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。

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。”

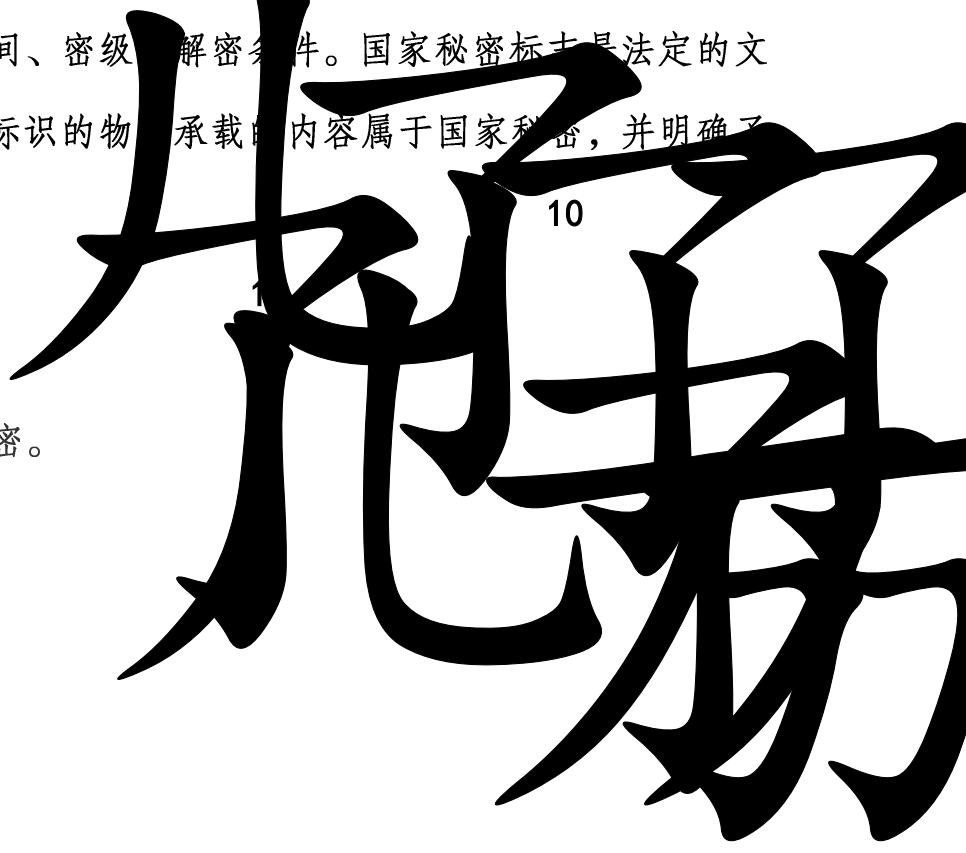
依据该规定,国家秘密必须具备三个要素,缺一不可。

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质承载的内容属于国家秘密，并明确了其密级和保密期限。



我们身边就有国家秘密。

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，[redacted]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[redacted]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。 2018

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，或者可以采取有效措施控制知悉范围的，或者丧失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。本质上国家秘密与国家利益一致，保密国家秘密是一种

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，如果国防秘密被窃取、出卖，造成的损失往往无法挽回。

86　3288　1　16

26　38

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。

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。

在社会活动和治理中也有很少必须保密的情况，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。 2011 10 5 13 6 5000

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[illegible]策反和情报窃密活动猖獗。

2020 4 15

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[redacted]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、泄密手段更加隐蔽。我国面临的计算机网络窃密风险一直居高不下。据统计，[redacted]以上的泄密案件涉及计算机和网络。

2018 12

VPN

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、[redacted]物资源等领[redacted]

[redacted]

2018 10

2019 5

2019 7

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，保护其知悉、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。任何危害国家秘密的行为都将受到严肃的处罚。

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。

12339

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。

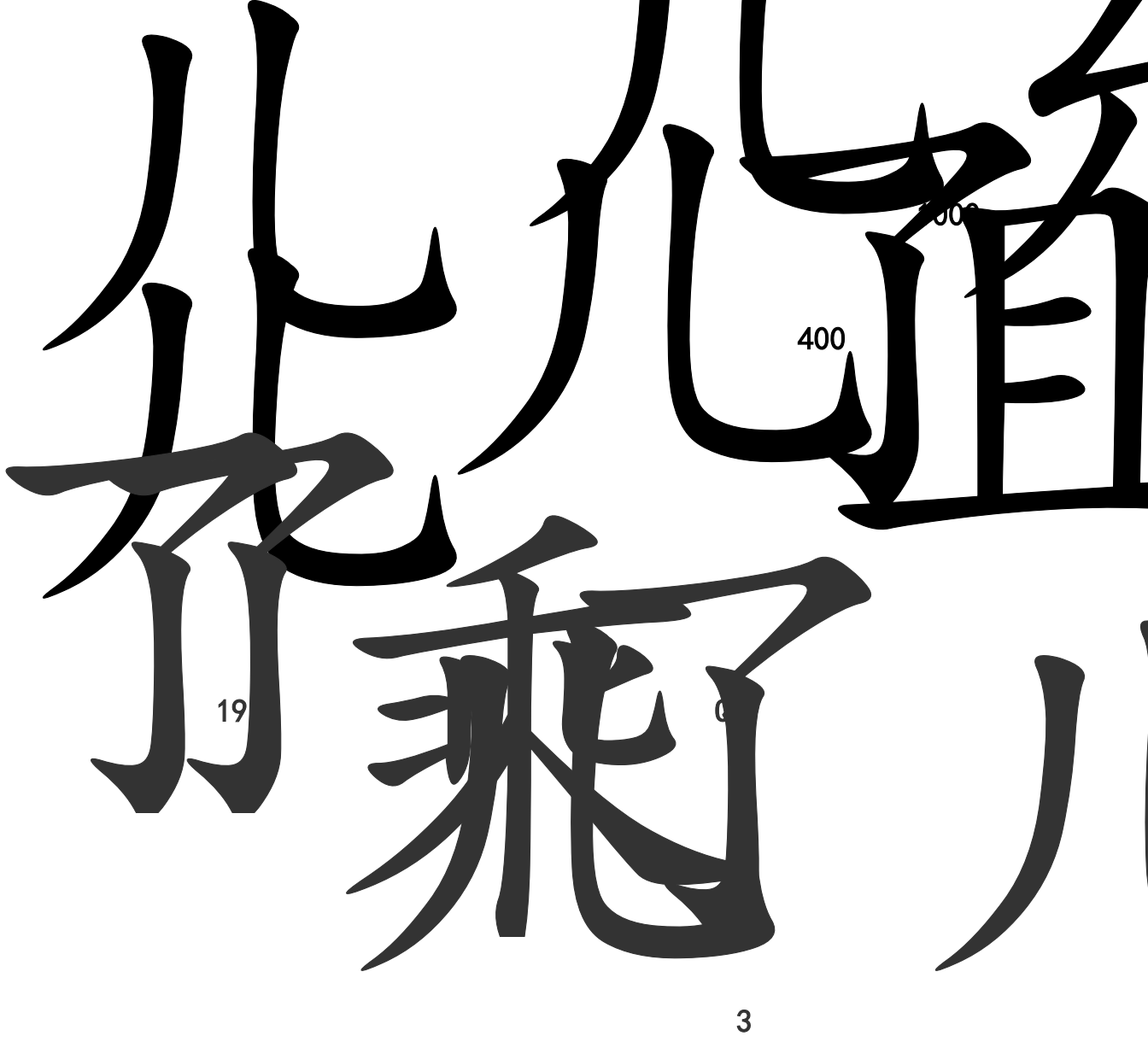
0 15

0 1674

U

5500 146 1753

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、拉拢我社会人员甚至在校学生窃取出卖国家秘密的例子绝非个例。



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。”

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

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

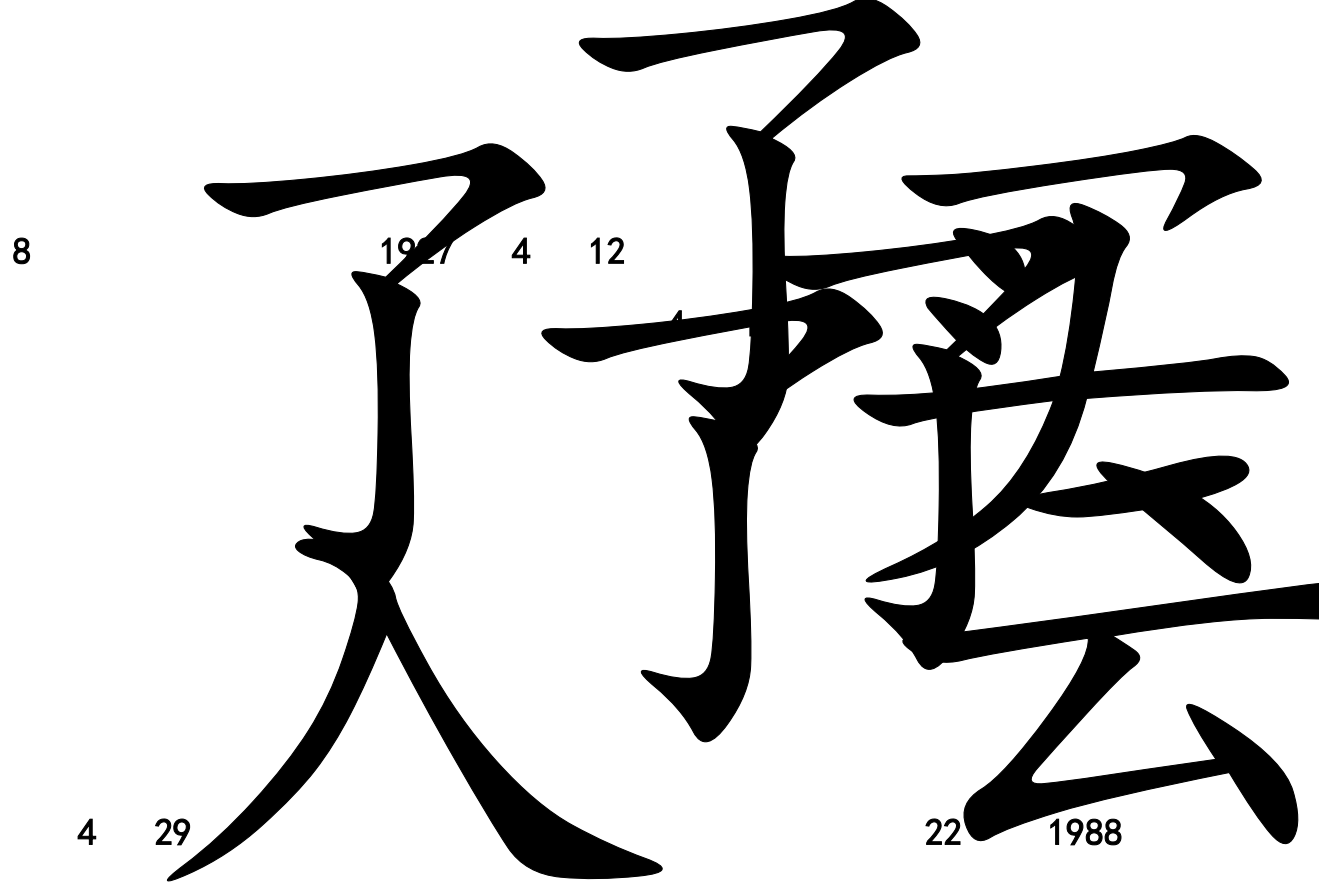
习近平总书记强调：“历史是最好的教科书。学习党史、国史，是坚持和发展中国特色社会主义、把党和国家各项事业继续推向前进的必修课。”党的保密工作历史，是党史的重要组成部分。高校师生了解党的保密工作历史，继承和发扬党的保密工作优良传统，对进一步做好新时代保密工作，维护国家安全和利益，具有非常重要的意义。

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。

1905-1927 1924



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，其建党的早期遭遇、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，国民党右派分子在共产党党权最重的时候，我们党几乎高于敌人一招先发

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。

1 27 8 7

（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，

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。

1927 4 12

20

（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[illegible]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[illegible]证明并且还将证明，人民群众永远是我们党的保密屏障，是[illegible]工作的基础。

1942　8

（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[illegible]期，党中央[illegible]党我军依靠保密技术与反动势力对抗，取得了骄人战绩。

1947 7

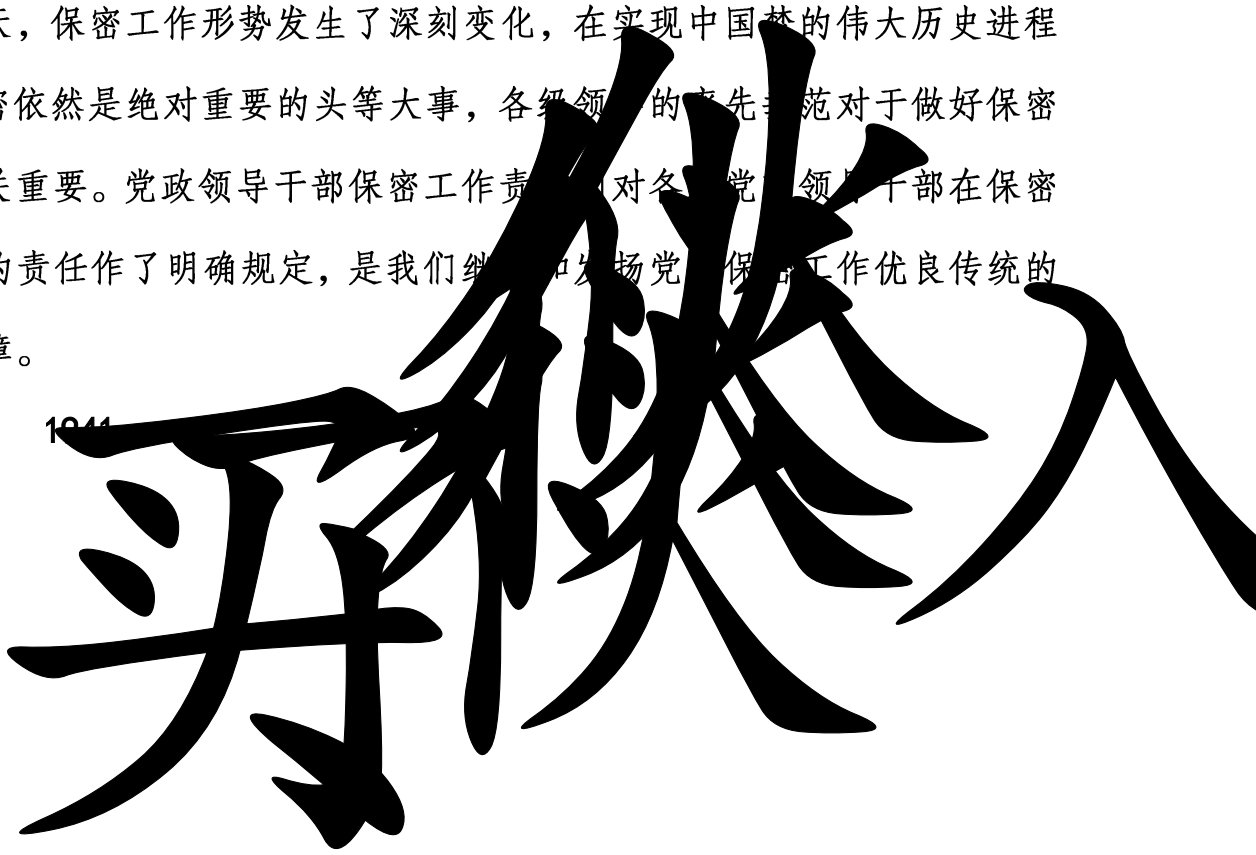
4 15

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。



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党章里，并熔入了入党誓言中。

土地革命时期虽然没有统一的党誓词，但各地党组织都规定在入党时要宣誓，使用的誓词也有所

抗日战争时期，中组部起草发布的标准的入党誓词：

解放战争时期，各地党组织都继续采用原有的入党誓词，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统一印发的入党志愿书内的入党誓词为：

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：

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：

为了

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的、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，也构成保密法律体系的重要内容。

（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发布的条例、办法和细则中有关保密条款的规定，

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

1992

2014

2015

2017

（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

（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公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

[redacted]

订保密协议，提出保密要求，采取保密措施。

（11[redacted]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[redacted]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技能造成的泄密事件屡有发生。

（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，也为了保护自己和他人，千万不要因为对法律无知而走上犯罪的道路。

（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。”

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

[redacted]

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、单位或者上级机关的批准。

一些工作人员保密纪律松散，对涉密载体失控不查，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。

（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[redacted]

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公务无关的其他事情。

3

（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[illegible]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，不能借阅；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[illegible]凡[illegible]准记录、录音、录像的，传达者应当事先声明。

1 3

（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。

（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。

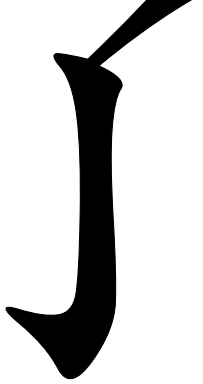
（6）涉密载体维修。涉密载体维修应由本单位专门技术人员负责；确需外单位人员维修的，要在本单位内部进行，并指定专人全程现场监督，严禁维修人员读取或复制涉密信息；确需送外维修的，应送保密行政管理部门审查批准有维修资质的定点单位进行，并在送修前拆除信息存储部件。

（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。

938 96 339

301

95 13 193 637



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[redacted]

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[redacted]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[redacted]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。

1019

1

违规使用非涉密计算机、非涉密存储设备以及公[redacted]储[redacted]

理、传递国家秘密信息的泄密事件频发。

QQ

QQ

QQ

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[illegible]，很容[illegible]级技术马等恶意软件，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[illegible]高[illegible]修、严[illegible]遵守使用手机的相关保密规定，包[illegible]社交媒体软[illegible]使用的安[illegible]保密要求。

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有的，往往难以清除，泄密风险极高。

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。

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。APP / 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。

“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。U USB Key

“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：APP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。12306

13

a123456

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。

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。

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

168

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，并可以进行各种非法的任何事情。

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[illegible]。[illegible]“震网”这样的网络武器级恶意代码甚至能突破物理隔离[illegible]屏障[illegible]2011

1/5

U

[illegible]通过恶意代码实施有组织的窃密攻击时有发生[illegible]

，

，

，

，

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 号和密 是钓鱼网站的常见手段。 ：

http://ww cbc.c cn cn

钓 和挂 网站也是实施有组织网络窃密攻 的

，

，

，

，

，

， 10 ，

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、结题报告、调研报告、[illegible]论证书、立项报告、分包合同书、[illegible]测试报告、关[illegible]技术报告、研究报告、验收鉴定[illegible]请书、[illegible]术总结报告、用户[illegible]报告、测试报告、成果[illegible]报表等，都应纳入涉密载体管理范围。

高校科研工作中泄[illegible]事件时有发生。

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[illegible]

因发表论文不慎而造成泄密的案件[illegible]过多起。

4

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表的过程中，违规涉密的案例也有多起。

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。

8

12

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。

50　　1

50

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。

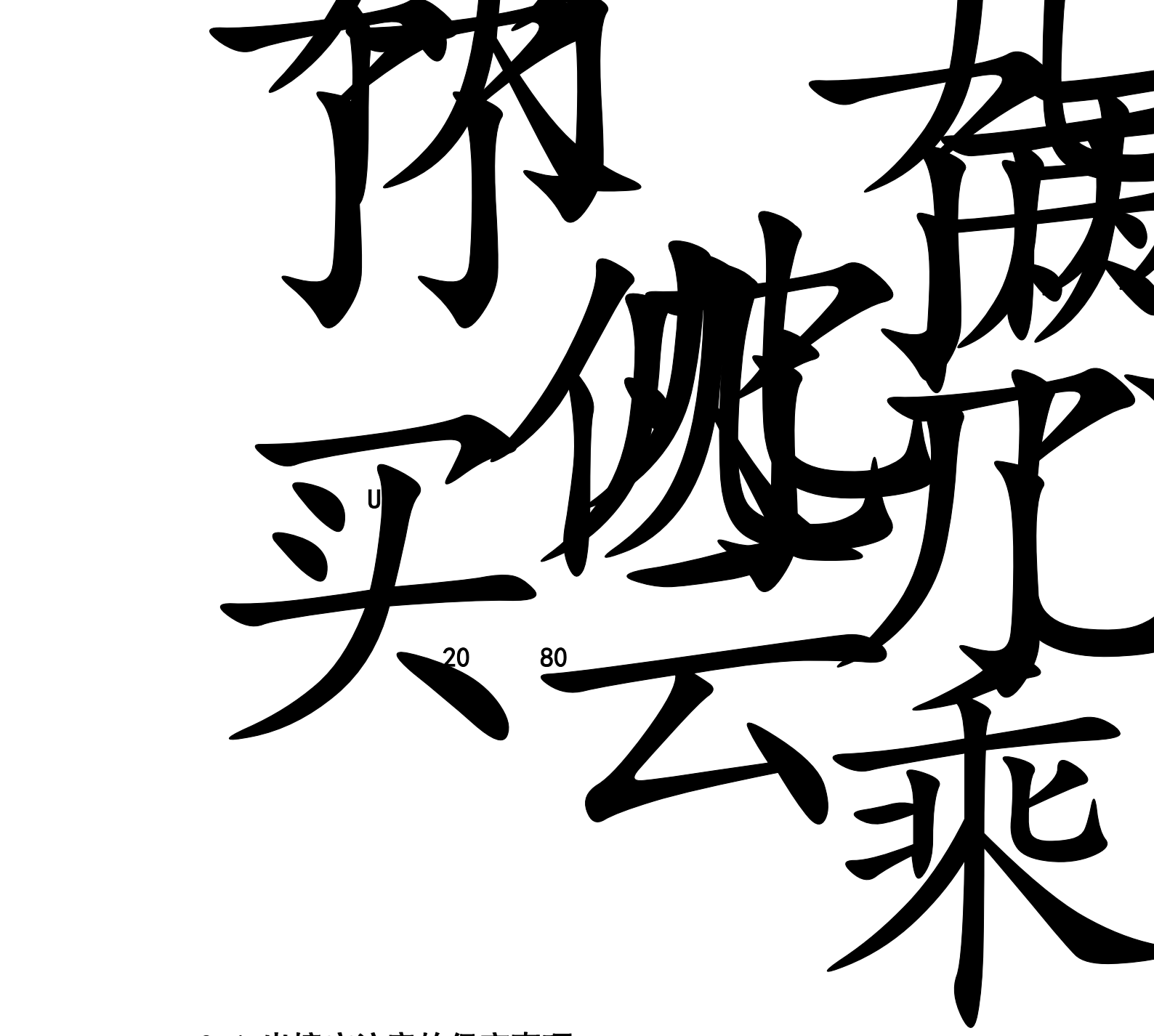
对保密期限届满的国家秘密，需要公开的仍应进行保密审查，一般情况下并不能直接公开，而是采取依申请审批阅读或依申请公开的方式。已解密但不属于本单位产生的国家秘密，应经原定密单位同意才能公开。

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。

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，[redacted]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。

[redacted]要知悉国家秘密的，应进行保密审查和[redacted]必要的技术处理，必须[redacted]过批准，与对方签订保密协议，并在有关[redacted]管部门备案。



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，应进行出境前保密提醒谈话，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。

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。我们必须有足够的警觉性，[illegible]古恨。

18

KTV

45000

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。

[redacted]

（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，处五年以上十年以下[redacted]

[redacted]

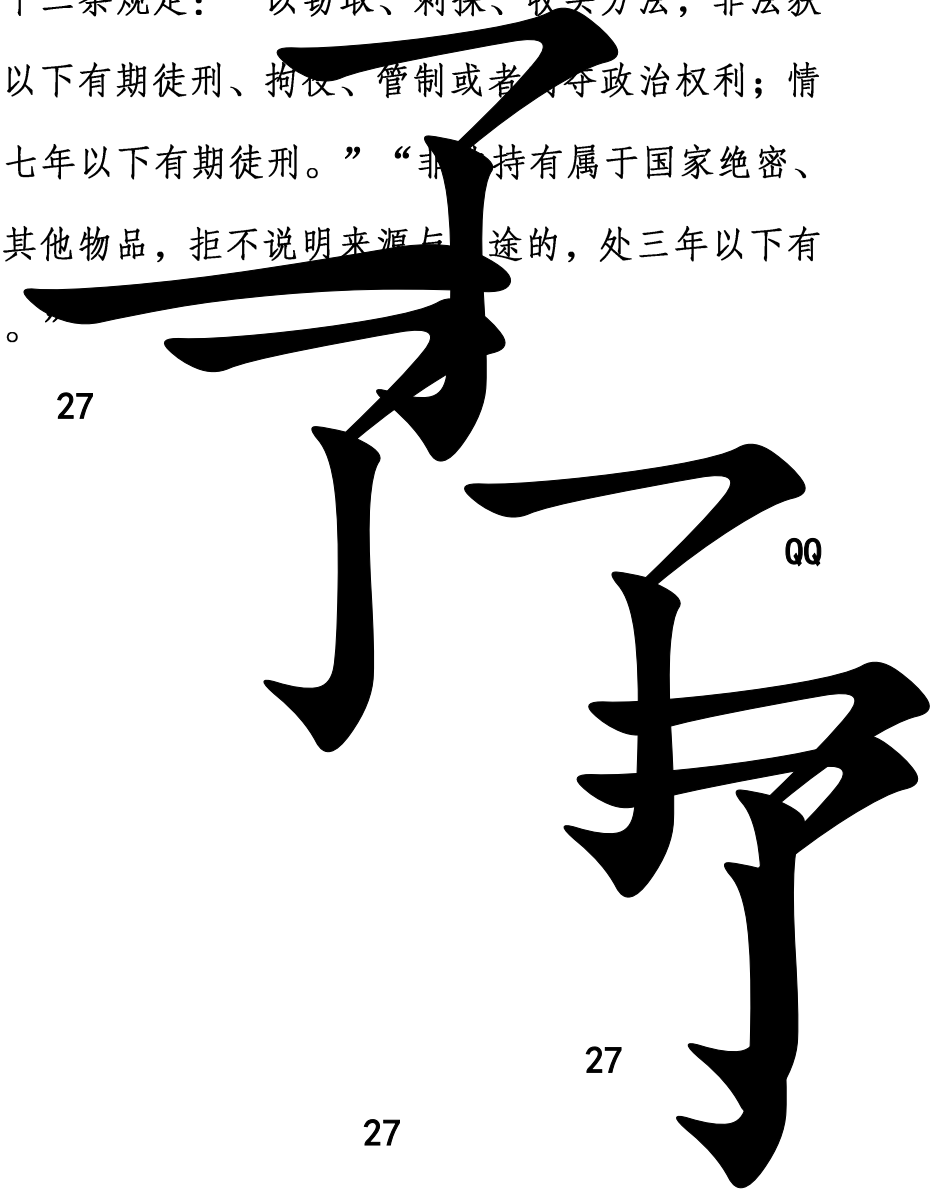
3 13

11

（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。”



27

QQ

APP

APP

VIP 27

500 27

26

（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[redacted]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[redacted]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[redacted]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[redacted]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

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。[redacted]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[redacted]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[redacted]

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）实施的行政制裁。

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。

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。

（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

[redacted]

不合格的，不得从事涉密业务。

[redacted]业事业单位违反保密管

[redacted]

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》

[redacted]

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

[redacted]

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[redacted]

（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，

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，[illegible]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。

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 [redacted]

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

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

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。

300　　200

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。

（2）进入、拍摄、窥视他人的住宅、宾馆房间等私密空间。

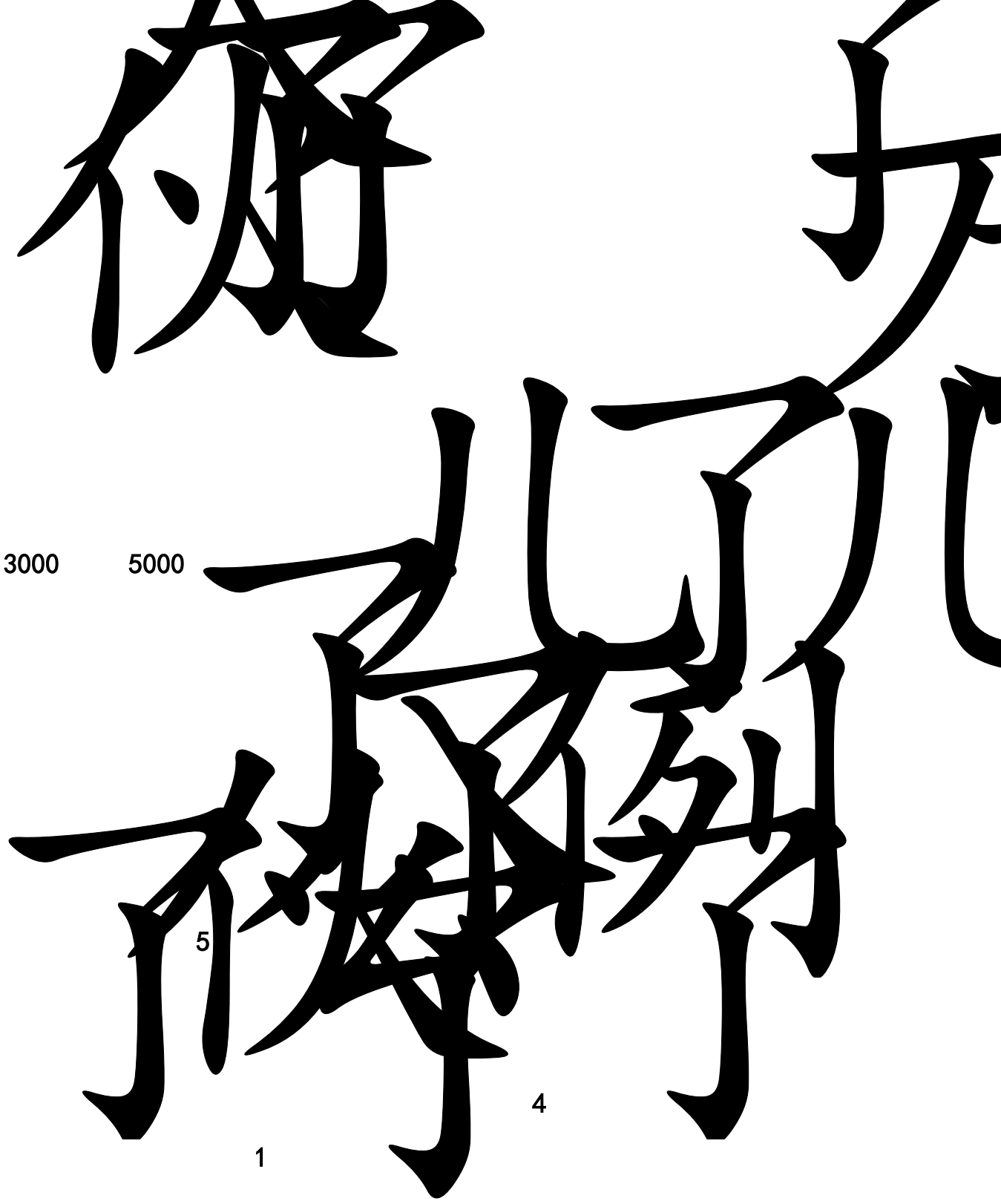
（3）拍摄、窥视、窃听、公开他人的私密活动。

（4）拍摄、窥视他人身体的私密部位。

（5）违规处理他人的私密信息。

（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。



10.4 个人[redacted]

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

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

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，

《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[illegible]事件[illegible]发生，对个人信[illegible]造成严[illegible]威胁，层出不穷的电信和网络诈骗[illegible]是因为个人信息泄[illegible]露引发的。

0

10

18

19

参考文献

[1] 2 .

[2] 2010 .

[3] 2014 .

[4] 2019 .

[5] 20 .

[6] .

[7] 2018 .

[8] 2018 .

[9] 019 .

[10] 202 .

[11]

[12] 201 16

.

[13] 2

[27 .

[14] :

2010 5

[15] : 2018

5 .

[16]

2010 1 .

[17] :

2016 3 .

[18] :

2019 4 .

[19] : 2020 5

.

[20] ,

2020 3 .

[21] .

[22] baomiguancha

[23] http://zgbmxh.cn