成为功能强大的“窃听器”“偷录机”。手机定位功能还有可能造成涉密人员和重要涉密单位位置信息的泄露。因此，必须提高警惕，严格遵守使用手机的相关保密规定，包括社交媒体软件使用的安全保密要求。

例如，某单位办公室副主任肖某，为向在外检查工作的分管领导汇报工作，找到保密员赵某查阅文件，擅自用手机对一份机密级文件部分内容进行拍照，并用微信发送给在外的领导。案发后，有关部门撤销了肖某办公室副主任的职务，并调离办公室岗位；给予负责管理涉密文件的赵某行政警告处分；对负有领导责任和监管责任的李某、秦某和邵某进行诫勉谈话，并责令作出书面检查。

又如，有一天，多个微信群中传播了一份涉密文件，造成严重泄密。

经查，某单位在内部招待所组织学习有关会议精神，学习人员刘某在房间学习阅读时，接到同事邹某的聊天微信，无意中聊到刘某正在阅读某涉密文件，勾起了邹某的兴趣，就让刘某讲讲其关注的部分内容。刘某虽意识到这是涉密文件，不能传播，但人情面子和侥幸心理压倒了保密意识，觉得邹某是铁哥们、又是同事，应该不会泄露出去，遂将有关内容拍照后微信给了邹某。邹某看后很感兴趣，向刘某索要全文，刘某竟花了2个多小时的时间将文件主要部分拍照微信给了邹某。邹某随即把部分照片分享到了自己的微信群，并整理成完整的文档传给了其好友王某，王某又转给了其朋友和同事，并被这些朋友和同事通过微信在更大的范围内扩散，造成大范围泄密。事后，刘某受到留党察看一年、撤职处分，并调离原岗位，邹某受到撤职处分。

5.3 使用办公自动化设备的保密要求

复印、打印、扫描涉密文件资料，需经审批并在相应的涉密设备上进行。复印机、打印机、扫描仪、多功能一体机等办公自动化设备也跟计算机一样存在信息泄露的风险，处理涉密信息的办公自动化设备也不得连接互联网等公共信息网络，与涉密计算机之间的连接不能采用无线方式。非涉密设备不得复印、打印、扫描涉密文件资料。

涉密复印机应安放在符合保密要求的场所，并指定专人负责管理。复印涉密文件资料，需即送即印，并履行签收手续。打印涉密文件资料时应进行审计记录，打印输出的涉密文件资料应按照相应密级进行管理。复印打印过程中产生的废页、不合格件和多余件必须及时按要求销毁。

涉密办公自动化设备和计算机等涉密设备，在维修时要严格按照涉密载体维修的相关规定执行。淘汰、报废涉密办公自动化设备应进行清点、

登记，经单位主管领导批准后，送交保密行政管理部门指定的销毁机构销毁，禁止转送、捐赠他人，更不能当作废品出售或随意丢弃。

目前使用的复印机都配备有内置硬盘，存储了复印过的内容，而且其数据格式一般都是专用的，往往难以清除，泄密风险极高。例如，某从事房地产工作的网友去某图文公司复印客户资料，几天后发现专属于公司的客户资料竟不胫而走，被竞争对手挖了墙脚。这些客户材料从未外传，怎么会？她百思不得其解。很快，技术人员将目标锁定那几台复印机，结果发现存留在复印机中的各种信息竟多达4万余份，内容包括医疗记录、个人薪酬、保单信息等许多个人隐私，复印机俨然成了“泄密炸弹”。

又如，有一次，有关部门在检查中发现，某涉密研究院违规复印大量涉密文件资料。经查，该研究院为召开涉密产品会议需要印制大量文件资料，因单位办公区刚刚启用，尚未配备复印设备，且因已过下班时间联系不到其他涉密单位承担印制工作。为了不耽误会议按期举行，负责会议材料准备工作的文秘处处长李某找到副院长张某，建议到研究院周边的某图文复印店复印，该复印店没有涉密资质。张、李两人商量纠结再三后，决定由李某和文秘处工作人员王某去该店印制含涉密内容的会议材料，虽采取了一定的安全防护措施，但已严重违反了保密规定，给国家秘密造成很大的泄密风险。事后，张某被党内严重警告处分、并处罚款，李某被党内严重警告处分、并处罚款，王某被通报批评，负有领导责任的研究院院长钱某、党委书记孙某被通报批评、责令书面检查、并处罚款。

第 6 讲　网络活动中的保密

6.1 身份鉴别中的信息保密

身份鉴别是指在信息系统中确认操作者身份的过程，即确定用户的真实性，是构筑信息安全的第一道防线。身份鉴别信息是掌握在用户手里的首要秘密，必须谨防泄露。**例如，我们在日常工作生活中使用的计算机登录、邮箱登录、网站登录和手机开机登录的口令就是身份鉴别信息的关键部分，都应该保密。**身份鉴别方法一般分为“用户知道什么”“用户有什么”和“用户是什么”三大类，它们可以结合在一起使用。

最为常用的口令认证是典型的“用户知道什么”的方式。口令又可分为静态口令和动态口令。静态口令指用户登录系统的口令在使用过程中是固定不变的，除非用户主动更改。**例如：大家登录邮箱、网站、APP 等通常需要输入用户名/口令就是典型的静态口令登录方式。**动态口令是指用户持有一个能生成强口令的令牌，令牌上显示的口令随时间或登录次数而变化。**例如：一些网络银行在用户注册时会发放一个动态令牌，在用户登录时需要输入令牌上的新口令才能登录。**

“用户有什么”，信息系统中可以通过用户所持有的电子钥匙或电子证书等认证令牌来进行身份鉴别，包括磁卡、智能卡、USB Key、PKI 证书等。**例如：大家在日常生活中使用的二代身份证、校园卡、银行卡都属于智能卡，登录网络银行时使用的 U 盾是 USB Key 产品。**

“用户是什么”是根据用户自身生物特征或行为特征来进行身份鉴别的方法，包括指纹识别、虹膜识别、人脸识别、声音识别、击键习惯等。

例如：智能手机中普遍支持的刷脸登录，支付APP中广泛使用的指纹支付、人脸支付等都是生物特征识别技术。但生物特征一般不可修改，且需采集用户生物特征信息并存储，可能带来较大的隐私泄露和鉴别失效的风险。

在上网和使用信息系统时，应特别注意保护身份鉴别中的信息和个人隐私的安全。在使用口令时，不要使用弱口令，应设置足够强度的口令并定期更新，安全级别不同的设备或网站上应使用不同的登录口令，防止“撞库攻击”。“撞库”是黑客通过获取用户在A网站的账户和口令去尝试登录B网站的一种常见攻击手段，一些用户在不同网站使用相同的账号和口令导致了撞库攻击有机可乘。

高安全要求时，应选择使用口令+物理令牌或生物特征识别的双因子鉴别方式。在使用生物特征识别时，应注意保护个人特征信息，对于信任度不高的网站或系统，应避免生物特征识别信息的注册和使用。

因身份鉴别信息泄露造成巨大损失的事件经常发生。例如，12306购票网站早期曾遭受撞库攻击，导致用户账号、口令、身份证号码、手机号码和电子邮箱等敏感信息在内的13万余条用户数据在互联网上流传。“123456”“a123456”“123456a”等弱口令首当其冲。

6.2 上网和通信过程中的泄密风险与防范

互联网和手机通信网络都是开放式的互联网络，信息流动便捷高效，对敏感信息和个人隐私的保护提出了挑战。上网和通信过程中的泄密风险主要包括通信过程中的泄密风险、网上信息存储的泄密风险和网上信息发布的泄密风险。

用户在连接互联网的过程中需通过多种信息传输设备和有线或无线

信道连接到远程服务器。目前大部分的网络都没有采取加密信息传输，明文上网数据在信道传输的过程中极易被窃取、篡改，其中的敏感信息和个人隐私更是黑客攻击窃取的首要目标。

此外，用户的大量信息存储在互联网上。许多互联网厂商提供了便捷的云存储服务，越来越多的用户将各种信息存储在云端服务器，如注册账户、文本信息、音视频多媒体数据，其中不乏敏感信息的存在。由于安全意识淡薄、防护手段缺失，这些包含了敏感或个人隐私信息的数据存在着极大的泄露风险。**例如：媒体上报道的各类网上数据泄露事件，经常涉及我们广泛使用的各类门户网站、云盘存储和网上论坛等。**

随着网络新媒体技术的不断发展，用户可采用多种形式便捷地将各种信息发布到互联网平台上。但在这一过程中，许多敏感信息也会有意或无意地随同发布到互联网上。而网络平台又具有传播迅速、覆盖面广、难于删除的特点，因此极易造成大规模的泄密事件发生。**例如：网上媒体平台经常爆料的各类涉及公民个人隐私等敏感信息的“热点新闻”就是不当信息发布的典型代表。**

用户在上网和通信过程中应采取有效措施保护敏感信息和个人隐私的安全。不使用普通电子邮件等通信工具在互联网等公共通信网络上处理、传输敏感信息；选择安全的信息通信信道和连接设备，如使用安全连接（https）浏览网站；不使用陌生环境中的无线路由器联网；网上存储信息要设置好相应的访问权限，避免公开共享；信息发布前应严格审查，避免敏感信息被发布到互联网。

上网通信过程中的泄密事件频繁发生。**例如，有关部门曾发现某知名建筑行业论坛违规登载大量地质资料图，其中部分涉及国家秘密。经查，**

某软件工程公司承接了一个地理信息综合应用系统项目，涉及使用一套含涉密资料的区域地质图，该公司员工顾某参与了原图数字化工作。顾某未经公司同意，擅自将扫描图压缩并分批发送至其电子邮箱，当作网络硬盘使用，在自己租住处处理加工数据。与顾某共租一处的王某也是同业人员，觊觎这些有一定经济价值的地质图，遂偷窥了顾某的电子邮箱账户名和口令，窃取了顾某违规存储在邮箱内的扫描图（未标密）。王某随后在行业论坛上发布了168幅地质图，其中有两幅属于秘密级国家秘密。事后，合同甲方依据签订的保密条款向该软件工程公司追索了全部经济损失并撤销了合同，顾某被公司解除劳动合同，相关责任人员被保密部门诫勉谈话和批评教育。

6.3 恶意代码的窃密风险与防范

恶意代码又称为恶意软件，是能够在计算机系统中进行非授权操作的代码，这些恶意代码在侵入信息系统后就会进行信息窃取、复制传播、非法操作等破坏活动。恶意代码感染可造成计算机系统的运行异常、性能下降、敏感信息泄漏等问题。常见的恶意代码包括：程序后门、逻辑炸弹、木马、病毒、蠕虫和僵尸网络等种类。通过恶意代码进行攻击是常用的窃密手段，在窃密方面使用较多的是木马程序，木马一旦被执行，恶意者将获得计算机的控制权，并可以神不知鬼不觉地做任何事情。例如：曾经广泛传播的“QQ 爱虫”“code red”“熊猫烧香”“网银大盗”“灰鸽子”“弼马温”和“Wanna Cry”等都是非常著名的恶意软件，其中不乏各种木马。

通过技术和管理手段防止恶意代码传播到敏感信息设备上可有效抵御此类攻击。常用的防护措施有：安装防病毒、防木马软件并定时进行查

杀、更新；不下载和安装来历不明的计算机程序；不轻易点开可疑邮件的附件程序；不轻易点击可疑的链接；不在计算机上连接不安全的移动存储介质；对于重要的敏感或涉密信息系统，应严格采取物理隔离措施。

面对恶意代码的渗透和攻击，绝不能掉以轻心。类似“震网”这样的网络武器级恶意代码甚至能突破物理隔离的屏障。例如，2011 年，中东某国突然宣布暂时卸载首座核电站的核燃料，因为电站遭到“震网”病毒攻击，1/5 的离心机报废。一种名为“震网”的蠕虫病毒，逐步侵入了核电站的工业控制软件，并可夺取对一系列核心生产设备的关键控制权。“震网”的传播方式是通过U盘交叉使用，从而打破了物理隔离网络的边界安全防护，将恶意代码植入关键系统中而实现了攻击。

通过恶意代码实施有组织的窃密攻击时有发生。例如，某境外组织曾利用特种木马，通过控制多个境外跳板设备对我国某行业数十台计算机设备实施高强度网络攻击活动。攻击者精心伪装窃密行为，所用特种木马平时处于静默潜伏状态，接收到远程控制指令后才会激活运行，整个过程十分隐蔽，防不胜防。

6.4 钓鱼和挂马网站的窃密风险与防范

网络钓鱼和挂马网站是用户上网浏览时易遭受的两类攻击。常见的网络钓鱼包括钓鱼邮件和网页仿冒等，通过发送附有恶意代码的钓鱼邮件使受害者上当，或通过仿冒正规网站来欺骗用户登录到恶意网站，是社会工程学欺骗原理与网络技术相结合的典型攻击行为。用户登录到钓鱼网站后，如果输入敏感信息，如个人账户、口令等，就会被攻击者获取，造成敏感信息泄露。攻击者就会用窃取的这些信息登录用户的个人账户并实施下一步的侵害。网页挂马是通过在网页中嵌入恶意程序或链接，致使用户

计算机在访问该页面时被植入恶意程序，这是黑客传播恶意程序的常用手段。用户的计算机一旦感染上恶意程序，就面临着被攻击的风险。

防止钓鱼和挂马网站的防护措施主要有：不点击接收来源不明的可疑邮件及其附件；安装防病毒、防木马的软件并定时进行查杀、更新；不登录不熟悉的网站，键入网站地址的时候要仔细校对；不轻易点击可疑的链接，仔细观察短链接并小心核对打开的网页；对于提供安全链接（https）的网站，应仔细检查网站证书的合法性。

建立假冒网上银行、网上证券网站，骗取用户账号和密码是钓鱼网站的常见手段。例如：曾出现过的假冒中国工商银行的网站，网址为http://www.1cbc.com.cn，而真正银行网址是http://www.icbc.com.cn，钓鱼网站利用数字1和字母i非常相近的特点来欺骗用户。

钓鱼和挂马网站也是实施有组织网络窃密攻击的常用手段。例如，某境外组织曾仿冒我国某军工领域重点单位邮件登录界面，专门搭建钓鱼攻击平台，冒用“系统管理员”身份向该单位多名人员发送钓鱼邮件。该单位职工王某点击了钓鱼邮件，输入了个人邮箱账号和口令，导致其电子邮箱被秘密控制。随后，该组织定期远程登录王某的电子邮箱收取邮箱内文件资料，并利用该邮箱向王某的同事、下级单位人员发送数百封嵌入木马的钓鱼邮件，导致10余人下载点击中招，相关计算机被控制。

第 7 讲　科研和学习活动中的保密

7.1 科研活动中的保密

高校承担涉密科研项目，通常都是项目下达单位已经定密且明确了相关保密要求。学校和项目组应按照与项目下达单位签订的保密协议或合同中的规定严格做好各项保密管理工作。高校也可以依据自身的定密权限对开展的科研项目依法定密。

为确保涉密科研的安全，应贯穿涉密科研项目论证、申报、立项、实施、结题、验收的全过程做好保密管理工作，包括：项目密级分解工作，与协作配套单位签订保密协议；制定项目各个环节的保密制度，采取保密措施，落实保密责任，组织参加人员签订保密承诺书；加强涉密科研项目文件、资料的管理；完善涉密科研场所人防、物防、技防等措施；结题时要明确评审专家的保密要求；加强成果验收、申报奖项、申请专利、发表论文等方面的保密管理。含有涉密内容的项目建议书、项目申请书、开题报告、调研报告、方案论证书、立项报告、分包合同书，年度报告、阶段测试报告、关键技术报告、研究报告、验收鉴定申请书、技术总结报告、用户使用报告、测试报告、成果申报表等，都应纳入涉密载体的管理范围。

高校科研工作中泄密事件时有发生。**例如，某大学重点实验室副教授乐某，是机密级国家安全重大基础项目子课题负责人。乐某违规通过电子邮箱将机密级课题协议书发送给合作单位，被有关部门截获。事发后，乐某受到行政警告处分，三年内取消承担涉密项目的资格；负有领导责任的实验室负责人崔某作书面检查。**

又如，某大学教师董某在参加某市电子政务项目设计工作时，接触到了一些涉密文件资料。项目结束后，董某为了方便自己使用，未经批准，私自留存了这些文件资料，并将内容录入到自己的非涉密计算机里，后又将涉密内容编入了课件发布在学校网站上，造成泄密。

还如，某大学教师郭某和王某在科研工作中借用了一些涉密资料，违规将其存储在连接互联网的家用计算机中，造成泄密。郭某和王某分别受到了党内警告和行政记过处分。另一高校教师吴某和课题组多名学生私自使用连接互联网的非涉密计算机存储和处理涉密项目相关文档，案发后，该教师和涉案学生均受到了相应的处分和处理。

另外，在校期间参与过涉密项目的高校毕业生一定要遵守保密协议中的各项要求，严格履行脱密期规定，在应聘和就业过程中，特别是对于外资企业，不得暴露参加过涉密项目的敏感背景，有效保护自己身份，降低成为策反对象的风险。

7.2 发表论文或报告的保密

发表论文或撰写报告是高校师生展现学术水平与学术成果的重要工作。由于涉密科研人员是涉密科研项目的实际参与者，涉及了调研、方案设计、实验分析、数据处理等环节，掌握了大量的关键涉密信息，在论文和报告的写作中就可能涉及敏感内容。因此，应对公开发表论文和报告的内容进行严格的保密审查。

审查人员包括研究生导师、项目负责人、领域专家和单位保密工作负责人等，审查时要针对论文和报告内容提出专业性审查意见，并经业务主管部门审查后，报学校保密管理部门备案。参与涉密科研项目的师生发表与项目有关的论文或报告，必须预先经过保密审查，确认不涉及国家秘密

的，才可以投稿。

因发表论文不慎而造成泄密的案件发生过多起。**例如，某法学网站刊登了一篇内容敏感的论文，经鉴定属于秘密级国家秘密。经查，论文作者为某政法大学在职研究生赵某，他同时是某省政法机关的科长。赵某在撰写论文时，利用工作之便，未经领导审批，擅自引用了有关涉密文件的内容。赵某将论文提交导师杨某审阅，未说明引用了涉密文件。杨某通过电子邮箱将文章投给某法学网站及4家学术期刊，被网站录用并刊登，造成泄密。事发后，有关部门给予赵某党内严重警告、行政撤职处分，对杨某进行通报批评。**

7.3 涉密学位论文的保密

学位论文主题、研究方向、主要内容或成果涉及国家秘密的，开题前，导师和研究生必须获得涉密论文的撰写资格，导师与研究生原则上为涉密人员、参研涉密项目，学位论文及相关资料应根据所涉及研究任务的密级定密。界定为涉密论文后，其研究过程以及开题、中期检查、论文评阅、答辩和学位审核等环节的有关工作，需按照国家对涉密论文的有关要求进行。

涉密学位论文的起草、研究、实验、存储等应当在符合保密要求的办公场所进行，撰写及修改必须在涉密计算机上进行，并在封面或首页标注国家秘密标志，严禁使用非涉密计算机和非涉密存储介质处理涉密内容。涉密学位论文的打印、复印和装订等制作过程应符合保密要求，送审应当履行清点、编号、登记、签收等手续，必须采用密封包装，并通过机要交通、机要通信或者专人的方式递送。

涉密学位论文应按照保密管理要求和流程及时完成归档工作，研究生本人不得私自留存涉密学位论文。涉密学位论文未解密公开前，不得对外公开。保密期满后，如需对外公开，应对该涉密学位论文进行保密审查，满足解密条件并履行解密手续后，方可对外公开。

在撰写涉密学位论文和论文发布的过程中，违规泄密的案例也有多起。**例如，某网站曾刊登了一篇硕士学位论文，经鉴定属于机密级国家秘密。经查，论文作者陈某曾参与某涉密科研项目，利用该项目的有关素材加工整理后完成了毕业论文。其所在学校未对论文进行保密审查，未经脱密处理便直接把该论文提交到了某学位论文数据库共建平台，造成泄密。**

7.4 国家统一考试中的保密

按照有关规定，高考、研究生入学考试、公务员考试、司法考试等国家统一考试试题、参考答案在考试启用前是国家秘密。评分标准等其他考试相关事项的保密管理按照考试主管部门要求进行。

国家统一考试有关事项，包括试卷的命题、印制、运送、保管等环节的保密管理工作，由组织考试的主管部门负责。命题工作采取全封闭工作形式，命题人员和工作人员应签订保密承诺书。原始试题应在符合安全保密要求的场所、设备和保险柜中存放，并由双人专门保管。试卷应当在具有保密资质的定点印制单位印制，应通过机要渠道运送，或使用可靠的交通工具由双人及以上专门押送。试卷封存保管场所应当安装防盗装置，并有全天候 24 小时的双人守卫。以电子信息形式进行的考试，还应在计算机信息系统、网络和存储介质等方面，采取严格的安全保密防范措施。

作为参与出题的教师应严格按照考试组织部门的保密要求，严格遵守

各项保密规定。参加考试的学生也要遵守保密规定，不得在考前购买泄密试题。对于一些有特殊保密要求的考试，考卷上如果标明其在考后仍属国家秘密的，在考试之后也应履行保密义务，不得以任何方式泄露。

考试试题泄密案件时有发生，保密管理工作尚需进一步加强。例如，某年全国硕士研究生考试前一天，教育部门监控到网上出现英语试卷泄题事件，在删除相关信息的同时由公安部门立案侦查。经查，某市教育考试院招考科科长周某伙同某大学人事处聘用人员段某、附属医院技师欧阳某某、某医学院研究生陈某等人，为谋取经济利益，利用职务之便从保密室窃取了考卷，并复印转卖。案发后，周某等四人被分别判处有期徒刑六年至三年，该案中抓获的贩卖试题的其他被告人被判处有期徒刑两年至九个月不等。该考试院和该市考区其他相关责任人受到相应的党纪政纪处分。

又如，另一年的全国硕士研究生招生考试前，负责印制试卷的某监狱原分监区长曹某，经罗某多次利诱，从该监区窃取试卷。曹某在监区先后拍摄 8 张试卷，并将存储上述照片的内存卡通过自制弹射装置投射至监狱外给罗某。罗某分两次将内存卡交给李某、王某，二人组织答题后将试题及答案提供给了涉案培训机构。案发后，曹某被判处有期徒刑一年六个月，其余 12 名被告也受到了法律的制裁。所有涉案作弊的考生也都受到了应有的处罚。

第 8 讲　宣传报道和对外交流活动中的保密

8.1 接受采访或公开报道中的保密

高校新闻宣传报道坚持“业务谁主管，保密谁负责”的“归口管理”原则，由学校宣传部门负责将保密管理要求融入各种形式的宣传报道活动中，并组织实施。

学校新闻宣传报道中可能涉及国家秘密和工作秘密，必须严格做好保密审查工作。特别是学校网站和自媒体，具有信息发布快速、广泛的特点，更要注重做好保密工作。撰写新闻稿件应当严格遵守新闻出版保密规定和相关保密要求。拟公开宣传与涉密科研活动有关事项的新闻宣传报道或参加国内外展览活动，应采取非密化处理并按照有关程序进行保密审查审批。

因宣传报道未进行保密审查而造成的泄密案件屡有发生。例如，某大学 50 周年校庆时，学校网站刊登了 1 幅秘密级军事飞行器的照片。经查，该大学某飞行器研究所研究人员在做静力试验时，拍摄了包括涉密照片在内的材料，作为该所学科建设成果上报了学校。学校网站负责人宋某根据学校党委宣传部部长于某的要求，安排一名学生从学校资料库中选取一些科研成果照片发布到学校 50 周年校庆网站上，这名学生将上述军事飞行器照片作为学校的科研成果之一发布到网站上，造成泄密。其泄密的主要原因就是宋某和于某未按程序履行保密审查的职责。事发后，有关部门给予宋某警告处分，对于某进行严肃批评。

又如，某大学网站曾被发现刊登一份秘密级文件。经查，该校科研处科长李某擅自摘录涉密文件中部分内容，发布到科研处网站，造成泄密。

有关部门给予李某行政警告处分，取消当年评优资格，并责令作出深刻检查。

8.2 信息公开中的保密

政府信息是指行政机关在履行行政管理职能过程中制作或者获取的，以一定形式记录、保存的信息。政府信息公开，对于保障公民民主权利，提高政府机关工作透明度，开发和利用政府信息的经济和社会价值，具有非常重要的意义。但在处理好信息公开的同时，还要落实保密要求，既要做到政府信息及时、准确的公开，又要防止因公开不当导致泄密事件的发生。因此，在倡导政府信息公开的同时也建立了相应的保密审查机制。

《中华人民共和国政府信息公开条例（2019 年修订）》（以下简称《条例》）规定：“行政机关公开政府信息，应当坚持以公开为常态、不公开为例外，遵循公正、公平、合法、便民的原则。”“除本条例第十四条、第十五条、第十六条规定的政府信息外，政府信息应当公开。行政机关公开政府信息，采取主动公开和依申请公开的方式。”其中，第十四条规定了对国家秘密的保护：“依法确定为国家秘密的政府信息，法律、行政法规禁止公开的政府信息，以及公开后可能危及国家安全、公共安全、经济安全、社会稳定的政府信息，不予公开。”第十五条是对商业秘密和个人隐私的保护：“涉及商业秘密、个人隐私等公开会对第三方合法权益造成损害的政府信息，行政机关不得公开。但是，第三方同意公开或者行政机关认为不公开会对公共利益造成重大影响的，予以公开。”第十六条涉及对工作秘密的保护：“行政机关的内部事务信息，包括人事管理、后勤管理、内部工作流程等方面的信息，可以不予公开。行政机关在履行行政

管理职能过程中形成的讨论记录、过程稿、磋商信函、请示报告等过程性信息以及行政执法案卷信息，可以不予公开。法律、法规、规章规定上述信息应当公开的，从其规定。”

《条例》第十七条专门对政府信息公开的保密审查提出了明确要求：“行政机关应当建立健全政府信息公开审查机制，明确审查的程序和责任。行政机关应当依照《保密法》以及其他法律、法规和国家有关规定对拟公开的政府信息进行审查。行政机关不能确定政府信息是否可以公开的，应当依照法律、法规和国家有关规定报有关主管部门或者保密行政管理部门确定。”

保密审查应以“先审查、后公开”和“一事一审”为原则，对拟公开发布的信息是否涉及国家秘密进行审查，也包括对是否涉及工作秘密、商业秘密和个人隐私等进行甄别。未经审查和批准，不得对外公开发布政府信息。

对保密期限届满的国家秘密，需要公开的仍应进行保密审查，一般情况下并不能直接公开，而是采取依申请审批阅读或依申请公开的方式。已解密但不属于本单位产生的国家秘密，应经原定密单位同意才能公开。

近年来，政府网站违规发布涉密信息的事件呈上升趋势，反映出在政府信息公开时个别单位和人员保密审查不严、工作环节疏漏、甚至违规操作等问题。保密规定要求：单位网站管理部门是网上信息公开的最后一道关口，应建立政府信息发布登记制度，承办单位应向网站管理部门提供保密审查机构的审查意见和单位负责人的审批意见，网站管理部门应做好记录备查。

例如，有关部门在工作中发现，某县政府网站违规发布了一份秘密级文件。经查，其所在省的省直某部门印发了一份秘密级文件，所在市某部门起草了转发通知并把该文件作为附件转发给各县，该县某县直单位办公室文件收发员孙某收到通知后不敢耽搁，立即起草转发通知给所属各乡镇等单位，由于孙某保密意识淡薄，未履行保密审查程序，擅自将通知和该涉密文件发布至县政府网站，造成泄密。事后，孙某被解聘，该直属单位副局长郑某被责令作深刻检查，该单位及相关责任人在全县范围内被通报批评。

8.3 对外交流活动中的保密

高校师生在接待境外人员来访、参加涉外学术交流、开展国际科研合作、对外提供或在外传递相关资料等涉外活动中应当严格按照保密规定的要求进行。不得带领境外人员进入涉密场所和涉密部门、部位，并应阻止其在相关区域照相、摄像和录音；与境外人员交流会谈时不得涉及国家秘密；出入境外驻华机构、组织及其人员驻地，或者陪同境外人员活动时，不得携带涉密载体；不得利用境外通信设施传递涉密信息；不得使用境外人员办公设备处理涉密信息；遇到境外人员索要有关涉密信息的应坚决拒绝，并及时向单位报告。涉密研究生在境内参加有境外机构、组织和人员参与的学术交流等活动，应经导师批准，并进行保密提醒谈话。

对外交流与合作中需要提供国家秘密的，或者任用聘用的境外人员需要知悉国家秘密的，应进行保密审查和进行必要的技术处理，必须经过批准，与对方签订保密协议，并在有关主管部门备案。

例如，某科研单位曾因工作需要，邀请国外某科研单位派技术人员联合开发某项目，双方为此签署了合作协议，其中规定了有关保密条款。起

初，该单位及其项目组人员能认真按照约定的保密条款和相关保密规定开展工作，项目实施和保密管理严格有序。但在一起工作生活数月后，项目组人员与外方人员越来越熟悉，甚至成为了好朋友，彼此之间产生了信任感，导致保密意识淡忘、保密规定执行不严，让外方人员金某有机可乘，知悉并掌握了不应该知道的国家秘密。在金某完成合作项目搭乘回国班机即将起飞前，我安全部门将其扣留，从其所携带的行李中搜查出装有我涉密科研项目资料的U盘。经鉴定，相关资料属于机密级国家秘密。事发后，金某因间谍罪被判刑，该单位有关责任人员分别受到党纪政纪处分。

又如，中国宣纸有“纸中之王”的美称，尤以安徽宣州泾县所产者为最，其核心工艺是秘密。20世纪80年代，某外国企业相关人员以“技术交流”为名，要求参观泾县宣纸制造全过程，遭我方拒绝。但不久，他们在浙江某造纸厂受到了热情款待，该厂是在泾县的扶持下建立并生产宣纸的。该厂厂长毫无保密意识，不仅向对方详细讲解了工艺流程，而且任其拍照、录像，甚至连属于绝密配方的碱水浓度也和盘托出，最后竟然还把檀树皮、长稻草浆、杨藤等原料样品相赠。此后，该外国企业掌握了宣纸的生产诀窍，宣布：世界宣纸，安徽泾县第一，某国第二，浙江第三。

8.4 出境应注意的保密事项

因公出境团组实行“谁派出谁负责，谁组团谁负责”，坚持内外有别、专人负责、全程管理、确保安全的原则。团组出境前应对在境外期间活动的组织管理作出安排，明确保密管理措施。

任何单位和个人不得擅自携带涉密载体出境。确因工作需要须携带国家秘密载体出境的，应当按照国家保密规定办理批准和携带手续，并采取严格的保密管理措施。

对出境人员，学校应在其出行前进行保密教育。特别是对于涉密人员，单位应认真执行对外科技交流保密提醒制度，签订保密承诺书，明确涉密人员的保密义务和责任，落实出境返校后的回访制度。出境人员要严格执行与外方接触的纪律要求，提高警惕，对自己的敏感信息也要注意保护，以防被人利用、误入歧途。特别地，出境使用的手机及电子设备中一定不要留存重要敏感信息，避免泄露。

对于涉密研究生，出入境证件应由培养单位统一保管，对拟出境的，应按有关保密要求履行保密审批手续；经批准出境的，应进行行前保密提醒谈话，签订出境保密承诺书；出境返回后一周内，将出入境证件交由培养单位统一保管，并书面报告出境期间保密规定执行情况。

例如，从事高精尖通信技术研究的周某，获博士学位后赴国外某大学做博士后研究，在申请签证时，表明了自己身份并在签证材料中附有其关于高精尖通信技术领域研究的博士论文复印件，引起了境外情报机构的注意。在国外期间，周某被策反，并在回国后被要求以技术交流的名义继续提供涉密资料。经查，周某先后向境外情报机构提供了大量国防军工重要涉密数据和文件资料，其中机密级、秘密级文件200余份，涉及我国多种重要武器装备的研制状况、作战性能、技术参数等核心秘密。周某因间谍罪被判处无期徒刑。

又如，某海关在出入境检查时发现，某涉密单位高某准备携带出境的公文包内有秘密级文件。经查，高某是单位委派担任境外援助项目考察工作人员，因工作需要携带该文件出境，但没有按照国家有关规定办理许可证及相关手续。事发后，有关部门给予高某行政记过处分。

高校在校学生，尤其是重点大学涉及政治、经济、国防科工、前沿科

技领域学习的学生，已经成为境外间谍组织策反的重点对象。我们必须要有足够的警觉性，千万不要一失足成千古恨。

例如，18 岁的小哲在一所重点大学机械专业读二年级，去台湾某大学交流学习。在台期间的一个同学聚会上认识了一名台湾女子许某，她对小哲非常关心，经常见面一起吃饭、去KTV唱歌、相约旅行。因小哲的专业可以接触到国防科工秘密，许某很感兴趣。小哲的交流学习即将结束回大陆时，许某以恋人的身份向小哲提出要求，让他回去以后及时把他取得的成果发过来和她分享，小哲被恋爱冲昏了头脑，听话地按照许某的要求，每天都把自己的生活、学习情况发给她。小哲就读研究生后，得以参与国家重点实验室的一些项目，许某对他的要求就越来越多，让其搜集各种资料和信息。小哲共向许某提供了涉及我国防军工的近百份情报，收取了 45000 元。他们的活动被国家安全部门发现，许某的真实姓名和身份也被揭露，实际上她是台湾“军情局”的间谍人员。她用尽手段引诱小哲，对小哲实施控制，以便获取情报。而小哲在色诱之下，没能守住底线。小哲因此被追究法律责任，中断了学业。

同样是出境学术交流，某高校博士李某就有较强的保密意识和警惕性。他在参加境外学术会议期间结识了一名自称某国际研究机构研究员的皮特，并通过邮箱保持联系、交流学术问题，皮特多次从境外给李某寄送学术资料和小礼物。经一年交往后，皮特提出可为李某办理绿卡，条件是要求李某提供其参与的涉密科研情况。李某将此情况通过“12339”举报电话向国家安全机关反映。经查，发现皮特是境外情报机构间谍人员。李某在国家安全机关的指导下摆脱了纠缠，有效避免了国家秘密的泄露。李某受到了奖励。

第 9 讲　保守国家秘密的违法违纪责任

9.1 保密法律责任概述

本讲所称的保密法律责任专指保守国家秘密的法律责任。

保密法律责任是责任主体违反保密法律的义务所应当承担的不利后果。保密法律责任的特点主要体现在以下四个方面。

首先，承担保密法律责任的依据是违反保密义务。保密义务即保密法律规范设定的保守国家秘密的义务，《保密法》强调保密法律责任的追究是以行为人违反保密义务为前提的。保密义务是义务主体对国家履行的法定义务，保密义务的核心是防止国家秘密泄露。

其次，保密法律责任的适用对象是保密行政违法行为和危害国家秘密安全的犯罪行为。违反保密行政法律规范，构成保密行政违法行为，是违反保密义务的一般违法行为；违反刑事法律规范，构成危害国家秘密安全的犯罪行为，是严重违反保密义务的行为。

第三，保密法律责任的基本形式是行政责任和刑事责任。保密法律规范既包括属于行政法调整范畴的专门保密法，也包括刑法调整范畴中涉及侵犯国家秘密犯罪的处罚条款。因此，保密法律责任的基本类型包括行政责任和刑事责任。

第四，保密法律责任的具体内容是法律制裁。在行政法律责任中，法律制裁体现为行政处分和行政处罚；在保密刑事责任中，体现的是刑罚。按照刑法规定，刑罚分为主刑和附加刑。主刑包括：管制、拘役、有期徒刑、无期徒刑、死刑。附加刑包括：罚金、剥夺政治权利、没收财产。

判定行为人是否承担保密法律责任的标准，一般考虑责任主体、行为、主观态度、危害后果等方面。在我国保密法律中，承担保密法律责任的主体既包括自然人，如涉密人员、单位工作人员、普通公民等，也包括组织，如国家机关、涉密单位等。承担法律责任要有违反保密法律规范的行为，实质上是违反保密义务的行为，既包括一般的违法行为，也包括犯罪行为。行为人违反保密法律规范行为的主观心理状态包括故意和过失两种，心理状态反映行为人的主观恶性程度，对于具体判断法律责任具有重要意义。行为人的行为对国家安全和利益造成的危害，既包括实际损害，有具体的损害事实发生，例如将国家秘密泄露给境外情报机构，也包括危险隐患，存在对国家安全和利益造成损害的现实可能性，例如违反保密规定将涉密计算机与互联网相连接。

9.2 刑事责任

保密刑事法律责任是指违反保密法律规范，构成犯罪所应承担的法律责任。保密刑事法律责任适用于严重危害国家秘密安全的行为，通过追究刑事责任对犯罪人进行惩罚。

保密刑事责任的规制对象是侵害国家秘密的犯罪行为，主要有以下几方面的特征：

第一，刑事犯罪的主体仅由自然人构成。

第二，侵害国家秘密行为严重危害国家安全和利益，这是危害国家秘密犯罪的本质特征。

第三，行为人以国家秘密为直接犯罪对象，有侵害国家秘密的行为。例如直接对外散布国家秘密信息的行为。危害国家秘密犯罪也可以指向各

种国家秘密载体，如非法持有、遗失国家秘密文件等。在行为方式上包括窃取、刺探、收买行为，也包括非法提供、非法持有等行为。

第四，侵害国家秘密犯罪在犯罪主观方面既包括故意，也包括过失。故意是指行为人明知自己的行为会造成国家秘密失控，给国家安全和利益造成损害，却希望或放任这种结果发生；过失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，却疏忽大意，未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，或者虽然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。

我国《刑法》中危害国家秘密犯罪的主要罪名有：

（1）为境外窃取、刺探、收买、非法提供国家秘密罪

《刑法》第一百一十一条规定：“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。”

例如，某市有关部门曾破获了一起非法向境外组织提供国家秘密的案件。犯罪嫌疑人段某是某涉密单位外包物业公司的日常保洁主管，承担为领导办公室的带班保洁任务。段某主动与境外组织联系并为其提供情报，用境外组织提供的经费购置智能手机，利用打扫卫生和代取文件之机，偷拍涉密文件和资料，通过互联网传递给境外组织。截至案发，段某共向境外提供国家秘密 3 份，获利 13 万元。段某因为境外非法提供国家秘密罪被判处有期徒刑十年，剥夺政治权利两年。涉案单位的 11 名责任人被党纪政纪处分。

（2）非法获取国家秘密罪；非法持有国家绝密、机密文件、

资料、物品罪

《刑法》第二百八十二条规定：“以窃取、刺探、收买方法，非法获取国家秘密的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利；情节严重的，处三年以上七年以下有期徒刑。”“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，处三年以下有期徒刑、拘役或者管制。”

例如，何某、王某等 27 名被告人曾分别组织在安徽省亳州市、云南省昆明市和山东省临沂市、东营市等地的考点进行国家一级建造师考试，并准备使用作弊方法帮助考生通过考试。何某通过其开办的某公司及 QQ 群，策划组织大规模考试作弊活动。何某联系王某，并商定向其购买考试试题。何某又与周某、陈某等人策划出资购买试题和组织“枪手”答题事宜，并通过下级代理“招生”。严某则专门为该团伙研发和改装无线传输、手机 APP 软件、米粒耳机等作弊设备。何某还找人开发了可将文字转化为语音播报的 APP 软件，以收听语音播报的答案。根据每个作弊考场的反作弊严密程度，何某设了不同的收费档次，每门从几千元到几万元不等，其中 VIP 考生要数万元。警方破获了此案，抓获犯罪嫌疑人 27 名，涉案考生达 500 余名。法院审理认为，何某、王某等 27 名被告人组成“一条龙”团伙，以收买的方式非法获取属于绝密级国家秘密的国家一级建造师统一考试试题，并使用作弊的方法帮助考生考试，均已构成非法获取国家秘密罪等罪名。何某因犯非法获取国家秘密罪被判处有期徒刑三年零六个月，其余 26 名被告分别领刑。涉案考生也受到了相应的处理。

（3）故意泄露国家秘密罪、过失泄露国家秘密罪

《刑法》第三百九十八条规定：“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，处三年以下有期徒刑或者拘役；情节特别严重的，处三年以上七年以下有期徒刑。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。”

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，且情节严重的行为。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，且情节严重的行为。

对于故意泄露国家秘密的，《最高人民检察院关于渎职侵权犯罪案件立案标准的规定》中规定，涉嫌下列情形之一的，应予立案：泄露绝密级国家秘密1项（件）以上的；泄露机密级国家秘密2项（件）以上的；泄露秘密级国家秘密3项（件）以上的；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；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；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；以牟取私利为目的泄露国家秘密的；其他情节严重的情形。

对于过失泄露国家秘密的，《最高人民检察院关于渎职侵权犯罪案件立案标准的规定》中规定，涉嫌下列情形之一的，应予立案：泄露绝密级国家秘密1项（件）以上的；泄露机密级国家秘密3项（件）以上的；泄露秘密级国家秘密4项（件）以上的；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；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；其他情节严重的情形。

例如，被告人伍某在中国人民银行金融研究所货币金融史研究室工作期间，违反国家保密法的规定，将其在价格监测分析行外专家咨询会上合法获悉的、尚未对外正式公布的属于秘密级国家秘密的 25 项国家宏观经济数据，多次以手机短信方式故意泄露给魏某等人共 224 次。法庭审理认为：被告人伍某身为国家工作人员，违反保密法的规定，故意泄露国家秘密情节特别严重，已构成故意泄露国家秘密罪。鉴于被告人认罪态度较好，如实供述自己的罪行，可从轻处罚。伍某被判处有期徒刑六年。

（4）非法获取军事秘密罪；为境外窃取、刺探、收买、非法提供军事秘密罪

《刑法》第四百三十一条规定：“以窃取、刺探、收买方法，非法获取军事秘密的，处五年以下有期徒刑；情节严重的，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。为境外的机构、组织、人员窃取、刺探、收买、非法提供军事秘密的，处十年以上有期徒刑、无期徒刑或者死刑。”

（5）故意泄露军事秘密罪、过失泄露军事秘密罪

《刑法》第四百三十二条规定：“违反保守国家秘密法规，故意或者过失泄露军事秘密，情节严重的，处五年以下有期徒刑或者拘役；情节特别严重的，处五年以上十年以下有期徒刑。战时犯前款罪的，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。”

9.3 行政责任

保密行政法律责任是指行政主体或行政相对方由于违反保密法律法规或不履行保密法律义务而依法承担的法律后果。根据《保密法》的规定，保密行政责任包括行政处分和行政处罚两种形式。

行政处分是指国家行政机关或单位依照隶属关系，对违反行政法规的所属工作人员给予的惩罚措施。行政处分具体包括警告、记过、记大过、降级、撤职、开除等种类，由任免机关或者监察机关具体实施。2020 年颁布的《中华人民共和国公职人员政务处分法》第三十九条规定，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，造成不良后果或者影响的，予以警告、记过或者记大过；情节较重的，予以降级或者撤职；情节严重的，予以开除。

行政处罚是指享有行政处罚权的特定行政主体依法对违反行政管理秩序但尚未构成犯罪的行政相对人（即公民、法人或其他组织）给予的行政制裁。**例如，根据《保密法》第五十条规定，出现互联网及其他公共信息网络运营商、服务商不配合司法机关调查等情况，致使涉密信息继续扩散的，公安、国家安全机关和信息产业主管部门可以依法对运营商、服务商给予行政处罚。**

行政法律责任主要有以下几个方面：

（1）严重违规的行政责任

《保密法》第四十八条列举了 12 种最常见、最典型的严重违规行为，这些违规行为会导致保密措施失效，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。包括：非法获取、持有国家秘密载体的；

买卖、转送或者私自销毁国家秘密载体的；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；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；非法复制、记录、存储国家秘密的；在私人交往和通信中涉及国家秘密的；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；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；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；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；擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；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。可见，只要发生上述列举的 12 种严重违规行为之一，不论是否产生泄密实际危害后果，均应按照《公务员法》《行政监察法》《公职人员政务处分法》的有关规定，依法给予处分。对于不依法给予处分的，保密行政管理部门应当提出纠正建议。对于不属于组织人事和监察机关规定的可以给予处分范围的人员，由保密行政管理部门督促其所在机关、单位根据内部管理规定，或者合同约定的条款，给予教育、训诫、经济处罚和解聘等不同形式的处理。

例如，在某市保密局对市直机关及其所属机构开展的一次保密抽查中，重点检查办公网络使用、存储介质管理、网站信息发布等。检查中发现，

该市发改委交通能源处的工作人员使用互联网办公，文件资料传递均通过某互联网公共电子邮箱收发。据了解，该市发改委交通能源处与辖区各区县相关部门需要传递大量业务资料和少量文件，因办公专网正在建设过程中，经处务会集体研究，决定给处内所有工作人员统一申领了连续编号的互联网公共电子邮箱，并在专网验收合格前用其传递各类文件资料，违反了不得用普通邮箱传递涉密文件和内部资料的保密规定。事后，该市发改委给予该处处长邱某行政降级处分并调离该处，副处长马某行政记大过处分，对使用互联网电子邮箱办公的其他 3 名工作人员进行通报批评，分管该处的发改委副主任袁某因负有领导责任受到行政警告、党内警告处分。

（2）机关、单位违反保密规定的行政责任

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。

机关、单位发生泄露国家秘密案件，应当立即采取补救措施并在规定的时间、按照规定程序和规定内容进行报告。不按照规定报告或者未采取补救措施的，对直接负责的主管人员和其他直接责任人员依法给予处分。发现国家秘密已经泄露或者可能泄露时，立即采取补救措施并及时报告，也是国家工作人员和其他公民的法定义务。

在保密检查或者泄露国家秘密案件查处中，有关机关、单位及其工作人员拒不配合，弄虚作假，隐匿、销毁证据，或者以其他方式逃避、妨碍

保密检查或者泄露国家秘密案件查处的，对直接负责的主管人员和其他直接责任人员依法给予处分。企业事业单位及其工作人员协助机关、单位逃避、妨碍保密检查或者泄露国家秘密案件查处的，由有关主管部门依法予以处罚。

涉密信息系统未按照规定进行检测评估和审查而投入使用的，由保密行政管理部门责令改正，并建议有关机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分。

（3）互联网运营商、服务商违反保密规定的行政责任

互联网及其他公共信息网络运营商、服务商违反《保密法》第二十八条规定的，由公安机关或者国家安全机关、信息产业主管部门按照各自职责分工依法予以处罚。

实践中，违反《保密法》第二十八条规定的行为主要包括：互联网及其他公共信息网络运营商、服务商没有履行配合公安机关、国家安全机关、检察机关对泄密案件进行调查的义务；发现利用互联网及其他公共信息网络发布的信息涉及国家秘密，没有立即停止传输和保存客户发布信息的内容及有关情况记录，并及时向公安机关、国家安全机关或者保密行政管理部门报告；没有按照公安机关、国家安全机关或者保密行政管理部门要求，及时对互联网或公共信息网上发布的涉密信息予以删除，致使涉密信息继续扩散。

（4）违反保密资质（资格）规定的行政责任

《保密法》第三十四条规定：“从事国家秘密载体制作、复制、维修、销毁，涉密信息系统集成，或者武器装备科研生产等涉及国家秘密业务的

企业事业单位，应当经过保密审查，具体办法由国务院规定。”

目前，保密资质（资格）涉及三项行政许可，分别是国家秘密载体印制资质、涉密信息系统集成资质和武器装备科研生产保密资格。保密审查不合格的，不得从事涉密业务。

经保密审查合格并获得保密资质（资格）的企业事业单位违反保密管理规定的，由保密行政管理部门责令限期整改，逾期不改或者整改后仍不符合要求的，暂停涉密业务；情节严重的，停止涉密业务。

未经保密审查的单位从事涉密业务的，由保密行政管理部门责令停止违法行为；有违法所得的，由工商行政管理部门没收违法所得。

机关、单位委托未经保密审查的单位从事涉密业务的，由有关机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分。

9.4 党纪处分

党章党规关于党的纪律的规定，给所有党员划定了一条红线，这条红线比法律的要求更高。根据党章要求，党员要模范遵守国家的法律法规，要模范遵守党的纪律。

在遵守党的保密纪律方面,2018 年修订的《中国共产党纪律处分条例》第四章明确了对违法犯罪党员的纪律处分，第十章明确了对违反工作纪律行为的处分，其中涉及保守国家秘密的有以下几个方面。

（1）泄露、扩散或者打探、窃取党组织关于干部选拔任用、纪律审查、巡视巡察等尚未公开事项或者其他应当保密的内容的，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。

私自留存涉及党组织关于干部选拔任用、纪律审查、巡视巡察等方面资料，情节较重的，给予警告或者严重警告处分；情节严重的，给予撤销党内职务处分。

（2）在考试、录取工作中，有泄露试题、考场舞弊、涂改考卷、违规录取等违反有关规定行为的，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。

（3）党组织在纪律审查中发现党员有滥用职权、玩忽职守等违反法律涉嫌犯罪行为的，应当给予撤销党内职务、留党察看或者开除党籍处分。

（4）党组织在纪律审查中发现党员有刑法规定的行为，虽不构成犯罪但须追究党纪责任的，或者有其他违法行为，损害党、国家和人民利益的，应当视具体情节给予警告直至开除党籍处分。

需要注意的是，根据《保密法》第九条规定，政党的秘密事项中符合法定条件的，属于国家秘密。故意或过失泄露国家秘密，可能构成犯罪的，要依法追究刑事责任。

第 10 讲　商业秘密与个人隐私保护

10.1 商业秘密的概念

《中华人民共和国反不正当竞争法（2019 年修订）》（以下简称《反不正当竞争法》）规定，商业秘密是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

商业秘密是国际上通用的法律术语，有的国家将其称为工商秘密，世界贸易组织的国际公约《与贸易有关的知识产权协定》将其归做未披露信息。构成商业秘密，必须具备如下条件：秘密性，这是商业秘密的首要特征，即并非被通常从事有关工作领域的人们所普遍了解或容易获得；保密性，商业秘密权利人在主观上必须具有保密意识，在客观上实施了合理的保密措施，**例如，告知雇员存在商业秘密、与相关人员签订保密合同、限制可以接触到商业秘密的人员数量等**；价值性，即商业秘密能给权利人带来竞争上的优势及现实的或潜在的经济利益。

商业秘密与专利的最大区别在于商业秘密是不公开的，且并不强调技术含量或创造性；而专利技术是公开的，并且符合法律对创造性的要求。在权利的取得上，商业秘密权的取得无需国家授权，只要其符合法律的规定，便可自动受到法律的保护；而专利权需要经过权利人申请、专利局审查和授权等一系列程序。此外，商业秘密权不受时间和地域的限制，而专利权的存在具有时限性，且通常只在被授权的国家或地区有效。

商业秘密包括技术信息、经营信息和其他商业信息等三类。技术信息，

是指与产品生产和制造有关的技术诀窍、生产方案、工艺流程、设计图纸、化学配方、技术情报等未公开的信息。经营信息，是指与生产经营销售活动有关的经营方法、管理方法、产销策略、货源情报、客户名单、标底及标书内容等未公开的信息。其他商业信息，是指技术信息和经营信息以外，与经营者经营活动有关的未公开的各种消息、数据、情报和资料等。

企业商业秘密泄密事件在全球范围内接二连三地发生，不少事件使企业遭受重大损失，甚至严重影响了企业的生存和发展。

例如，某大型企业发现其投入大笔资金设计的A产品被某国外竞争对手领先一步完成设计并发布。但该企业在项目立项及开发过程中，从未听说有哪家企业也在进行A产品的开发，为什么竞争对手开发速度如此之快？该产品的设计开发是该企业保密的重大研发项目，企业老总随即下令该项目暂停开发，并向公安部门报案。公安部门技术人员到达现场后，发现其研发中心保密工作存在重大疏漏：设计开发电脑与普通工作电脑连在同一个局域网上且都可以上互联网、一些技术秘密文件被设成共享、资料允许随意拷出和带出……几乎没有采取任何保密措施！公安部门初步判定为内部人员泄密，但是要查出具体是谁，几无可能。最终该案不了了之，企业也只能对研发中心负责人进行降职处罚，付出的1000余万元研发费用和众多研发人员的辛勤劳动付诸东流。

又如，某国际化妆品巨头L集团曾有意并购另一护发品牌公司O公司，但最终流产。O公司指控L集团在并购尽职调查过程中窃取了其某款畅销产品的秘密配方并推出类似产品抢占市场。O公司胜诉，L集团上诉。随后，法庭再次裁定L集团败诉，陪审团认为，L集团的行为构成两项专利侵权、盗取商业机密以及违反保密条款。L集团或将赔偿O公司超过1.12亿美元。

再如，A公司诉硅谷注册的X公司盗窃其商业秘密一案，法院作出了A公司胜诉的判决。X公司需支付8.45亿美元赔偿，并遵守临时禁制令。禁制令禁止X公司对包含A公司知识产权的软件产品进行开发活动，也禁止X公司在与A公司相同的业务领域经营。A公司指控X公司诱使A公司当地子公司的几名雇员为其工作，窃取A公司的源代码、软件、公司定价策略和供内部使用的设备手册等商业秘密，并帮助X公司与A公司的一个最大客户获得有利可图的合同；指控X公司利用窃取的商业秘密快速启动计算光刻业务，使其发展速度远远超出可能的范围。由于X公司已处于破产状态，A公司虽无法获得全部赔偿金，但将通过破产程序能获得X公司的大部分知识产权和资产，并可获得X公司的实际或潜在客户。A公司之所以胜诉，关键在于能提供大量证据证明其为保护商业秘密采取了众多严格的安全保密措施。

为了加强国有企业的商业秘密保护，2010年，国务院国有资产监督管理委员会发布了《中央企业商业秘密保护暂行规定》，对央企的商业秘密管理问题进行了全面的规定。该规定分为总则、机构与职责、商业秘密的确定、保护措施、奖励与惩处以及附则六个部分。中央企业商业秘密，根据泄露会使企业的经济利益遭受损害的程度，分为核心商业秘密、普通商业秘密两级，密级标注规定为“核心商密”“普通商密”。

10.2 侵犯商业秘密的行为及其处罚

侵犯商业秘密是指行为人未经商业秘密权利人的许可，以非法手段获取商业秘密并加以利用的行为。主要分为四类：

（1）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密。

（2）非法披露或者公开他人的商业秘密的行为。包括负有保密义务的人违反约定或要求而非法披露或者公开商业秘密；第三人明知或应知他人是以非法手段获得的商业秘密而将其披露或公开等情形。

（3）非法使用商业秘密的行为。包括使用或者允许他人使用不正当获得的他人商业秘密；违反约定或要求使用，或者允许他人使用其所掌握的商业秘密；第三人明知或应知他人是以非法手段获得的商业秘密而使用的行为等情形。

（4）教唆、引诱和帮助他人侵犯商业秘密的行为。

此外，第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人以不正当手段获取了商业秘密，仍使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

侵犯商业秘密应当承担相应的民事、行政和刑事法律责任。

根据《反不正当竞争法》第十七条的规定，侵犯他人商业秘密的，应当依法承担民事责任，停止侵害和赔偿损失。赔偿数额，按照实际损失或侵权人所获利益确定，情节严重的按一倍以上五倍以下赔偿。难以确定的，根据侵权行为的情节确定五百万元以下的赔偿。

根据《反不正当竞争法》第二十一条的规定，经营者以及其他自然人、法人和非法人组织侵犯商业秘密的，应当依法承担行政责任。由监督检查部门责令其停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处五十万元以上五百万元以下的罚款。

根据《刑法》第二百一十九条的规定，行为人侵犯商业秘密、给商业秘密权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单

处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金。

例如，某公司（以下简称甲公司）外贸部主管许某曾违反公司保密要求，将含有四个核心程序源代码的技术信息提供给他人，并伙同采购员徐某等人使用上述核心程序源代码制作电表，通过其控制的某科贸公司向境外合营公司出口销售相关电表，非法获利。经查，根据立项、研发等材料、非公知性鉴定、劳动合同、保密协议及相关证人证言等，证实涉及的四个核心程序源代码是甲公司的商业秘密，且采取了严格的保密措施。法院判决：许某和徐某犯侵犯商业秘密罪，均被判处有期徒刑四年，并分别处以罚金300万元和200万元。

10.3 个人隐私保护

隐私权作为一种人身权利，在现代社会越来越被重视。而随着信息和网络技术的发展，隐私权更加容易受到侵犯。2020年5月28日颁布的《中华人民共和国民法典》（以下简称《民法典》）进一步完善了我国关于隐私权保护的立法设计，隐私权作为一种具体人格权被确定，享有不受侵害的权利。

《民法典》第一百一十条规定："自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。"第一千零三十二条规定："自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。"该条明确定义了隐私的两部分主要内容：自然人对于自己的正常生活所享有的不受他人非法打扰、妨碍的权利；不愿为他人知晓的私密空间、私密活动、私密信息。其中，私密信息的认定，需要考虑两个重要因素：一是该信息

对于维护自然人的人身财产权益、人格尊严和人格自由的重要程度，越重要的，越可能属于私密信息；二是该信息对于维护社会正常交往、信息自由的重要程度如何，越重要的，越不属于私密信息。

《民法典》第一千零三十三条列举了侵害隐私权的主要方式，包括：

（1）以电话、短信、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁。例如，经常在深夜给他人打骚扰电话，就是典型的对私人生活安宁的侵犯。

（2）进入、拍摄、窥视他人的住宅、宾馆房间等私密空间。例如，在他人住宅、宾馆房间的隐蔽地方安装摄像头，偷窥他人在房间里的活动，即属于此种类型。

（3）拍摄、窥视、窃听、公开他人的私密活动。例如，“盯梢”就属于此类行为。

（4）拍摄、窥视他人身体的私密部位。例如，在浴室里安装摄像头，偷窥他人私密部位即属于此种类型。

（5）违规处理他人的私密信息。例如，未经许可，公开他人患有艾滋病的行为即属于此种类型。

（6）以其他方式侵害他人的隐私权。

对于上述行为，在法律另有规定和权利人明确同意的情况下，不构成侵权。

例如，王某以侵犯隐私权、名誉权为由将张某及其创始的某网站、以及另外两家网络公司起诉至法院，该案被媒体冠为“人肉搜索第一案”“网络暴力第一案”。事情的缘由是：女士姜某自杀身亡，生前在网

络上写下了自己近两个月的心路历程，将丈夫王某的不忠诉诸于博客并贴出了丈夫和第三者的照片。王某成为众矢之的，网友运用“人肉搜索”将王某及其家人的个人信息，包括姓名、照片、住址以及身份证信息和工作单位等全部披露。王某在网上被“通缉”“追杀”、围攻、谩骂、威胁，不断收到恐吓邮件。张某和另两家公司等三家网站在其中起到了主要的传播作用。法院一审判决，认定其中两家网站及其管理者构成对原告王某名誉及隐私权的侵犯，被判停止侵权、公开道歉，并分别赔偿王某精神抚慰金 3000 元和 5000 元；另一网站在王某起诉前及时删除了侵权帖子，因此判决认定不构成侵权。一审宣判后，张某不服判决提起上诉。法院进行了终审宣判：王某在与姜某婚姻关系存续期间与他人有不正当男女关系，是造成姜某自杀的因素之一，王某的行为应当受到批评和谴责。但批评和谴责应在法律允许范围内进行，不应披露、宣扬其隐私。张某作为网站的管理者泄露王某个人隐私已构成对王某的侵害，应当承担相应民事责任，法院故此维持原判。

又如，某医院 5 名工作人员利用职务便利，私自用手机偷拍并通过微信转发传播该院新冠肺炎感染者的病历信息，其中包括患者姓名、详细住址、工作单位、诊疗信息等情况，造成恶劣影响。他们的行为已侵犯了他人隐私，被公安部门依法给予行政处罚，其中 4 人受到了行政拘留十日、罚款五百元的处罚，另 1 人被罚款五百元。

10.4 个人信息保护

除了个人隐私，现代社会的个人信息保护也受到了高度重视。世界上有 120 多个国家和地区有专门的个人信息保护的立法。在《民法典》颁布之前，我国在相关法律法规中规定了个人信息保护的内容，《民法典》则系统确立了个人信息保护制度，明确规定了个人信息权益，对个人信息的

合理使用和处理进行了规定。2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过并发布了《中华人民共和国个人信息保护法》(简称《个人信息保护法》)。

相比个人隐私，个人信息的范围非常广泛，除了能识别自然人身份的信息外，其他诸如健康信息、行踪信息等均属于个人信息的范畴。《民法典》第一千零三十四条中规定：“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。”该条界定了个人信息的内涵与外延，即只要能够直接或间接地识别特定自然人的信息都属于个人信息。

《民法典》第一百一十一条与第一千零三十四条中都明文规定：“自然人的个人信息受法律保护。”《民法典》没有规定个人信息权，而是使用了“个人信息保护”的表述，以协调自然人的个人信息保护与信息的自由流动和利用之间的关系。《民法典》第一千零三十四条中还规定：“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。”

《民法典》用“处理”来表述与个人信息相关的各种行为，包括个人信息的收集、存储、使用、加工、传输、提供、公开等。实践中，除了上述七种行为外，还可能包括其他的类型，如个人信息的删除、销毁等。《民法典》第一千零三十五条规定，处理个人信息的基本原则是合法、正当、必要，不得过度处理，并符合如下条件：①征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外。②公开处理信息的规则。③明

示处理信息的目的、方式和范围。④不违反法律、行政法规的规定和双方的约定。

《民法典》第一千零三十六条规定，处理个人信息，有下列情形之一的，行为人不承担民事责任：①在该自然人或者其监护人同意的范围内合理实施的行为。②合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外。③为维护公共利益或者该自然人合法权益，合理实施的其他行为，**例如，在发生大规模自然灾害或者疫情的时候，为了防灾减灾或者控制疫情的需要，对个人信息进行收集、使用等处理行为；为了寻找失踪的自然人，而以适当的方式对该人的姓名、肖像、行踪等加以公布。**

《民法典》第一千零三十七条还规定了个人信息决定权：“自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。”“自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。”

随着信息技术和互联网技术的发展及广泛应用，个人信息安全受到了极大的威胁。信息处理者保障其处理的自然人个人信息安全，是信息处理者最基本也是最重要的任务。《民法典》第一千零三十八条规定：“信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。”“信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发

生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。”

《民法典》第一千零三十九条还特别规定了国家机关及其工作人员对个人信息的保密义务：“国家机关、承担行政职能的法定机构及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供。”这里的“法定机构”是指根据特定的法律、法规或者规章设立，依法承担公共事务管理职能或者公共服务职能，不列入行政机构序列，具有独立法人地位的公共机构，例如高等学校、医院等。

2021 年 11 月 1 日起施行的《个人信息保护法》共八章，包括：总则、个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任、附则，共七十四条，细化、完善了个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利和义务，为最大程度地保护个人信息划定了底线。

近年来，泄露个人信息的事件时有发生，对个人信息造成严重威胁，层出不穷的电信和网络诈骗往往都是因为个人信息被泄露引发的。例如，媒体曾披露在网上发现“裸奔”的用户敏感数据，涉及一家 AI 公司存储处理的大规模人脸识别数据，超过 250 万用户的 680 多万条信息记录被泄露，包括姓名、身份证号码、身份证签发日期、性别、国籍、家庭住址、出生日期、照片、工作单位以及监控器 GPS 位置等。相关公司和单位对网络安全和个人信息保护不重视，没有采取必要的安全保密措施，给恶意窃取信息者大开方便之门，对个人信息和社会安全造成巨大隐患。

又如,某县公安局交警大队秩序科原辅警刘某甲违法在公安网上查询公民车辆档案信息,并以每条人民币 20 至 30 元不等的价格出售给刘某乙、刘某丙。刘某甲还介绍原单位辅警鲁某、唐某查询并出售公民车辆档案信息给刘某乙、刘某丙，刘某甲从中抽取每条人民币 10 元的好处费。刘某甲共计违法所得人民币 18.7 万余元。案发后，刘某甲因侵犯公民个人信息罪被判处有期徒刑三年零六个月，并处罚金人民币 19 万元。其他涉案人员另案处理，均受到相应的处罚。

参考文献

[1]《中华人民共和国宪法（2018 年修订)》.

[2]《中华人民共和国保守国家秘密法（2010 年修订)》.

[3]《中华人民共和国保守国家秘密法实施条例（2014 年)》.

[4]《中华人民共和国政府信息公开条例（2019 年修订)》.

[5]《中华人民共和国刑法（2017 年修订)》.

[6]《中华人民共和国反间谍法（2014 年)》.

[7]《中华人民共和国公务员法（2018 年修订)》.

[8]《中国共产党纪律处分条例（2018 年修订)》.

[9]《中华人民共和国反不正当竞争法（2019 年修订)》.

[10]《中华人民共和国民法典（2020 年)》.

[11]《中华人民共和国个人信息保护法（2021 年)》.

[12]《科学技术保密规定（2015 年)》(科学技术部、国家保密局令第 16 号）.

[13]《涉密研究生与涉密学位论文管理办法（2016 年)》(国务院学位委员会、教育部、国家保密局通知（学位[2016]27 号)).

[14] 国家保密局编写组:《中华人民共和国保守国家秘密法释义》，金城

出版社，2010 年 5 月.

[15] 王吉胜，杨世保:《保密工作实用速查手册》，金城出版社，2018 年 5 月.

[16] 教育部保密委员会办公室编:《高等学校保密知识手册》，金城出版社，2010 年 1 月.

[17] 本书编写组:《红色往事：镌刻在党旗上的保密故事》，金城出版社，2016 年 3 月.

[18] 本书编写组:《举案说法警钟长鸣：近年来典型失泄密案例警示录》，金城出版社，2019 年 4 月.

[19] 吴同斌、解玮玮编:《科技人员保密必读》，金城出版社，2020 年 5 月.

[20] 胡岩、朱鹏涛、崔艳华主编,《大学生保密教育》，华南理工大学出版社，2020 年 3 月.

[21]《保密工作》期刊，金城出版社，历期.

[22] 金城出版社微信公众号“保密观”，微信号：baomiguancha

[23] 中国保密协会网站“案例警示”栏目，http://zgbmxh.cn