

**教职工理论学习资料 二〇二二年第二期**

**党委宣传部编**

**目 录**

1. **重要讲话**

[张庆伟在参加“4·15”全民国家安全教育日](#_Toc22005)[参观展览活动时强调 1](#_Toc6056)

**二、重要会议和通知**

（一）[全国保密工作会议在北京召开 4](#_Toc2301)

（二）[中共中央宣传部中央国家安全委员会办公室](#_Toc1504)[关于认真组织学习《总体国家安全观学习纲要》的通知 6](#_Toc2)

（三）[“4·15”全民国家安全教育日保密公益宣传片《保密防线》发布 9](#_Toc21742)

**三、法规规章**

（一）《[中华人民共和国保守国家秘密法》 10](#_Toc2849)

（二）《[中华人民共和国保守国家秘密法实施条例》](#_Toc3282)

[23](#_Toc3282)

（三）《[中华人民共和国国家安全法》 36](#_Toc4432)

（四）《[中华人民共和国网络安全法》 51](#_Toc17367)

（五）《[中华人民共和国反间谍法》 72](#_Toc5677)

（六）《[中华人民共和国反间谍法实施细则》 80](#_Toc9115)

（七）[《武器装备科研生产单位保密资格审查认证管理办法》 87](#_Toc26481)

**四、理论文章**

（一）【人民日报】[树牢总体国家安全观 96](#_Toc11068)

（二）【人民日报】[深刻认识中国特色国家安全道路](#_Toc30439)

[99](#_Toc30439)

（三）【保密工作】[数据安全法有哪些重点 107](#_Toc16372)

**五、警示教育**

【保密工作】[机关单位内部信息外泄案件观察 115](#_Toc19724)

**张庆伟在参加“4·15”全民国家安全教育日**

**参观展览活动时强调**

**把国家安全贯穿工作各方面全过程**

**为建设现代化新湖南提供坚强保障**

李微微朱国贤参加

来源：《湖南日报》 2022年4月15日 01版

15日上午，在第七个全民国家安全教育日到来之际，省委书记、省人大常委会主任、省委国家安全委员会主任张庆伟在省委机关展区参观“4·15”全民国家安全教育日展览。他强调，要深入学习贯彻习近平总书记关于国家安全的重要论述，牢固树立总体国家安全观，把国家安全贯穿党和政府工作各方面全过程，做到守土有责、守土尽责，以全省政治安全、社会安定、人民安宁、网络安靖迎接党的二十大胜利召开。省政协主席李微微，省委副书记、省委国家安全委员会副主任朱国贤参加。

省领导王双全、李殿勋、吴桂英、隋忠诚、谢卫江、杨浩东、南小冈、刘莲玉、许显辉参加。

在省委机关展区，张庆伟认真了解政治安全、经济安全、科技安全、网络安全、生物安全等国家安全成就，询问交流有关情况。张庆伟指出，党的十八大以来，习近平总书记创造性提出总体国家安全观，突出强调加快构建与新发展格局相适应的大安全格局，以高水平安全保障高质量发展，为我们做好新时代国家安全工作提供了根本遵循。湖南坚决贯彻党中央关于国家安全的决策部署，坚决扛牢防范化解重大风险的政治责任，坚决守住各领域安全防线，全省国家安全形势总体稳定。开展全民国家安全教育日活动，对于贯彻总体国家安全观、增强全民国家安全意识、夯实国家安全的群众基础，具有十分重要的意义。我们要进一步增强忧患意识、强化底线思维，更好统筹发展和安全，为建设现代化新湖南提供坚强保障。

张庆伟强调，要树牢总体国家安全观，立足“两个大局”，胸怀“国之大者”，深刻领会把握总体国家安全观的丰富内涵和实践要求，扎实推进国家安全体系和能力现代化。要筑牢维护国家安全防线，坚决守护好政治安全，科学统筹好疫情防控和经济社会发展，全力维护好社会大局稳定，注重开展好宣传教育，形成维护国家安全人人有责、人人可为的社会共识。要扛牢维护国家安全责任，坚持党对国家安全工作的绝对领导，严格落实各级党委（党组）国家安全工作责任制，充分发挥各级党委国安委牵头抓总作用，建立健全国家安全风险研判和防范化解机制，抓好国家安全教育基地和人才队伍建设，打造一支让党放心、让人民满意的国安铁军。

今年全民国家安全教育日的活动主题是“树牢总体国家安全观，感悟新时代国家安全成就，为迎接党的二十大胜利召开营造良好氛围”。全省各地结合疫情防控实际，通过多种形式和手段，因地制宜开展全民国家安全教育日主题宣传教育活动，提高全社会国家安全意识。

**全国保密工作会议在北京召开**

来源：国家保密局网站 2022年1月26日

2022年1月10日，全国保密工作会议以视频会议形式召开。会议全面贯彻落实党的十九大和十九届历次全会精神，总结2021年保密工作，分析形势，安排部署2022年重点工作。中共中央政治局委员、中央保密委员会主任丁薛祥出席会议并讲话。

丁薛祥指出，2021年是党和国家历史上具有里程碑意义的一年，也是保密工作开启新篇章的一年。全国保密战线以习近平新时代中国特色社会主义思想为指导，按照党中央关于保密工作的决策部署和习近平总书记重要指示批示精神，坚持统筹发展和安全，突出定密、网络保密、涉密人员“三大管理”，强化新时代保密工作保党的长期执政地位、保国家安全、保人民幸福、保民族复兴的职责使命，真抓实干、锐意进取，推动保密工作取得显著成效，实现了“十四五”良好开局。

丁薛祥强调，世界百年变局加速演进，保密工作面临的外部环境更趋复杂严峻，要深刻领会党中央决策部署的政治意图、战略谋划和实践要求，不断增强做好保密工作的使命感、责任感、紧迫感，思想上要高度警觉起来，工作上要抓紧行动起来，精神上要全面振作起来。

丁薛祥指出，做好2022年的保密工作，对于营造平稳健康的经济环境、国泰民安的社会环境、风清气正的政治环境具有特殊重要的意义。要坚持以习近平新时代中国特色社会主义思想为指导，深入学习贯彻党的十九大和十九届历次全会精神，坚决贯彻落实党中央关于保密工作的决策部署和习近平总书记重要指示批示精神，坚持总体国家安全观，统筹发展和安全，主动适应新形势新挑战，突出精准施策，加强综合防范，着力补短板、强弱项，切实强化重点领域区域保密管理，防范化解重大泄密风险，进一步加固保密防线，推动新时代保密事业高质量发展，全力保障党和国家工作大局，以实际行动迎接党的二十大胜利召开。

中央办公厅分管日常工作的副主任、中央保密委员会副主任孟祥锋主持会议。中央保密委员会组成人员和中央保密委员会成员单位、中央办公厅各单位有关负责同志在主会场参加会议，各省（自治区、直辖市）和新疆生产建设兵团党委保密委员会主要负责同志和有关部门负责同志、中央和国家机关各部门保密委员会主要负责同志和有关负责同志在分会场参加会议。

## 中共中央宣传部中央国家安全委员会办公室

## 关于认真组织学习《总体国家安全观学习纲要》的通知

来源：《人民日报》 2022年4月16日 04版

新华社北京4月15日电 中共中央宣传部中央国家安全委员会办公室关于认真组织学习《总体国家安全观学习纲要》的通知

各省、自治区、直辖市党委宣传部，中央和国家机关各部委、各人民团体宣传部门，全国党委国家安全系统，各中管金融企业党委，部分国有重要骨干企业党组（党委），部分高等学校党委，中央军委政治工作部宣传局：

　　党的十八大以来，以习近平同志为核心的党中央顺应时代发展大势，从新时代坚持和发展中国特色社会主义的战略高度，把马克思主义国家安全理论和当代中国安全实践、中华优秀传统战略文化结合起来，创造性提出了总体国家安全观。党的十九大将坚持总体国家安全观纳入新时代坚持和发展中国特色社会主义的基本方略，并写入党章，反映了全党全国人民的共同意志。总体国家安全观是我们党历史上第一个被确立为国家安全工作指导思想的重大战略思想，是中国共产党和中国人民捍卫国家主权、安全、发展利益百年奋斗实践经验和集体智慧的结晶，是马克思主义国家安全理论中国化的最新成果，是习近平新时代中国特色社会主义思想的重要组成部分，是新时代国家安全工作的根本遵循和行动指南。

　　根据党中央统一部署，为把学习贯彻习近平新时代中国特色社会主义思想特别是总体国家安全观不断引向深入，中共中央宣传部、中央国安办组织编写了《总体国家安全观学习纲要》（以下简称《纲要》）。《纲要》全面反映习近平新时代中国特色社会主义思想在国家安全方面的原创性贡献，系统阐释总体国家安全观的基本精神、基本内容、基本方法、基本要求，为广大干部群众学习贯彻总体国家安全观提供了权威辅助读物。

　　各级党委（党组）要坚持不懈用习近平新时代中国特色社会主义思想武装头脑、指导实践、推动工作。要组织党员认真学习领会总体国家安全观的重大意义、核心要义、精神实质、丰富内涵、实践要求，坚持读原著、学原文、悟原理，努力掌握贯穿其中的马克思主义立场观点方法，不断深化认识，全面理解把握。要把《纲要》纳入学习计划，作为党委（党组）理论学习中心组学习、干部培训、党员学习的重要内容。全国党委国家安全系统要结合工作实际组织好本系统党员干部的学习。要坚持全面系统学、及时跟进学、深入思考学、联系实际学，更加自觉用总体国家安全观指导驾驭纷繁复杂国家安全形势、提高应对风险挑战能力，切实把学习成效转化为坚决维护国家主权、安全、发展利益的生动实践。

要通过广泛的学习宣传阐释工作，引导广大干部群众进一步学懂弄通做实习近平新时代中国特色社会主义思想，深入学习贯彻总体国家安全观，深刻领会“两个确立”的决定性意义，增强“四个意识”、坚定“四个自信”、做到“两个维护”，在思想上政治上行动上同以习近平同志为核心的党中央保持高度一致，不忘初心、牢记使命，常怀远虑、居安思危，砥砺奋进、攻坚克难，坚定不移走中国特色国家安全道路，不断开创新时代国家安全工作新局面，为夺取全面建设社会主义现代化国家新胜利、实现中华民族伟大复兴的中国梦不懈奋斗。

## **“4·15”全民国家安全教育日保密公益宣传片《保密防线》发布**

来源：国家保密局网站 2022年4月15日

2022年保密公益宣传片《保密防线》于“4·15”全民国家安全教育日面向全社会发布。宣传片以总体国家安全观为指导，重点突出“保守国家秘密，公民人人有责”这一主题，旨在增强社会公民保密意识，筑牢安全保密防线。

保密公益宣传片立足诠释“保密为了人民、保密依靠人民”的理念，以“每个人心中都有一道保密防线”开篇，通过个人和家庭、社会和国家等各场景保密防线连接，说明保密防线对国家安全、社会发展、个人成长的重要意义，呼吁全社会筑牢安全保密防线，共同守护国家秘密安全。

此次发布的保密公益宣传片，由国家保密局制作推出。此外，国家保密局还通过设计推出保密公益宣传海报、开展“保密故事大家讲”等活动，积极阐释新时代公民的保密责任，大力弘扬党的保密工作优良传统。

附链接：http://www.gjbmj.gov.cn/n1/2022/0415/c409082-32400028.html

## **中华人民共和国保守国家秘密法**

（自2010年10月1日起施行）

来源：中国政府网

第一章 总 则

第一条 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。

第二条 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。

第三条 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。

第四条 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。

第五条 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管理部门主管本行政区域的保密工作。

第六条 国家机关和涉及国家秘密的单位（以下简称机关、单位）管理本机关和本单位的保密工作。

中央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。

第七条 机关、单位应当实行保密工作责任制，健全保密管理制度，完善保密防护措施，开展保密宣传教育，加强保密检查。

第八条 国家对在保守、保护国家秘密以及改进保密技术、措施等方面成绩显著的单位或者个人给予奖励。

第二章 国家秘密的范围和密级

第九条 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：

（一）国家事务重大决策中的秘密事项；

（二）国防建设和武装力量活动中的秘密事项；

（三）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；

（四）国民经济和社会发展中的秘密事项；

（五）科学技术中的秘密事项；

（六）维护国家安全活动和追查刑事犯罪中的秘密事项；

（七）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。

第十条 国家秘密的密级分为绝密、机密、秘密三级。

绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害；机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害；秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害。

第十一条 国家秘密及其密级的具体范围，由国家保密行政管理部门分别会同外交、公安、国家安全和其他中央有关机关规定。

军事方面的国家秘密及其密级的具体范围，由中央军事委员会规定。

国家秘密及其密级的具体范围的规定，应当在有关范围内公布，并根据情况变化及时调整。

第十二条 机关、单位负责人及其指定的人员为定密责任人，负责本机关、本单位的国家秘密确定、变更和解除工作。

机关、单位确定、变更和解除本机关、本单位的国家秘密，应当由承办人提出具体意见，经定密责任人审核批准。

第十三条 确定国家秘密的密级，应当遵守定密权限。

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

机关、单位执行上级确定的国家秘密事项，需要定密的，根据所执行的国家秘密事项的密级确定。下级机关、单位认为本机关、本单位产生的有关定密事项属于上级机关、单位的定密权限，应当先行采取保密措施，并立即报请上级机关、单位确定；没有上级机关、单位的，应当立即提请有相应定密权限的业务主管部门或者保密行政管理部门确定。

公安、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。

第十四条 机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级，同时确定保密期限和知悉范围。

第十五条 国家秘密的保密期限，应当根据事项的性质和特点，按照维护国家安全和利益的需要，限定在必要的期限内；不能确定期限的，应当确定解密的条件。

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

机关、单位应当根据工作需要，确定具体的保密期限、解密时间或者解密条件。

机关、单位对在决定和处理有关事项工作过程中确定需要保密的事项，根据工作需要决定公开的，正式公布时即视为解密。

第十六条 国家秘密的知悉范围，应当根据工作需要限定在最小范围。

国家秘密的知悉范围能够限定到具体人员的，限定到具体人员；不能限定到具体人员的，限定到机关、单位，由机关、单位限定到具体人员。

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

第十七条 机关、单位对承载国家秘密的纸介质、光介质、电磁介质等载体（以下简称国家秘密载体）以及属于国家秘密的设备、产品，应当做出国家秘密标志。

不属于国家秘密的，不应当做出国家秘密标志。

第十八条 国家秘密的密级、保密期限和知悉范围，应当根据情况变化及时变更。国家秘密的密级、保密期限和知悉范围的变更，由原定密机关、单位决定，也可以由其上级机关决定。

国家秘密的密级、保密期限和知悉范围变更的，应当及时书面通知知悉范围内的机关、单位或者人员。

第十九条 国家秘密的保密期限已满的，自行解密。

机关、单位应当定期审核所确定的国家秘密。对在保密期限内因保密事项范围调整不再作为国家秘密事项，或者公开后不会损害国家安全和利益，不需要继续保密的，应当及时解密；对需要延长保密期限的，应当在原保密期限届满前重新确定保密期限。提前解密或者延长保密期限的，由原定密机关、单位决定，也可以由其上级机关决定。

第二十条 机关、单位对是否属于国家秘密或者属于何种密级不明确或者有争议的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门确定。

第三章 保密制度

第二十一条 国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁，应当符合国家保密规定。

绝密级国家秘密载体应当在符合国家保密标准的设施、设备中保存，并指定专人管理；未经原定密机关、单位或者其上级机关批准，不得复制和摘抄；收发、传递和外出携带，应当指定人员负责，并采取必要的安全措施。

第二十二条 属于国家秘密的设备、产品的研制、生产、运输、使用、保存、维修和销毁，应当符合国家保密规定。

第二十三条 存储、处理国家秘密的计算机信息系统（以下简称涉密信息系统）按照涉密程度实行分级保护。

涉密信息系统应当按照国家保密标准配备保密设施、设备。保密设施、设备应当与涉密信息系统同步规划，同步建设，同步运行。

涉密信息系统应当按照规定，经检查合格后，方可投入使用。

第二十四条 机关、单位应当加强对涉密信息系统的管理，任何组织和个人不得有下列行为：

（一）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；

（二）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；

（三）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；

（四）擅自卸载、修改涉密信息系统的安全技术程序、管理程序；

（五）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。

第二十五条 机关、单位应当加强对国家秘密载体的管理，任何组织和个人不得有下列行为：

（一）非法获取、持有国家秘密载体；

（二）买卖、转送或者私自销毁国家秘密载体；

（三）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；

（四）邮寄、托运国家秘密载体出境；

（五）未经有关主管部门批准，携带、传递国家秘密载体出境。

第二十六条 禁止非法复制、记录、存储国家秘密。

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

禁止在私人交往和通信中涉及国家秘密。

第二十七条 报刊、图书、音像制品、电子出版物的编辑、出版、印制、发行，广播节目、电视节目、电影的制作和播放，互联网、移动通信网等公共信息网络及其他传媒的信息编辑、发布，应当遵守有关保密规定。

第二十八条 互联网及其他公共信息网络运营商、服务商应当配合公安机关、国家安全机关、检察机关对泄密案件进行调查；发现利用互联网及其他公共信息网络发布的信息涉及泄露国家秘密的，应当立即停止传输，保存有关记录，向公安机关、国家安全机关或者保密行政管理部门报告；应当根据公安机关、国家安全机关或者保密行政管理 部门的要求，删除涉及泄露国家秘密的信息。

第二十九条 机关、单位公开发布信息以及对涉及国家秘密的工程、货物、服务进行采购时，应当遵守保密规定。

第三十条 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。

第三十一条 举办会议或者其他活动涉及国家秘密的，主办单位应当采取保密措施，并对参加人员进行保密教育，提出具体保密要求。

第三十二条 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。

第三十三条 军事禁区和属于国家秘密不对外开放的其他场所、部位，应当采取保密措施，未经有关部门批准，不得擅自决定对外开放或者扩大开放范围。

第三十四条 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。

机关、单位委托企业事业单位从事前款规定的业务，应当与其签订保密协议，提出保密要求，采取保密措施。

第三十五条 在涉密岗位工作的人员（以下简称涉密人员），按照涉密程度分为核心涉密人员、重要涉密人员和一般涉密人员，实行分类管理。

任用、聘用涉密人员应当按照有关规定进行审查。

涉密人员应当具有良好的政治素质和品行，具有胜任涉密岗位所要求的工作能力。

涉密人员的合法权益受法律保护。

第三十六条 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。

第三十七条 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。

第三十八条 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。

第三十九条 机关、单位应当建立健全涉密人员管理制度，明确涉密人员的权利、岗位责任和要求，对涉密人员履行职责情况开展经常性的监督检查。

第四十条 国家工作人员或者其他公民发现国家秘密已经泄露或者可能泄露时，应当立即采取补救措施并及时报告有关机关、单位。机关、单位接到报告后，应当立即作出处理，并及时向保密行政管理部门报告。

第四章 监督管理

第四十一条 国家保密行政管理部门依照法律、行政法规的规定，制定保密规章和国家保密标准。

第四十二条 保密行政管理部门依法组织开展保密宣传教育、保密检查、保密技术防护和泄密案件查处工作，对机关、单位的保密工作进行指导和监督。

第四十三条 保密行政管理部门发现国家秘密确定、变更或者解除不当的，应当及时通知有关机关、单位予以纠正。

第四十四条 保密行政管理部门对机关、单位遵守保密制度的情况进行检查，有关机关、单位应当配合。保密行政管理部门发现机关、单位存在泄密隐患的，应当要求其采取措施，限期整改；对存在泄密隐患的设施、设备、场所，应当责令停止使用；对严重违反保密规定的涉密人员，应当建议有关机关、单位给予处分并调离涉密岗位；发现涉嫌泄露国家秘密的，应当督促、指导有关机关、单位进行调查处理。涉嫌犯罪的，移送司法机关处理。

第四十五条 保密行政管理部门对保密检查中发现的非法获取、持有的国家秘密载体，应当予以收缴。

第四十六条 办理涉嫌泄露国家秘密案件的机关，需要对有关事项是否属于国家秘密以及属于何种密级进行鉴定的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门鉴定。

第四十七条 机关、单位对违反保密规定的人员不依法给予处分的，保密行政管理部门应当建议纠正，对拒不纠正的，提请其上一级机关或者监察机关对该机关、单位负有责任的领导人员和直接责任人员依法予以处理。

第五章 法律责任

第四十八条 违反本法规定，有下列行为之一的，依法给予处分；构成犯罪的，依法追究刑事责任：

（一）非法获取、持有国家秘密载体的；

（二）买卖、转送或者私自销毁国家秘密载体的；

（三）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；

（四）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；

（五）非法复制、记录、存储国家秘密的；

（六）在私人交往和通信中涉及国家秘密的；

（七）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；

（八）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；

（九）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；

（十）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；

（十一）擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；

（十二）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。

有前款行为尚不构成犯罪，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。

第四十九条 机关、单位违反本法规定，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、单位违反本法规定，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。

第五十条 互联网及其他公共信息网络运营商、服务商违反本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。

第五十一条 保密行政管理部门的工作人员在履行保密管理职责中滥用职权、玩忽职守、徇私舞弊的，依法给予处分；构成犯罪的，依法追究刑事责任。

第六章 附 则

第五十二条 中央军事委员会根据本法制定中国人民解放军保密条例。

第五十三条 本法自2010年10月1日起施行。

**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）

来源：中国政府网

第一章 总 则

第一条 根据《中华人民共和国保守国家秘密法》（以下简称保密法）的规定，制定本条例。

第二条 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管理部门在上级保密行政管理部门指导下，主管本行政区域的保密工作。

第三条 中央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，监督执行保密法律法规，可以根据实际情况制定或者会同有关部门制定主管业务方面的保密规定。

第四条 县级以上人民政府应当加强保密基础设施建设和关键保密科技产品的配备。

省级以上保密行政管理部门应当加强关键保密科技产品的研发工作。

保密行政管理部门履行职责所需的经费，应当列入本级人民政府财政预算。机关、单位开展保密工作所需经费应当列入本机关、本单位的年度财政预算或者年度收支计划。

第五条 机关、单位不得将依法应当公开的事项确定为国家秘密，不得将涉及国家秘密的信息公开。

第六条 机关、单位实行保密工作责任制。机关、单位负责人对本机关、本单位的保密工作负责，工作人员对本岗位的保密工作负责。

机关、单位应当根据保密工作需要设立保密工作机构或者指定人员专门负责保密工作。

机关、单位及其工作人员履行保密工作责任制情况应当纳入年度考评和考核内容。

第七条 各级保密行政管理部门应当组织开展经常性的保密宣传教育。机关、单位应当定期对本机关、本单位工作人员进行保密形势、保密法律法规、保密技术防范等方面的教育培训。

第二章 国家秘密的范围和密级

第八条 国家秘密及其密级的具体范围（以下称保密事项范围）应当明确规定国家秘密具体事项的名称、密级、保密期限、知悉范围。

保密事项范围应当根据情况变化及时调整。制定、修订保密事项范围应当充分论证，听取有关机关、单位和相关领域专家的意见。

第九条 机关、单位负责人为本机关、本单位的定密责任人，根据工作需要，可以指定其他人员为定密责任人。

专门负责定密的工作人员应当接受定密培训，熟悉定密职责和保密事项范围，掌握定密程序和方法。

第十条 定密责任人在职责范围内承担有关国家秘密确定、变更和解除工作。具体职责是：

（一）审核批准本机关、本单位产生的国家秘密的密级、保密期限和知悉范围；

（二）对本机关、本单位产生的尚在保密期限内的国家秘密进行审核，作出是否变更或者解除的决定；

（三）对是否属于国家秘密和属于何种密级不明确的事项先行拟定密级，并按照规定的程序报保密行政管理部门确定。

第十一条 中央国家机关、省级机关以及设区的市、自治州级机关可以根据保密工作需要或者有关机关、单位的申请，在国家保密行政管理部门规定的定密权限、授权范围内作出定密授权。

定密授权应当以书面形式作出。授权机关应当对被授权机关、单位履行定密授权的情况进行监督。

中央国家机关、省级机关作出的授权，报国家保密行政管理部门备案；设区的市、自治州级机关作出的授权，报省、自治区、直辖市保密行政管理部门备案。

第十二条 机关、单位应当在国家秘密产生的同时，由承办人依据有关保密事项范围拟定密级、保密期限和知悉范围，报定密责任人审核批准，并采取相应保密措施。

第十三条 机关、单位对所产生的国家秘密，应当按照保密事项范围的规定确定具体的保密期限；保密事项范围没有规定具体保密期限的，可以根据工作需要，在保密法规定的保密期限内确定；不能确定保密期限的，应当确定解密条件。

国家秘密的保密期限，自标明的制发日起计算；不能标明制发日的，确定该国家秘密的机关、单位应当书面通知知悉范围内的机关、单位和人员，保密期限自通知之日起计算。

第十四条 机关、单位应当按照保密法的规定，严格限定国家秘密的知悉范围，对知悉机密级以上国家秘密的人员，应当作出书面记录。

第十五条 国家秘密载体以及属于国家秘密的设备、产品的明显部位应当标注国家秘密标志。国家秘密标志应当标注密级和保密期限。国家秘密的密级和保密期限发生变更的，应当及时对原国家秘密标志作出变更。

无法标注国家秘密标志的，确定该国家秘密的机关、单位应当书面通知知悉范围内的机关、单位和人员。

第十六条 机关、单位对所产生的国家秘密，认为符合保密法有关解密或者延长保密期限规定的，应当及时解密或者延长保密期限。

机关、单位对不属于本机关、本单位产生的国家秘密，认为符合保密法有关解密或者延长保密期限规定的，可以向原定密机关、单位或者其上级机关、单位提出建议。

已经依法移交各级国家档案馆的属于国家秘密的档案，由原定密机关、单位按照国家有关规定进行解密审核。

第十七条 机关、单位被撤销或者合并的，该机关、单位所确定国家秘密的变更和解除，由承担其职能的机关、单位负责，也可以由其上级机关、单位或者保密行政管理部门指定的机关、单位负责。

第十八条 机关、单位发现本机关、本单位国家秘密的确定、变更和解除不当的，应当及时纠正；上级机关、单位发现下级机关、单位国家秘密的确定、变更和解除不当的，应当及时通知其纠正，也可以直接纠正。

第十九条 机关、单位对符合保密法的规定，但保密事项范围没有规定的不明确事项，应当先行拟定密级、保密期限和知悉范围，采取相应的保密措施，并自拟定之日起10日内报有关部门确定。拟定为绝密级的事项和中央国家机关拟定的机密级、秘密级的事项，报国家保密行政管理部门确定；其他机关、单位拟定的机密级、秘密级的事项，报省、自治区、直辖市保密行政管理部门确定。

保密行政管理部门接到报告后，应当在10日内作出决定。省、自治区、直辖市保密行政管理部门还应当将所作决定及时报国家保密行政管理部门备案。

第二十条 机关、单位对已定密事项是否属于国家秘密或者属于何种密级有不同意见的，可以向原定密机关、单位提出异议，由原定密机关、单位作出决定。

机关、单位对原定密机关、单位未予处理或者对作出的决定仍有异议的，按照下列规定办理：

（一）确定为绝密级的事项和中央国家机关确定的机密级、秘密级的事项，报国家保密行政管理部门确定。

（二）其他机关、单位确定的机密级、秘密级的事项，报省、自治区、直辖市保密行政管理部门确定；对省、自治区、直辖市保密行政管理部门作出的决定有异议的，可以报国家保密行政管理部门确定。

在原定密机关、单位或者保密行政管理部门作出决定前，对有关事项应当按照主张密级中的最高密级采取相应的保密措施。

第三章 保密制度

第二十一条 国家秘密载体管理应当遵守下列规定：

（一）制作国家秘密载体，应当由机关、单位或者经保密行政管理部门保密审查合格的单位承担，制作场所应当符合保密要求。

（二）收发国家秘密载体，应当履行清点、编号、登记、签收手续。

（三）传递国家秘密载体，应当通过机要交通、机要通信或者其他符合保密要求的方式进行。

（四）复制国家秘密载体或者摘录、引用、汇编属于国家秘密的内容，应当按照规定报批，不得擅自改变原件的密级、保密期限和知悉范围，复制件应当加盖复制机关、单位戳记，并视同原件进行管理。

（五）保存国家秘密载体的场所、设施、设备，应当符合国家保密要求。

（六）维修国家秘密载体，应当由本机关、本单位专门技术人员负责。确需外单位人员维修的，应当由本机关、本单位的人员现场监督；确需在本机关、本单位以外维修的，应当符合国家保密规定。

（七）携带国家秘密载体外出，应当符合国家保密规定，并采取可靠的保密措施；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。

第二十二条 销毁国家秘密载体应当符合国家保密规定和标准，确保销毁的国家秘密信息无法还原。

销毁国家秘密载体应当履行清点、登记、审批手续，并送交保密行政管理部门设立的销毁工作机构或者保密行政管理部门指定的单位销毁。机关、单位确因工作需要，自行销毁少量国家秘密载体的，应当使用符合国家保密标准的销毁设备和方法。

第二十三条 涉密信息系统按照涉密程度分为绝密级、机密级、秘密级。机关、单位应当根据涉密信息系统存储、处理信息的最高密级确定系统的密级，按照分级保护要求采取相应的安全保密防护措施。

第二十四条 涉密信息系统应当由国家保密行政管理部门设立或者授权的保密测评机构进行检测评估，并经设区的市、自治州级以上保密行政管理部门审查合格，方可投入使用。

公安、国家安全机关的涉密信息系统投入使用的管理办法，由国家保密行政管理部门会同国务院公安、国家安全部门另行规定。

第二十五条 机关、单位应当加强涉密信息系统的运行使用管理，指定专门机构或者人员负责运行维护、安全保密管理和安全审计，定期开展安全保密检查和风险评估。

涉密信息系统的密级、主要业务应用、使用范围和使用环境等发生变化或者涉密信息系统不再使用的，应当按照国家保密规定及时向保密行政管理部门报告，并采取相应措施。

第二十六条 机关、单位采购涉及国家秘密的工程、货物和服务的，应当根据国家保密规定确定密级，并符合国家保密规定和标准。机关、单位应当对提供工程、货物和服务的单位提出保密管理要求，并与其签订保密协议。

政府采购监督管理部门、保密行政管理部门应当依法加强对涉及国家秘密的工程、货物和服务采购的监督管理。

第二十七条 举办会议或者其他活动涉及国家秘密的，主办单位应当采取下列保密措施：

（一）根据会议、活动的内容确定密级，制定保密方案，限定参加人员范围；

（二）使用符合国家保密规定和标准的场所、设施、设备；

（三）按照国家保密规定管理国家秘密载体；

（四）对参加人员提出具体保密要求。

第二十八条 企业事业单位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的业务（以下简称涉密业务），应当由保密行政管理部门或者保密行政管理部门会同有关部门进行保密审查。保密审查不合格的，不得从事涉密业务。

第二十九条 从事涉密业务的企业事业单位应当具备下列条件：

（一）在中华人民共和国境内依法成立3年以上的法人，无违法犯罪记录；

（二）从事涉密业务的人员具有中华人民共和国国籍；

（三）保密制度完善，有专门的机构或者人员负责保密工作；

（四）用于涉密业务的场所、设施、设备符合国家保密规定和标准；

（五）具有从事涉密业务的专业能力；

（六）法律、行政法规和国家保密行政管理部门规定的其他条件。

第三十条 涉密人员的分类管理、任（聘）用审查、脱密期管理、权益保障等具体办法，由国家保密行政管理部门会同国务院有关主管部门制定。

第四章 监督管理

第三十一条 机关、单位应当向同级保密行政管理部门报送本机关、本单位年度保密工作情况。下级保密行政管理部门应当向上级保密行政管理部门报送本行政区域年度保密工作情况。

第三十二条 保密行政管理部门依法对机关、单位执行保密法律法规的下列情况进行检查：

（一）保密工作责任制落实情况；

（二）保密制度建设情况；

（三）保密宣传教育培训情况；

（四）涉密人员管理情况；

（五）国家秘密确定、变更和解除情况；

（六）国家秘密载体管理情况；

（七）信息系统和信息设备保密管理情况；

（八）互联网使用保密管理情况；

（九）保密技术防护设施设备配备使用情况；

（十）涉密场所及保密要害部门、部位管理情况；

（十一）涉密会议、活动管理情况；

（十二）信息公开保密审查情况。

第三十三条 保密行政管理部门在保密检查过程中，发现有泄密隐患的，可以查阅有关材料、询问人员、记录情况；对有关设施、设备、文件资料等可以依法先行登记保存，必要时进行保密技术检测。有关机关、单位及其工作人员对保密检查应当予以配合。

保密行政管理部门实施检查后，应当出具检查意见，对需要整改的，应当明确整改内容和期限。

第三十四条 机关、单位发现国家秘密已经泄露或者可能泄露的，应当立即采取补救措施，并在24小时内向同级保密行政管理部门和上级主管部门报告。

地方各级保密行政管理部门接到泄密报告的，应当在24小时内逐级报至国家保密行政管理部门。

第三十五条 保密行政管理部门对公民举报、机关和单位报告、保密检查发现、有关部门移送的涉嫌泄露国家秘密的线索和案件，应当依法及时调查或者组织、督促有关机关、单位调查处理。调查工作结束后，认为有违反保密法律法规的事实，需要追究责任的，保密行政管理部门可以向有关机关、单位提出处理建议。有关机关、单位应当及时将处理结果书面告知同级保密行政管理部门。

第三十六条 保密行政管理部门收缴非法获取、持有的国家秘密载体，应当进行登记并出具清单，查清密级、数量、来源、扩散范围等，并采取相应的保密措施。

保密行政管理部门可以提请公安、工商行政管理等有关部门协助收缴非法获取、持有的国家秘密载体，有关部门应当予以配合。

第三十七条 国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门应当依据保密法律法规和保密事项范围，对办理涉嫌泄露国家秘密案件的机关提出鉴定的事项是否属于国家秘密、属于何种密级作出鉴定。

保密行政管理部门受理鉴定申请后，应当自受理之日起30日内出具鉴定结论；不能按期出具鉴定结论的，经保密行政管理部门负责人批准，可以延长30日。

第三十八条 保密行政管理部门及其工作人员应当按照法定的职权和程序开展保密审查、保密检查和泄露国家秘密案件查处工作，做到科学、公正、严格、高效，不得利用职权谋取利益。

第五章 法律责任

第三十九条 机关、单位发生泄露国家秘密案件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。

第四十条 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。

第四十一条 经保密审查合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。

第四十二条 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。

第四十三条 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。

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。

第四十四条 保密行政管理部门未依法履行职责，或者滥用职权、玩忽职守、徇私舞弊的，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；构成犯罪的，依法追究刑事责任。

第六章 附 则

第四十五条 本条例自2014年3月1日起施行。1990年4月25日国务院批准、1990年5月25日国家保密局发布的《中华人民共和国保守国家秘密法实施办法》同时废止。

**中华人民共和国国家安全法**

（2015年7月1日第十二届全国人民代表大会常务委员会第十五次会议通过）

来源：中国政府网

第一章 总则

第一条 为了维护国家安全，保卫人民民主专政的政权和中国特色社会主义制度，保护人民的根本利益，保障改革开放和社会主义现代化建设的顺利进行，实现中华民族伟大复兴，根据宪法，制定本法。

第二条 国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

第三条 国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。

第四条 坚持中国共产党对国家安全工作的领导，建立集中统一、高效权威的国家安全领导体制。

第五条 中央国家安全领导机构负责国家安全工作的决策和议事协调，研究制定、指导实施国家安全战略和有关重大方针政策，统筹协调国家安全重大事项和重要工作，推动国家安全法治建设。

第六条 国家制定并不断完善国家安全战略，全面评估国际、国内安全形势，明确国家安全战略的指导方针、中长期目标、重点领域的国家安全政策、工作任务和措施。

第七条 维护国家安全，应当遵守宪法和法律，坚持社会主义法治原则，尊重和保障人权，依法保护公民的权利和自由。

第八条 维护国家安全，应当与经济社会发展相协调。

国家安全工作应当统筹内部安全和外部安全、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。

第九条 维护国家安全，应当坚持预防为主、标本兼治，专门工作与群众路线相结合，充分发挥专门机关和其他有关机关维护国家安全的职能作用，广泛动员公民和组织，防范、制止和依法惩治危害国家安全的行为。

第十条 维护国家安全，应当坚持互信、互利、平等、协作，积极同外国政府和国际组织开展安全交流合作，履行国际安全义务，促进共同安全，维护世界和平。

第十一条 中华人民共和国公民、一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织，都有维护国家安全的责任和义务。

中国的主权和领土完整不容侵犯和分割。维护国家主权、统一和领土完整是包括港澳同胞和台湾同胞在内的全中国人民的共同义务。

第十二条 国家对在维护国家安全工作中作出突出贡献的个人和组织给予表彰和奖励。

第十三条 国家机关工作人员在国家安全工作和涉及国家安全活动中，滥用职权、玩忽职守、徇私舞弊的，依法追究法律责任。

任何个人和组织违反本法和有关法律，不履行维护国家安全义务或者从事危害国家安全活动的，依法追究法律责任。

第十四条 每年4月15日为全民国家安全教育日。

第二章 维护国家安全的任务

第十五条 国家坚持中国共产党的领导，维护中国特色社会主义制度，发展社会主义民主政治，健全社会主义法治，强化权力运行制约和监督机制，保障人民当家作主的各项权利。

国家防范、制止和依法惩治任何叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力的渗透、破坏、颠覆、分裂活动。

第十六条 国家维护和发展最广大人民的根本利益，保卫人民安全，创造良好生存发展条件和安定工作生活环境，保障公民的生命财产安全和其他合法权益。

第十七条 国家加强边防、海防和空防建设，采取一切必要的防卫和管控措施，保卫领陆、内水、领海和领空安全，维护国家领土主权和海洋权益。

第十八条 国家加强武装力量革命化、现代化、正规化建设，建设与保卫国家安全和发展利益需要相适应的武装力量；实施积极防御军事战略方针，防备和抵御侵略，制止武装 颠覆和分裂；开展国际军事安全合作，实施联合国维和、国际救援、海上护航和维护国家海外利益的军事行动，维护国家主权、安全、领土完整、发展利益和世界和 平。

第十九条 国家维护国家基本经济制度和社会主义市场经济秩序，健全预防和化解经济安全风险的制度机制，保障关系国民经济命脉的重要行业和关键领域、重点产业、重大基础设施和重大建设项目以及其他重大经济利益安全。

第二十条 国家健全金融宏观审慎管理和金融风险防范、处置机制，加强金融基础设施和基础能力建设，防范和化解系统性、区域性金融风险，防范和抵御外部金融风险的冲击。

第二十一条 国家合理利用和保护资源能源，有效管控战略资源能源的开发，加强战略资源能源储备，完善资源能源运输战略通道建设和安全保护措施，加强国际资源能源合作，全面提升应急保障能力，保障经济社会发展所需的资源能源持续、可靠和有效供给。

第二十二条 国家健全粮食安全保障体系，保护和提高粮食综合生产能力，完善粮食储备制度、流通体系和市场调控机制，健全粮食安全预警制度，保障粮食供给和质量安全。

第二十三条 国家坚持社会主义先进文化前进方向，继承和弘扬中华民族优秀传统文化，培育和践行社会主义核心价值观，防范和抵制不良文化的影响，掌握意识形态领域主导权，增强文化整体实力和竞争力。

第二十四条 国家加强自主创新能力建设，加快发展自主可控的战略高新技术和重要领域核心关键技术，加强知识产权的运用、保护和科技保密能力建设，保障重大技术和工程的安全。

第二十五条 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领 域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间 主权、安全和发展利益。

第二十六条 国家坚持和完善民族区域自治制度，巩固和发展平等团结互助和谐的社会主义民族关系。坚持各民族一律平等，加强民族交往、交流、交融，防范、制止和依法惩治民族分裂活动，维护国家统一、民族团结和社会和谐，实现各民族共同团结奋斗、共同繁荣发展。

第二十七条 国家依法保护公民宗教信仰自由和正常宗教活动，坚持宗教独立自主自办的原则，防范、制止和依法惩治利用宗教名义进行危害国家安全的违法犯罪活动，反对境外势力干涉境内宗教事务，维护正常宗教活动秩序。

国家依法取缔邪教组织，防范、制止和依法惩治邪教违法犯罪活动。

第二十八条 国家反对一切形式的恐怖主义和极端主义，加强防范和处置恐怖主义的能力建设，依法开展情报、调查、防范、处置以及资金监管等工作，依法取缔恐怖活动组织和严厉惩治暴力恐怖活动。

第二十九条 国家健全有效预防和化解社会矛盾的体制机制，健全公共安全体系，积极预防、减少和化解社会矛盾，妥善处置公共卫生、社会安全等影响国家安全和社会稳定的突发事件，促进社会和谐，维护公共安全和社会安定。

第三十条 国家完善生态环境保护制度体系，加大生态建设和环境保护力度，划定生态保护红线，强化生态风险的预警和防控，妥善处置突发环境事件，保障人民赖以生存发展的大气、水、土壤等自然环境和条件不受威胁和破坏，促进人与自然和谐发展。

第三十一条 国家坚持和平利用核能和核技术，加强国际合作，防止核扩散，完善防扩散机制，加强对核设施、核材料、核活动和核废料处置的安全管理、监管和保护，加强核事 故应急体系和应急能力建设，防止、控制和消除核事故对公民生命健康和生态环境的危害，不断增强有效应对和防范核威胁、核攻击的能力。

第三十二条 国家坚持和平探索和利用外层空间、国际海底区域和极地，增强安全进出、科学考察、开发利用的能力，加强国际合作，维护我国在外层空间、国际海底区域和极地的活动、资产和其他利益的安全。

第三十三条 国家依法采取必要措施，保护海外中国公民、组织和机构的安全和正当权益，保护国家的海外利益不受威胁和侵害。

第三十四条 国家根据经济社会发展和国家发展利益的需要，不断完善维护国家安全的任务。

第三章 维护国家安全的职责

第三十五条 全国人民代表大会依照宪法规定，决定战争和和平的问题，行使宪法规定的涉及国家安全的其他职权。

全国人民代表大会常务委员会依照宪法规定，决定战争状态的宣布，决定全国总动员或者局部动员，决定全国或者个别省、自治区、直辖市进入紧急状态，行使宪法规定的和全国人民代表大会授予的涉及国家安全的其他职权。

第三十六条 中华人民共和国主席根据全国人民代表大会的决定和全国人民代表大会常务委员会的决定，宣布进入紧急状态，宣布战争状态，发布动员令，行使宪法规定的涉及国家安全的其他职权。

第三十七条 国务院根据宪法和法律，制定涉及国家安全的行政法规，规定有关行政措施，发布有关决定和命令；实施国家安全法律法规和政策；依照法律规定决定省、自治区、 直辖市的范围内部分地区进入紧急状态；行使宪法法律规定的和全国人民代表大会及其常务委员会授予的涉及国家安全的其他职权。

第三十八条 中央军事委员会领导全国武装力量，决定军事战略和武装力量的作战方针，统一指挥维护国家安全的军事行动，制定涉及国家安全的军事法规，发布有关决定和命令。

第三十九条 中央国家机关各部门按照职责分工，贯彻执行国家安全方针政策和法律法规，管理指导本系统、本领域国家安全工作。

第四十条 地方各级人民代表大会和县级以上地方各级人民代表大会常务委员会在本行政区域内，保证国家安全法律法规的遵守和执行。

地方各级人民政府依照法律法规规定管理本行政区域内的国家安全工作。

香港特别行政区、澳门特别行政区应当履行维护国家安全的责任。

第四十一条 人民法院依照法律规定行使审判权，人民检察院依照法律规定行使检察权，惩治危害国家安全的犯罪。

第四十二条 国家安全机关、公安机关依法搜集涉及国家安全的情报信息，在国家安全工作中依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。

有关军事机关在国家安全工作中依法行使相关职权。

第四十三条 国家机关及其工作人员在履行职责时，应当贯彻维护国家安全的原则。

国家机关及其工作人员在国家安全工作和涉及国家安全活动中，应当严格依法履行职责，不得超越职权、滥用职权，不得侵犯个人和组织的合法权益。

第四章 国家安全制度

第一节 一般规定

第四十四条 中央国家安全领导机构实行统分结合、协调高效的国家安全制度与工作机制。

第四十五条 国家建立国家安全重点领域工作协调机制，统筹协调中央有关职能部门推进相关工作。

第四十六条 国家建立国家安全工作督促检查和责任追究机制，确保国家安全战略和重大部署贯彻落实。

第四十七条 各部门、各地区应当采取有效措施，贯彻实施国家安全战略。

第四十八条 国家根据维护国家安全工作需要，建立跨部门会商工作机制，就维护国家安全工作的重大事项进行会商研判，提出意见和建议。

第四十九条 国家建立中央与地方之间、部门之间、军地之间以及地区之间关于国家安全的协同联动机制。

第五十条 国家建立国家安全决策咨询机制，组织专家和有关方面开展对国家安全形势的分析研判，推进国家安全的科学决策。

第二节 情报信息

第五十一条 国家健全统一归口、反应灵敏、准确高效、运转顺畅的情报信息收集、研判和使用制度，建立情报信息工作协调机制，实现情报信息的及时收集、准确研判、有效使用和共享。

第五十二条 国家安全机关、公安机关、有关军事机关根据职责分工，依法搜集涉及国家安全的情报信息。

国家机关各部门在履行职责过程中，对于获取的涉及国家安全的有关信息应当及时上报。

第五十三条 开展情报信息工作，应当充分运用现代科学技术手段，加强对情报信息的鉴别、筛选、综合和研判分析。

第五十四条 情报信息的报送应当及时、准确、客观，不得迟报、漏报、瞒报和谎报。

第三节 风险预防、评估和预警

第五十五条 国家制定完善应对各领域国家安全风险预案。

第五十六条 国家建立国家安全风险评估机制，定期开展各领域国家安全风险调查评估。

有关部门应当定期向中央国家安全领导机构提交国家安全风险评估报告。

第五十七条 国家健全国家安全风险监测预警制度，根据国家安全风险程度，及时发布相应风险预警。

第五十八条 对可能即将发生或者已经发生的危害国家安全的事件，县级以上地方人民政府及其有关主管部门应当立即按照规定向上一级人民政府及其有关主管部门报告，必要时可以越级上报。

第四节 审查监管

第五十九条 国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

第六十条 中央国家机关各部门依照法律、行政法规行使国家安全审查职责，依法作出国家安全审查决定或者提出安全审查意见并监督执行。

第六十一条 省、自治区、直辖市依法负责本行政区域内有关国家安全审查和监管工作。

第五节 危机管控

第六十二条 国家建立统一领导、协同联动、有序高效的国家安全危机管控制度。

第六十三条 发生危及国家安全的重大事件，中央有关部门和有关地方根据中央国家安全领导机构的统一部署，依法启动应急预案，采取管控处置措施。

第六十四条 发生危及国家安全的特别重大事件，需要进入紧急状态、战争状态或者进行全国总动员、局部动员的，由全国人民代表大会、全国人民代表大会常务委员会或者国务院依照宪法和有关法律规定的权限和程序决定。

第六十五条 国家决定进入紧急状态、战争状态或者实施国防动员后，履行国家安全危机管控职责的有关机关依照法律规定或者全国人民代表大会常务委员会规定，有权采取限制公民和组织权利、增加公民和组织义务的特别措施。

第六十六条 履行国家安全危机管控职责的有关机关依法采取处置国家安全危机的管控措施，应当与国家安全危机可能造成的危害的性质、程度和范围相适应；有多种措施可供选择的，应当选择有利于最大程度保护公民、组织权益的措施。

第六十七条 国家健全国家安全危机的信息报告和发布机制。

国家安全危机事件发生后，履行国家安全危机管控职责的有关机关，应当按照规定准确、及时报告，并依法将有关国家安全危机事件发生、发展、管控处置及善后情况统一向社会发布。

第六十八条 国家安全威胁和危害得到控制或者消除后，应当及时解除管控处置措施，做好善后工作。

第五章 国家安全保障

第六十九条 国家健全国家安全保障体系，增强维护国家安全的能力。

第七十条 国家健全国家安全法律制度体系，推动国家安全法治建设。

第七十一条 国家加大对国家安全各项建设的投入，保障国家安全工作所需经费和装备。

第七十二条 承担国家安全战略物资储备任务的单位，应当按照国家有关规定和标准对国家安全物资进行收储、保管和维护，定期调整更换，保证储备物资的使用效能和安全。

第七十三条 鼓励国家安全领域科技创新，发挥科技在维护国家安全中的作用。

第七十四条 国家采取必要措施，招录、培养和管理国家安全工作专门人才和特殊人才。

根据维护国家安全工作的需要，国家依法保护有关机关专门从事国家安全工作人员的身份和合法权益，加大人身保护和安置保障力度。

第七十五条 国家安全机关、公安机关、有关军事机关开展国家安全专门工作，可以依法采取必要手段和方式，有关部门和地方应当在职责范围内提供支持和配合。

第七十六条 国家加强国家安全新闻宣传和舆论引导，通过多种形式开展国家安全宣传教育活动，将国家安全教育纳入国民教育体系和公务员教育培训体系，增强全民国家安全意识。

第六章 公民、组织的义务和权利

第七十七条 公民和组织应当履行下列维护国家安全的义务：

（一）遵守宪法、法律法规关于国家安全的有关规定；

（二）及时报告危害国家安全活动的线索；

（三）如实提供所知悉的涉及危害国家安全活动的证据；

（四）为国家安全工作提供便利条件或者其他协助；

（五）向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；

（六）保守所知悉的国家秘密；

（七）法律、行政法规规定的其他义务。

任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。

第七十八条 机关、人民团体、企业事业组织和其他社会组织应当对本单位的人员进行维护国家安全的教育，动员、组织本单位的人员防范、制止危害国家安全的行为。

第七十九条 企业事业组织根据国家安全工作的要求，应当配合有关部门采取相关安全措施。

第八十条 公民和组织支持、协助国家安全工作的行为受法律保护。

因支持、协助国家安全工作，本人或者其近亲属的人身安全面临危险的，可以向公安机关、国家安全机关请求予以保护。公安机关、国家安全机关应当会同有关部门依法采取保护措施。

第八十一条 公民和组织因支持、协助国家安全工作导致财产损失的，按照国家有关规定给予补偿；造成人身伤害或者死亡的，按照国家有关规定给予抚恤优待。

第八十二条 公民和组织对国家安全工作有向国家机关提出批评建议的权利，对国家机关及其工作人员在国家安全工作中的违法失职行为有提出申诉、控告和检举的权利。

第八十三条 在国家安全工作中，需要采取限制公民权利和自由的特别措施时，应当依法进行，并以维护国家安全的实际需要为限度。

第七章 附则

第八十四条 本法自公布之日起施行。

**中华人民共和国网络安全法**

（自2017年6月1日起施行）

来源：中国政府网

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；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。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，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。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自2017年6月1日起施行。

**中华人民共和国反间谍法**

（2014年11月1日第十二届全国人民代表大会常务委员会第十一次会议通过）

来源：中国政府网

第一章 总 则

第一条 为了防范、制止和惩治间谍行为，维护国家安全，根据宪法，制定本法。

第二条 反间谍工作坚持中央统一领导，坚持公开工作与秘密工作相结合、专门工作与群众路线相结合、积极防御、依法惩治的原则。

第三条 国家安全机关是反间谍工作的主管机关。

公安、保密行政管理等其他有关部门和军队有关部门按照职责分工，密切配合，加强协调，依法做好有关工作。

第四条 中华人民共和国公民有维护国家的安全、荣誉和利益的义务，不得有危害国家的安全、荣誉和利益的行为。

一切国家机关和武装力量、各政党和各社会团体及各企业事业组织，都有防范、制止间谍行为，维护国家安全的义务。

国家安全机关在反间谍工作中必须依靠人民的支持，动员、组织人民防范、制止危害国家安全的间谍行为。

第五条 反间谍工作应当依法进行，尊重和保障人权，保障公民和组织的合法权益。

第六条 境外机构、组织、个人实施或者指使、资助他人实施的，或者境内机构、组织、个人与境外机构、组织、个人相勾结实施的危害中华人民共和国国家安全的间谍行为，都必须受到法律追究。

第七条 国家对支持、协助反间谍工作的组织和个人给予保护，对有重大贡献的给予奖励。

第二章 国家安全机关在反间谍工作中的职权

第八条 国家安全机关在反间谍工作中依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。

第九条 国家安全机关的工作人员依法执行任务时，依照规定出示相应证件，有权查验中国公民或者境外人员的身份证明，向有关组织和人员调查、询问有关情况。

第十条 国家安全机关的工作人员依法执行任务时，依照规定出示相应证件，可以进入有关场所、单位；根据国家有关规定，经过批准，出示相应证件，可以进入限制进入的有关地区、场所、单位，查阅或者调取有关的档案、资料、物品。

第十一条 国家安全机关的工作人员在依法执行紧急任务的情况下，经出示相应证件，可以优先乘坐公共交通工具，遇交通阻碍时，优先通行。

国家安全机关因反间谍工作需要，按照国家有关规定，可以优先使用或者依法征用机关、团体、企业事业组织和个人的交通工具、通信工具、场地和建筑物，必要时，可以设置相关工作场所和设备、设施，任务完成后应当及时归还或者恢复原状，并依照规定支付相应费用；造成损失的，应当补偿。

第十二条 国家安全机关因侦察间谍行为的需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦察措施。

第十三条 国家安全机关因反间谍工作需要，可以依照规定查验有关组织和个人的电子通信工具、器材等设备、设施。查验中发现存在危害国家安全情形的，国家安全机关应当责令其整改；拒绝整改或者整改后仍不符合要求的，可以予以查封、扣押。

对依照前款规定查封、扣押的设备、设施，在危害国家安全的情形消除后，国家安全机关应当及时解除查封、扣押。

第十四条 国家安全机关因反间谍工作需要，根据国家有关规定，可以提请海关、边防等检查机关对有关人员和资料、器材免检。有关检查机关应当予以协助。

第十五条 国家安全机关对用于间谍行为的工具和其他财物，以及用于资助间谍行为的资金、场所、物资，经设区的市级以上国家安全机关负责人批准，可以依法查封、扣押、冻结。

第十六条 国家安全机关根据反间谍工作需要，可以会同有关部门制定反间谍技术防范标准，指导有关部门落实反间谍技术防范措施，对存在隐患的部门，经过严格的批准手续，可以进行反间谍技术防范检查和检测。

第十七条 国家安全机关及其工作人员在工作中，应当严格依法办事，不得超越职权、滥用职权，不得侵犯组织和个人的合法权益。

国家安全机关及其工作人员依法履行反间谍工作职责获取的组织和个人的信息、材料，只能用于反间谍工作。对属于国家秘密、商业秘密和个人隐私的，应当保密。

第十八条 国家安全机关工作人员依法执行职务受法律保护。

第三章 公民和组织的义务和权利

第十九条 机关、团体和其他组织应当对本单位的人员进行维护国家安全的教育，动员、组织本单位的人员防范、制止间谍行为。

第二十条 公民和组织应当为反间谍工作提供便利或者其他协助。

因协助反间谍工作，本人或者其近亲属的人身安全面临危险的，可以向国家安全机关请求予以保护。国家安全机关应当会同有关部门依法采取保护措施。

第二十一条 公民和组织发现间谍行为，应当及时向国家安全机关报告；向公安机关等其他国家机关、组织报告的，相关国家机关、组织应当立即移送国家安全机关处理。

第二十二条 在国家安全机关调查了解有关间谍行为的情况、收集有关证据时，有关组织和个人应当如实提供，不得拒绝。

第二十三条 任何公民和组织都应当保守所知悉的有关反间谍工作的国家秘密。

第二十四条 任何个人和组织都不得非法持有属于国家秘密的文件、资料和其他物品。

第二十五条 任何个人和组织都不得非法持有、使用间谍活动特殊需要的专用间谍器材。专用间谍器材由国务院国家安全主管部门依照国家有关规定确认。

第二十六条 任何个人和组织对国家安全机关及其工作人员超越职权、滥用职权和其他违法行为，都有权向上级国家安全机关或者有关部门检举、控告。受理检举、控告的国家安全机关或者有关部门应当及时查清事实，负责处理，并将处理结果及时告知检举人、控告人。

对协助国家安全机关工作或者依法检举、控告的个人和组织，任何个人和组织不得压制和打击报复。

第四章 法律责任

第二十七条 境外机构、组织、个人实施或者指使、资助他人实施，或者境内机构、组织、个人与境外机构、组织、个人相勾结实施间谍行为，构成犯罪的，依法追究刑事责任。

实施间谍行为，有自首或者立功表现的，可以从轻、减轻或者免除处罚；有重大立功表现的，给予奖励。

第二十八条 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。

第二十九条 明知他人有间谍犯罪行为，在国家安全机关向其调查有关情况、收集有关证据时，拒绝提供的，由其所在单位或者上级主管部门予以处分，或者由国家安全机关处十五日以下行政拘留；构成犯罪的，依法追究刑事责任。

第三十条 以暴力、威胁方法阻碍国家安全机关依法执行任务的，依法追究刑事责任。

故意阻碍国家安全机关依法执行任务，未使用暴力、威胁方法，造成严重后果的，依法追究刑事责任；情节较轻的，由国家安全机关处十五日以下行政拘留。

第三十一条 泄露有关反间谍工作的国家秘密的，由国家安全机关处十五日以下行政拘留；构成犯罪的，依法追究刑事责任。

第三十二条 对非法持有属于国家秘密的文件、资料和其他物品的，以及非法持有、使用专用间谍器材的，国家安全机关可以依法对其人身、物品、住处和其他有关的地方进行搜查；对其非法持有的属于国家秘密的文件、资料和其他物品，以及非法持有、使用的专用间谍器材予以没收。非法持有属于国家秘密的文件、资料和其他物品，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由国家安全机关予以警告或者处十五日以下行政拘留。

第三十三条 隐藏、转移、变卖、损毁国家安全机关依法查封、扣押、冻结的财物的，或者明知是间谍活动的涉案财物而窝藏、转移、收购、代为销售或者以其他方法掩饰、隐瞒的，由国家安全机关追回。构成犯罪的，依法追究刑事责任。

第三十四条 境外人员违反本法的，可以限期离境或者驱逐出境。

第三十五条 当事人对行政处罚决定、行政强制措施决定不服的，可以自接到决定书之日起六十日内，向作出决定的上一级机关申请复议；对复议决定不服的，可以自接到复议决定书之日起十五日内向人民法院提起诉讼。

第三十六条 国家安全机关对依照本法查封、扣押、冻结的财物，应当妥善保管，并按照下列情形分别处理：

（一）涉嫌犯罪的，依照刑事诉讼法的规定处理；

（二）尚不构成犯罪，有违法事实的，对依法应当没收的予以没收，依法应当销毁的予以销毁；

（三）没有违法事实的，或者与案件无关的，应当解除查封、扣押、冻结，并及时返还相关财物；造成损失的，应当依法赔偿。

国家安全机关没收的财物，一律上缴国库。

第三十七条 国家安全机关工作人员滥用职权、玩忽职守、徇私舞弊，构成犯罪的，或者有非法拘禁、刑讯逼供、暴力取证、违反规定泄露国家秘密、商业秘密和个人隐私等行为，构成犯罪的，依法追究刑事责任。

第五章 附 则

第三十八条 本法所称间谍行为，是指下列行为：

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

（二）参加间谍组织或者接受间谍组织及其代理人的任务的；

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

（四）为敌人指示攻击目标的；

（五）进行其他间谍活动的。

第三十九条 国家安全机关、公安机关依照法律、行政法规和国家有关规定，履行防范、制止和惩治间谍行为以外的其他危害国家安全行为的职责，适用本法的有关规定。

第四十条 本法自公布之日起施行。1993年2月22日第七届全国人民代表大会常务委员会第三十次会议通过的《中华人民共和国国家安全法》同时废止。

**中华人民共和国反间谍法实施细则**

来源：中国政府网

第一章　总则

第一条　根据《中华人民共和国反间谍法》（以下简称《反间谍法》），制定本实施细则。

第二条　国家安全机关负责本细则的实施。

公安、保密行政管理等其他有关部门和军队有关部门按照职责分工，密切配合，加强协调，依法做好有关工作。

第三条　《反间谍法》所称“境外机构、组织”包括境外机构、组织在中华人民共和国境内设立的分支（代表）机构和分支组织；所称“境外个人”包括居住在中华人民共和国境内不具有中华人民共和国国籍的人。

第四条　《反间谍法》所称“间谍组织代理人”，是指受间谍组织或者其成员的指使、委托、资助，进行或者授意、指使他人进行危害中华人民共和国国家安全活动的人。

间谍组织和间谍组织代理人由国务院国家安全主管部门确认。

第五条　《反间谍法》所称“敌对组织”，是指敌视中华人民共和国人民民主专政的政权和社会主义制度，危害国家安全的组织。

敌对组织由国务院国家安全主管部门或者国务院公安部门确认。

第六条　《反间谍法》所称“资助”实施危害中华人民共和国国家安全的间谍行为，是指境内外机构、组织、个人的下列行为：

（一）向实施间谍行为的组织、个人提供经费、场所和物资的；

（二）向组织、个人提供用于实施间谍行为的经费、场所和物资的。

第七条　《反间谍法》所称“勾结”实施危害中华人民共和国国家安全的间谍行为，是指境内外组织、个人的下列行为：

（一）与境外机构、组织、个人共同策划或者进行危害国家安全的间谍活动的；

（二）接受境外机构、组织、个人的资助或者指使，进行危害国家安全的间谍活动的；

（三）与境外机构、组织、个人建立联系，取得支持、帮助，进行危害国家安全的间谍活动的。

第八条　下列行为属于《反间谍法》第三十九条所称“间谍行为以外的其他危害国家安全行为”：

（一）组织、策划、实施分裂国家、破坏国家统一，颠覆国家政权、推翻社会主义制度的；

（二）组织、策划、实施危害国家安全的恐怖活动的；

（三）捏造、歪曲事实，发表、散布危害国家安全的文字或者信息，或者制作、传播、出版危害国家安全的音像制品或者其他出版物的；

（四）利用设立社会团体或者企业事业组织，进行危害国家安全活动的；

（五）利用宗教进行危害国家安全活动的；

（六）组织、利用邪教进行危害国家安全活动的；

（七）制造民族纠纷，煽动民族分裂，危害国家安全的；

（八）境外个人违反有关规定，不听劝阻，擅自会见境内有危害国家安全行为或者有危害国家安全行为重大嫌疑的人员的。

第二章　国家安全机关在反间谍工作中的职权

第九条　境外个人被认为入境后可能进行危害中华人民共和国国家安全活动的，国务院国家安全主管部门可以决定其在一定时期内不得入境。

第十条　对背叛祖国、危害国家安全的犯罪嫌疑人，依据《反间谍法》第八条的规定，国家安全机关可以通缉、追捕。

第十一条　国家安全机关依法执行反间谍工作任务时，有权向有关组织和人员调查询问有关情况。

第十二条　国家安全机关工作人员依法执行反间谍工作任务时，对发现身份不明、有危害国家安全行为的嫌疑人员，可以检查其随带物品。

第十三条　国家安全机关执行反间谍工作紧急任务的车辆，可以配置特别通行标志和警灯、警报器。

第十四条　国家安全机关工作人员依法执行反间谍工作任务的行为，不受其他组织和个人的非法干涉。

国家安全机关工作人员依法执行反间谍工作任务时，应当出示国家安全部侦察证或者其他相应证件。

国家安全机关及其工作人员在工作中，应当严格依法办事，不得超越职权、滥用职权，不得侵犯组织和个人的合法权益。

第三章　公民和组织维护国家安全的义务和权利

第十五条　机关、团体和其他组织对本单位的人员进行维护国家安全的教育，动员、组织本单位的人员防范、制止间谍行为的工作，应当接受国家安全机关的协调和指导。

机关、团体和其他组织不履行《反间谍法》和本细则规定的安全防范义务，未按照要求整改或者未达到整改要求的，国家安全机关可以约谈相关负责人，将约谈情况通报该单位上级主管部门，推动落实防范间谍行为和其他危害国家安全行为的责任。

第十六条　下列情形属于《反间谍法》第七条所称“重大贡献”：

（一）为国家安全机关提供重要线索，发现、破获严重危害国家安全的犯罪案件的；

（二）为国家安全机关提供重要情况，防范、制止严重危害国家安全的行为发生的；

（三）密切配合国家安全机关执行国家安全工作任务，表现突出的；

（四）为维护国家安全，与危害国家安全的犯罪分子进行斗争，表现突出的；

（五）在教育、动员、组织本单位的人员防范、制止危害国家安全行为的工作中，成绩显著的。

第十七条　《反间谍法》第二十四条所称“非法持有属于国家秘密的文件、资料和其他物品”是指：

（一）不应知悉某项国家秘密的人员携带、存放属于该项国家秘密的文件、资料和其他物品的；

（二）可以知悉某项国家秘密的人员，未经办理手续，私自携带、留存属于该项国家秘密的文件、资料和其他物品的。

第十八条　《反间谍法》第二十五条所称“专用间谍器材”，是指进行间谍活动特殊需要的下列器材：

（一）暗藏式窃听、窃照器材；

（二）突发式收发报机、一次性密码本、密写工具；

（三）用于获取情报的电子监听、截收器材；

（四）其他专用间谍器材。

专用间谍器材的确认，由国务院国家安全主管部门负责。

第四章　法律责任

第十九条　实施危害国家安全的行为，由有关部门依法予以处分，国家安全机关也可以予以警告；构成犯罪的，依法追究刑事责任。

第二十条　下列情形属于《反间谍法》第二十七条所称“立功表现”：

（一）揭发、检举危害国家安全的其他犯罪分子，情况属实的；

（二）提供重要线索、证据，使危害国家安全的行为得以发现和制止的；

（三）协助国家安全机关、司法机关捕获其他危害国家安全的犯罪分子的；

（四）对协助国家安全机关维护国家安全有重要作用的其他行为。

“重大立功表现”，是指在前款所列立功表现的范围内对国家安全工作有特别重要作用的。

第二十一条　有证据证明知道他人有间谍行为，或者经国家安全机关明确告知他人有危害国家安全的犯罪行为，在国家安全机关向其调查有关情况、收集有关证据时，拒绝提供的，依照《反间谍法》第二十九条的规定处理。

第二十二条　国家安全机关依法执行反间谍工作任务时，公民和组织依法有义务提供便利条件或者其他协助，拒不提供或者拒不协助，构成故意阻碍国家安全机关依法执行反间谍工作任务的，依照《反间谍法》第三十条的规定处罚。

第二十三条　故意阻碍国家安全机关依法执行反间谍工作任务，造成国家安全机关工作人员人身伤害或者财物损失的，应当依法承担赔偿责任，并由司法机关或者国家安全机关依照《反间谍法》第三十条的规定予以处罚。

第二十四条　对涉嫌间谍行为的人员，国家安全机关可以决定其在一定期限内不得出境。对违反《反间谍法》的境外个人，国务院国家安全主管部门可以决定限期离境或者驱逐出境，并决定其不得入境的期限。被驱逐出境的境外个人，自被驱逐出境之日起10年内不得入境。

第五章　附则

第二十五条　国家安全机关、公安机关依照法律、行政法规和国家有关规定，履行防范、制止和惩治间谍行为以外的其他危害国家安全行为的职责，适用本细则的有关规定。

第二十六条　本细则自公布之日起施行。1994年6月4日国务院发布的《中华人民共和国国家安全法实施细则》同时废止。

**《武器装备科研生产单位保密资格审查认证管理办法》**

来源：湖南省人民政府网站 2020年7月30日

第一章 总 则

第一条 为规范武器装备科研生产单位保密资格审查认证工作，确保国家秘密安全，依据《中华人民共和国保守国家秘密法》和有关保密规定，制定本办法。

第二条 本办法适用于承担涉密武器装备科研生产任务企事业单位的保密资格审查认证工作。

第三条 对承担涉密武器装备科研生产任务的企事业单位，实行保密资格审查认证制度。承担涉密武器装备科研生产任务，应当取得相应保密资格。

第四条 武器装备科研生产单位保密资格审查认证工作坚持严格标准、严格程序、突出重点、公平公正的原则。

第五条 武器装备科研生产单位保密资格分为一级、二级、三级三个等级。一级保密资格单位可以承担绝密级科研生产任务；二级保密资格单位可以承担机密级科研生产任务；三级保密资格单位可以承担秘密级科研生产任务。

第六条 经审查认证取得保密资格的单位，列入《武器装备科研生产单位保密资格名录》（以下简称《名录》）。军队系统装备部门的涉密武器装备科研生产合同项目，应当在列入《名录》的具有相应等级保密资格的单位中招标订货。 承包单位分包涉密合同项目，分包单位应当是列入《名录》的具有相应等级保密资格的单位。

第二章 审查认证机构

第七条 国家保密局会同国家国防科技工业局、总装备部等部门组成国防武器装备科研生产单位保密资格审查认证委员会（以下简称国家军工保密资格认证委），履行下列职责：

（一）制定审查认证工作的政策、规定；

（二）制定《武器装备科研生产单位保密资格标准》（以下简称《标准》）和《武器装备科研生产单位保密资格评分标准》（以下简称《评分标准》）；

（三）决定审查认证工作中的重大问题；

（四）组织保密资格审查和复查；

（五）审查、审批一级保密资格申请单位；

（六）发布保密资格单位名录，制发保密资格证书；

（七）变更、注销、撤销保密资格；

（八）受理有关单位提出的复议申请；

（九）建立保密资格审查认证人员库，聘任和管理保密资格审查认证人员；

（十）对审查认证工作进行监督管理。

第八条 省（区、市）保密工作部门、国防科技工业管理部门和有关部门，以及有关地市级保密工作部门组成省（区、市）武器装备科研生产单位保密资格审查认证委员会（以下简称省（区、市）军工保密资格认证委），履行下列职责：

（一）受国家军工保密资格认证委委托，审查部分一级保密资格申请单位；

（二）审查、审批本地区二级、三级保密资格申请单位；

（三）进行保密资格复查；

（四）审核保密资格证书变更和注销申请；

（五）聘用保密资格审查认证人员；

（六）对本地区审查认证工作进行监督管理。 第九条 省（区、市）军工保密资格认证委在国家军工保密资格认证委的领导下开展工作，其组成人员应当报国家军工保密资格认证委批准。

第十条 国家军工保密资格认证委下设办公室，由国家保密局、国家国防科技工业局、总装备部等有关部门人员组成，负责审查认证日常工作。 省（区、市）军工保密资格认证委下设办公室，由省（区、市）保密工作部门、国防科技工业管理部门和有关部门人员组成，负责本行政区域内审查认证日常工作。

第三章 保密资格申请

第十一条 申请保密资格的单位应当具备以下基本条件：

（一）中华人民共和国境内登记注册的企业法人或事业法人；

（二）承担或拟承担武器装备科研生产的项目或产品涉密；

（三）无外商（含港澳台）投资和雇用外籍人员，国家有特殊规定的除外；

（四）承担涉密武器装备科研生产任务的人员，应当具有中华人民共和国国籍，在中华人民共和国境内居住，与境外人员（含港澳台）无婚姻关系；

（五）有固定的科研生产和办公场所，并符合国家有关安全保密要求；

（六）1年内未发生泄密事件；

（七）无非法获取、持有国家秘密以及其他严重违法行为。

第十二条 申请保密资格的单位，应当填写《武器装备科研生产单位保密资格申请书》（以下简称《申请书》），并提供以下材料：

（一）《申请书》；

（二）工商营业执照正本、副本（复印件）；

（三）组织机构代码证书（复印件）；

（四）公司章程；

（五）上一个年度财务验资报告；

（六）科研生产场所产权证书或租赁合同（复印件）；

（七）合同甲方出具的研制项目或产品的密级证明，或者合同意向单位出具的合同意向证明及密级证明；

（八）国家军工保密资格认证委要求提供的其他材料。

第十三条 上市公司申请保密资格的，其承担武器装备科研生产任务的范围应当符合国家有关政策规定。

第十四条 高等学校申请保密资格的，应当结合科研项目管理建立保密管理体制；具备相对集中的涉密科研场所，与开放区域隔离。

第十五条 非公有制企业申请保密资格的，限定于申请二级、三级保密资格。

第十六条 企事业单位提出保密资格申请，应当经上级部门审核。没有上级部门的，应当经省级业务主管部门或所在地的地市级以上保密工作部门审核。申请保密资格的单位，向有关审核部门报送《申请书》和有关材料。

第十七条 审核部门负责下列内容的审核：

（一）《申请书》的填写是否符合本办法的有关规定，填写内容是否属实；

（二）申请单位是否符合本办法规定的申请条件；

（三）申请的保密资格等级是否适当。

第十八条 审核部门经审核认为具备申请条件的，在《申请书》中签署同意意见后，由申请单位向有关军工保密资格认证委提出申请；经审核认为不具备申请条件的，应在《申请书》中说明理由，退回申请单位。

第四章 审查批准

第十九条 保密资格审查分为书面审查和现场审查。 国家或省（区、市）军工保密资格认证委收到申请单位《申请书》及相关材料后，进行书面审查，并在10个工作日内作出是否受理的决定。省（区、市）军工保密资格认证委应当征求军队派驻的军事代表机构对申请单位是否符合申请条件的意见。对决定受理的单位，应当在30个工作日内组成审查组进行现场审查。

第二十条 审查组负责人由同级军工保密资格认证委指定，审查组工作人员应当从审查认证人员库中抽取，人数为5至8人。

第二十一条 现场审查依据相应等级的《标准》及《评分标准》实行评分制，满分为500分，达到450分（含）以上为符合标准。

第二十二条 审查组现场审查程序：

（一）提前7个工作日通知被审查单位；

（二）听取被审查单位情况汇报和对有关事项的说明；

（三）审查有关文字材料；

（四）接触有关人员了解情况；

（五）组织涉密人员进行保密知识考试；

（六）进行现场审查，并作出审查记录；

（七）对现场检查情况进行评议，研究或表决形成审查意见和评分结果。审查意见和评分结果填写在《武器装备科研生产单位保密资格审查（复查）意见书》（以下简称《审查（复查）意见书》）中，并由审查组组长在签名栏内签名；

（八）向被审查单位通报审查意见和评分结果，对存在问题提出整改要求；

（九）被审查单位在《审查（复查）意见书》签名栏内对审查结论签署意见。

第二十三条 审查中发现被审查单位重要事项达不到《标准》或严重违反保密规定，存在重大泄密隐患的，应当中止审查，要求其采取整改措施。对中止审查的单位，3个月后视整改情况决定是否恢复审查。

第二十四条 对不符合《标准》未予通过审查的单位，6个月后方可重新申请。

第二十五条 国家或省（区、市）军工保密资格认证委应当根据审查结论和有关材料，在60个工作日内作出是否批准的决定。

第二十六条 省（区、市）军工保密资格认证委应当将审查批准的保密资格申请单位有关材料，报国家军工保密资格认证委复核备案。

第二十七条 保密资格有效期为5年。有效期满，需继续承担涉密武器装备科研生产任务的，应当提前90个工作日重新提出申请。

第五章 监督管理

第二十八条 国家和省（区、市）军工保密资格认证委应当加强对审查认证工作的监督管理，建立健全监督机制，及时纠正工作中的违规行为。

第二十九条 取得保密资格的单位应当实行年度自检制度，每年1月底前，向审查认证机构报送《标准》执行情况自检报告。

第三十条 对取得保密资格满2年的单位应当进行复查。对重要事项达不到《标准》或严重违反保密规定，存在重大泄密隐患的，应当中止复查，给予警告，并要求其限期采取整改措施。对中止复查的单位，3个月后再行复查，对未达到整改要求的，撤销其保密资格。

第三十一条 取得保密资格的单位，具有下列情形之一的，应当申请变更证书：

（一）法定代表人变更的；

（二）单位名称变更的；

（三）注册地址变更的。 申请变更的单位，应当报原批准机关审核同意后，由国家军工保密资格认证委办理变更手续。

第三十二条 取得保密资格的单位，具有下列情形之一的，应当重新申请：

（一）需要提高保密资格等级的；

（二）资本构成、企业性质发生重大变化的；

（三）涉密场所发生重大变化的。

第三十三条 取得保密资格的单位，具有下列情形之一的，应当注销保密资格：

（一）保密资格有效期满的；

（二）不再承担涉密武器装备科研生产任务的；

（三）单位申请注销的；

（四）单位撤销的。

第三十四条 申请或取得保密资格的单位对有关审查认证决定有异议的，可在60个工作日内向国家军工保密资格认证委提出复议申请。国家军工保密资格认证委应当自受理申请之日起60个工作日内作出最终决定。

第六章 法律责任

第三十五条 违反本办法，选择不具有保密资格的单位分包涉密武器装备科研生产任务的，撤销其保密资格。构成犯罪的，依法追究刑事责任。

第三十六条 申请单位在申报过程中，隐瞒重要情况或提供虚假材料的，1年内不予受理申请。

第三十七条 取得保密资格的单位，有下列情形之一的，撤销保密资格：

（一）以欺骗、贿赂等不正当手段取得保密资格的；

（二）擅自引入外商投资或雇用外籍人员的；

（三）出租、转让、转借保密资格证书的；

（四）存在重大泄密隐患，经警告逾期不改的；

（五）严重违反保密规定，发生重大泄密事件的；

（六）有非法获取、持有国家秘密行为以及其他严重违法行为的。被撤销保密资格的，自被撤销之日起1年内不得再次申请。

第三十八条 审查认证人员违反本办法，利用职权谋取私利，徇私舞弊、玩忽职守的，撤销其审查认证资格，由有关部门给予行政处分。

第七章 附 则

第三十九条 保密资格审查认证人员从保密工作部门、国防科技工业管理部门和有关单位人员中聘任。

第四十条 依照本办法实施武器装备科研生产单位保密资格审查认证，不得以任何方式收取任何费用。

第四十一条 本办法由国家保密局负责解释。

第四十二条 本办法自2009年1月1日起施行。

## **树牢总体国家安全观**

**——写在全民国家安全教育日**

来源：《人民日报》 2022年4月15日   02版

在高校，“新时代国家安全成就主题展”吸引师生驻足观看，广大师生加深了对总体国家安全观的理解；在基层，国家安全教育宣传活动走进乡村、社区，人民群众提高了维护国家安全的自觉……今天是全民国家安全教育日，今年活动主题是“树牢总体国家安全观，感悟新时代国家安全成就，为迎接党的二十大胜利召开营造良好氛围”，连日来各地各单位举办形式多样的国家安全宣传教育活动。深入浅出的讲解，引人入胜的海报，鲜活生动的互动，让大安全理念深入人心，让大安全格局凝聚起广泛社会共识。

国家安全工作是党治国理政一项十分重要的工作，也是保障国泰民安一项十分重要的工作。党的十八大以来，以习近平同志为核心的党中央坚持总体国家安全观，把国家安全贯穿到党和国家工作各方面全过程，着力构建大安全格局。在制度设计上，设立中央国家安全委员会，完善国家安全法治体系、战略体系和政策体系；在经济社会发展中，实现高质量发展和高水平安全的良性互动，注重防范化解影响我国现代化进程的重大风险；在应对外部冲击挑战上，严密防范和严厉打击敌对势力渗透、破坏、颠覆、分裂活动，顶住和反击外部极端打压遏制……一系列重大决策部署，推动新时代国家安全工作发生历史性变革、取得历史性成就，国家安全得到全面加强，经受住了来自政治、经济、意识形态、自然界等方面的风险挑战考验，为党和国家兴旺发达、长治久安提供了有力保证。

习近平总书记以统揽全局的战略思维和宽广的世界眼光深刻把握国家安全问题，坚持底线思维、居安思危、未雨绸缪，坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、科技、文化、社会安全为保障，以促进国际安全为依托，统筹发展和安全，统筹开放和安全，统筹传统安全和非传统安全，统筹自身安全和共同安全，统筹维护国家安全和塑造国家安全，提出了总体国家安全观。总体国家安全观涵盖政治、军事、国土、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、深海、极地、生物等诸多领域，集中体现了习近平总书记对国家安全形势的深刻洞察，深化和拓展了我们党关于国家安全问题的理论视野和实践领域，为新时代做好国家安全工作指明了前进方向、提供了根本遵循。

当前，国际形势继续发生深刻复杂变化，百年变局和世纪疫情相互交织，经济全球化遭遇逆流，大国博弈日趋激烈，世界进入新的动荡变革期，国内改革发展稳定任务艰巨繁重。我们面临的风险既包括国内的经济、政治、意识形态、社会风险以及来自自然界的风险，也包括国际经济、政治、军事风险等。我国发展所处的历史方位、国家安全所面临的形势任务，决定了国家安全在党和国家工作大局中的重要地位。新的伟大征程上，要贯彻总体国家安全观，坚持中国特色国家安全道路，构建大安全格局，把安全发展贯穿国家发展各领域和全过程，防范和化解影响我国现代化进程的各种风险，为建设社会主义现代化国家提供坚强保障。维护国家安全，人人有责、人人可为，要坚持国家安全一切为了人民、一切依靠人民，动员全党全社会共同努力，汇聚起维护国家安全的强大力量，夯实国家安全的社会基础，不断提高人民群众的安全感、幸福感。

国家安全是安邦定国的重要基石，维护国家安全是全国各族人民根本利益所在。奋斗新征程、建功新时代，贯彻总体国家安全观，下好先手棋、打好主动仗，不断塑造总体有利的国家安全战略态势，我们就一定能牢牢掌握维护国家安全的战略主动权，“中国号”巨轮就一定能越过激流险滩，驶向更加光明的未来。

**深刻认识中国特色国家安全道路**

来源：《人民日报》 2022年4月15日 09版

在以习近平同志为核心的党中央坚强领导下，我们走出一条中国特色国家安全道路，开创了维护国家安全的崭新局面。这条道路以总体国家安全观为统领，契合新的时代条件下维护国家安全的紧迫要求，彰显鲜明中国特色，为实现国家长治久安和人民安居乐业、实现中华民族伟大复兴提供了坚强安全保障。

习近平总书记强调：“保证国家安全是头等大事”。国家安全是安邦定国的重要基石，是人民安居乐业的保证，维护国家安全是全国各族人民根本利益所在。党的十八大以来，以习近平同志为核心的党中央准确把握国家安全形势变化新特点新趋势，创造性地提出坚持总体国家安全观，走出一条中国特色国家安全道路。中国特色国家安全道路，本质上是中国特色社会主义道路在国家安全领域的具体体现。总体国家安全观为走中国特色国家安全道路提供科学理论指导。走中国特色国家安全道路，努力开创国家安全工作新局面，是对总体国家安全观的贯彻落实。新时代，我国国家安全全面加强，国家安全工作取得历史性成就、发生历史性变革，彰显了总体国家安全观的科学价值和实践伟力，中国特色国家安全道路越走越宽广。

以总体国家安全观为统领

当前，我国国家安全内涵和外延比历史上任何时候都要丰富，时空领域比历史上任何时候都要宽广，内外因素比历史上任何时候都要复杂。党的十八大以来，以习近平同志为核心的党中央坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、科技、文化、社会安全为保障，以促进国际安全为依托，走出一条中国特色国家安全道路。

总体国家安全观深化和拓展了我们党关于国家安全问题的理论视野和实践领域，为新时代做好国家安全工作提供了根本遵循、指明了前进方向。党的十九大将坚持总体国家安全观作为新时代坚持和发展中国特色社会主义基本方略的重要内容并写入党章。党的十九届五中全会把统筹发展和安全纳入“十四五”时期我国经济社会发展的指导思想，“十四五”规划和2035年远景目标纲要对此列专章作出战略部署。2020年12月11日，习近平总书记在主持中央政治局第二十六次集体学习时发表重要讲话，就贯彻总体国家安全观提出“十个坚持”的要求，使总体国家安全观内容更加全面、逻辑更加严密。党的十九届六中全会通过的《中共中央关于党的百年奋斗重大成就和历史经验的决议》提出，必须坚持底线思维、居安思危、未雨绸缪，坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、科技、文化、社会安全为保障，以促进国际安全为依托，统筹发展和安全，统筹开放和安全，统筹传统安全和非传统安全，统筹自身安全和共同安全，统筹维护国家安全和塑造国家安全。这一重要论述进一步从党的百年奋斗历程把握总体国家安全观，凝结着我们党探索国家安全工作规律的实践经验。

坚持以总体国家安全观为统领，坚定不移走中国特色国家安全道路，就既能实现新时代国家安全全面加强，又能维护好重点领域国家安全。在以习近平同志为核心的党中央坚强领导下，我们坚持总体国家安全观，抓住和用好我国发展的重要战略机遇期，把国家安全贯穿到党和国家工作各方面全过程，同经济社会发展一起谋划、一起部署，为全面建设社会主义现代化国家提供了坚强安全保障。

彰显鲜明中国特色

不同国家的自然条件、历史文化、社会制度等不同，所面临的国家安全形势不同，国家安全道路也必然有所不同。当前，我国正处于实现中华民族伟大复兴的关键时期，世界百年未有之大变局加速演进，改革发展稳定任务艰巨繁重。面对复杂严峻的形势和前所未有的风险挑战，以习近平同志为核心的党中央站在党和国家事业发展全局的高度，以统揽全局的战略思维和宽广的世界眼光深刻把握国家安全问题，以强烈的忧患意识和责任担当谋划国家安全工作，大力推进国家安全领域理论创新、实践创新、制度创新，走出中国特色国家安全道路。这条道路契合新的时代条件下维护国家安全的紧迫要求，彰显鲜明中国特色。

坚持党对国家安全工作的绝对领导。党的十八大以来，以习近平同志为核心的党中央科学研判时与势，辩证把握危与机，打赢了一场又一场硬仗，化解了一个又一个风险，有力捍卫了国家主权、安全、发展利益，维护了政治安全、社会安定、人民安宁。实践充分证明，办好中国的事情关键在党，党的绝对领导是做好国家安全工作的根本原则，是维护国家安全和社会安定的根本保证。在全面建设社会主义现代化国家、实现中华民族伟大复兴的历史进程中，我们必须坚持党的领导，完善集中统一、高效权威的国家安全领导体制，充分发挥党总揽全局、协调各方的领导核心作用，团结带领人民形成万众一心维护国家安全的磅礴伟力。

坚持人民安全、政治安全、国家利益至上有机统一。在我国，国家利益与人民安全、政治安全具有内在一致性。国家安全以人民安全为宗旨，以政治安全为根本，以国家利益至上为准则，实现人民安居乐业、党的长期执政、国家长治久安。我们党始终把为中国人民谋幸福、为中华民族谋复兴作为初心和使命，以人民安全为宗旨，把保持社会平安稳定作为治国理政的重大任务。政治安全涉及国家主权、政权、制度和意识形态的稳固，是一个国家最根本的需求，是一切国家生存和发展的基础条件。一个国家对外不能独立自主，内部政治动荡，就不可能维护自身利益，就不可能实现长远发展。政治安全的核心是政权安全和制度安全。我国是中国共产党领导的社会主义国家，维护政治安全最根本的就是维护中国共产党的领导和执政地位、维护中国特色社会主义制度。维护政治安全是全国各族人民根本利益所在，只有坚定不移地维护政治安全，才能更好地保障国家利益。

统筹发展和安全两件大事。习近平总书记指出：“安全是发展的前提，发展是安全的保障，安全和发展要同步推进。”统筹发展和安全，是对新中国成立70多年来推进社会主义现代化建设经验的深刻总结。没有发展，安全就没有保障；没有安全，发展就不可持续，已经取得的成果也会失去。中国特色国家安全道路坚持统筹发展和安全两件大事，既善于运用发展成果夯实国家安全的实力基础，又善于塑造有利于经济社会发展的安全环境，做到坚持发展不停步、维护安全不懈怠，实现高质量发展和高水平安全良性互动。

树立共同、综合、合作、可持续的全球安全观，坚持走和平发展道路。当今世界安全形势的新特点新趋势决定了全球性挑战需要各国通力合作来应对。习近平总书记指出：“安全问题确实是事关人类前途命运的重大问题，如果解决不好，人类和平与发展的崇高事业就难以顺利推进。”要有效应对人类面临的困难和挑战，合作是我们唯一的选择，必须坚持合作共建，实现持久安全。中国坚持走和平发展道路，只有坚持和平发展的理念，才能有基础牢固、真正持久的安全。中国主张任何国家都不能也不应脱离世界安全、以他国安全为代价而实现自身安全，始终做维护世界和平的坚定力量。

坚定不移走中国特色国家安全道路

方向决定前途，道路决定命运。我们要坚持总体国家安全观，坚定不移走中国特色国家安全道路，不断塑造总体有利的国家安全战略态势，把维护国家安全的战略主动权牢牢掌握在自己手中，为实现第二个百年奋斗目标提供坚强安全保障。

不断增强走中国特色国家安全道路的自觉性坚定性。随着中国日益走近世界舞台中央，国际影响力、感召力、塑造力显著提升，我们前所未有地接近实现中华民族伟大复兴的目标。与此同时，我国也面临更为复杂严峻的国家安全形势，各种风险挑战不断显现，既有国内的也有国际的，既有政治、经济、文化、社会等领域的也有来自自然界的，既有传统的也有非传统的，而且这些风险挑战呈现出交织性、复杂性、综合性等特点。我们必须坚定不移走中国特色国家安全道路，顺应时代呼唤，回应人民需要，破解发展面临的各种难题，化解来自各方面的风险挑战。

全面提高国家安全工作能力和水平。我们党在内忧外患中诞生，在磨难挫折中成长，在攻坚克难中壮大，对国家安全的重要性有着深刻的认识，历来把维护国家安全和社会安定作为党和国家的一项基础性工作。中国特色国家安全道路着眼党和国家工作大局，统筹发展和安全，既通过发展提升国家安全实力，又深入推进国家安全思路、体制、手段创新，营造有利于经济社会发展的安全环境。新时代，我们要在发展中更多考虑安全因素，努力实现发展和安全的动态平衡，全面提高国家安全工作能力和水平。根据国家安全规律特点，统筹传统安全和非传统安全，推进国家安全体系和能力现代化，统筹应对各领域安全风险挑战。

努力为解决人类面临的安全问题贡献中国智慧和中国方案。坚定不移走中国特色国家安全道路，要把握世界发展大势，立足我国发展重要战略机遇期大背景来谋划，保持战略定力、战略自信、战略耐心，把战略主动权牢牢掌握在自己手中。同时充分发挥负责任大国作用，不走国强必霸之路，而是坚定不移走和平发展道路，促进自身安全和共同安全相协调。我们要坚定不移走中国特色国家安全道路，为解决人类面临的安全问题贡献中国智慧和中国方案，助力维护国际秩序、完善全球治理，促进世界和平发展。

**数据安全法有哪些重点**

来源：《保密工作》 2021年第9期

9月1日，《中华人民共和国数据安全法》正式实施。数据安全法的出台是对当前数据安全内外部形势的积极回应，是护航数字经济发展的重要举措，开创了新时代数据安全治理的新局面。当下，面对大数据的洪流，数据安全问题如何应对，国家数据安全制度怎样布局，不仅关涉国家安全、公共安全、个人安全，也关系我国在全球新一轮信息技术变革中如何实现从跟跑、并跑到领跑的转变。

随着人类社会进入数字化时代，网络空间、物理世界和人类社会开始实现深度融合。数据不仅是网络空间自身运行的产物，也是物理世界、人类社会运行的数字画像，蕴含着数字化世界的运行规律。在数字化时代，数据同时兼具国家安全、数字经济、社会治理、个人隐私等多个属性，因此，发达国家陆续开展相关立法工作，我国数据安全立法可谓恰逢其时。

2021年6月10日，经全国人民代表大会常务委员会审议，通过了《中华人民共和国数据安全法》（简称数据安全法），并于9月1日起施行。数据安全法作为国家安全法律体系的一部分，既要解决现有数据安全制度供给不足的问题，又要符合总体国家安全观的整体性要求，避免过度介入应由其他法律规制的领域。因此，数据安全法是一部数据安全领域基础性、框架性的法律，为后续各类数据领域配套制度、规范及标准的制定提供了依据。

主要内容

数据安全法以总体国家安全观为指导，坚持统筹发展与安全的原则，明确了一系列数据安全制度，规定了数据处理主体的数据安全义务，并就政务数据安全与开放提出了相关要求，此外还明确了主管部门的职责及违规的法律责任。

1.数据安全与发展。当前，数据已经成为我国数字经济的核心生产要素之一，其有效利用事关社会和经济发展，同时又从微观到宏观层面影响国家安全。因此，数据安全法首先阐明了数据安全与发展的关系，强调“国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展”。同时，数据安全法还明确了同步促进数据开发利用、数据安全的技术研究与应用、标准化以及教育培训的措施，要求鼓励数据安全检测评估、认证等服务的发展，支持有关专业机构依法开展服务活动；建立健全了数据交易管理制度，要求规范数据交易行为，培育数据交易市场。

2.数据安全制度。数据安全法明确了6项数据安全制度：（1）数据分类分级与核心数据保护制度。确立了依据对国家安全、公共利益或者个人、组织合法权益造成的危害程度进行分类分级的原则，要求国家网信部门协调编制重要数据目录，各地区、各部门负责地方、领域的目录编制和数据保护，特别强调对于关系国家安全、国民经济命脉、重要民生、重大公共利益等国家核心数据，实行更加严格的管理制度。（2）数据安全风险评估与工作协调机制。规定国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制，建立工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。（3）数据安全应急处置机制。要求对于发生数据安全事件的，主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患。（4）数据安全审查制度。要求对影响或者可能影响国家安全的数据处理活动进行国家安全审查。（5）数据出口管制制度。要求对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。（6）歧视反制制度。规定对我国采取相关歧视性的禁止、限制或者其他类似措施的国家和地区，我国可以对其采取对等措施。

3.数据安全义务。数据安全法规定了4类数据安全义务：（1）数据处理者的安全义务。重要数据处理者应明确数据安全负责人和管理机构，定期开展风险评估，并向主管部门报送风险评估报告；关键信息基础设施的运营者在国内运营中收集和产生的重要数据的出境安全管理依据网络安全法执行，其他数据处理者的数据出境管理由网信办另行制定政策；组织、个人应合法、依规收集和使用数据等。（2）数据交易中介服务机构义务。数据交易中介服务机构应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。（3）有关组织、个人的数据支持义务。公安或国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。（4）跨境司法或执法机构数据提供审批义务。未经主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于境内的数据。

4.政务数据安全与开放。数据安全法就政务数据安全与开放作出相应规定。（1）政务数据安全要求。一方面，国家机关应当依法合规收集、使用数据，并对履职中知悉的个人隐私、个人信息、商业秘密等数据予以保密。另一方面，国家机关需要建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。（2）外包政务系统数据安全要求。国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，同时国家机关应当监督受托方履行相应的数据安全保护义务。（3）政务数据开放要求。除依法不予公开的数据外，国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据，同时应制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

5.法律责任。对于数据处理者与数据交易中介服务机构不履行数据安全义务、数据安全监管履职国家工作人员滥权舞弊、违法获取或滥用数据等行为，数据安全法也作出了相应的处罚规定。其中，对于不履行数据安全义务的数据处理者除罚款外可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，而对于违反国家核心数据管理制度且构成犯罪的可以追究刑事责任，对于违规数据出境或未经授权向外国司法或者执法机构提供数据的，同样会处以相应处罚。

需要关注的重点

1.基础性与可实施性的关系。数据安全法是我国数据安全领域的一部基础性法律，系统地搭建了一系列的制度框架，但目前在数据分类分级与重要数据保护、数据安全风险评估与工作协调、数据安全应急处置、数据安全审查、数据出口管制、歧视反制等方面的制度建设都尚处于初级阶段，在执行层面还需要制定大量的配套法规、制度、标准，以保障法律的细化实施。

2.主权性与全球化的关系。数据安全法涉及的数据绝大部分处于高度全球化的网络空间，各大互联网巨头的数据处理都是全球化的，而数据本身无论作为数字经济的要素还是国家安全的重要资源都具有强烈的主权属性。我国必将成为全球最大的数据生产与消费国，因此必须具备域外执法能力，同时也要有效限制境外的长臂管辖，这也是应对全球数据竞争的需要。数据安全法赋予了我国司法机构域外管辖权，同时还加强了对向境外司法或执法机构提供数据的监管，以封堵境外机构的长臂管辖。在未来执法实践过程中，我国与美欧等发达国家在数据管辖权争夺上必然是长期激烈博弈。

3.战略打压与反制的关系。与数据安全法同时颁布的反外国制裁法明确规定，外国以各种借口或者依据其本国法律对我国进行遏制、打压，对我国公民、组织采取歧视性限制措施，干涉我国内政的，我国有权采取相应反制措施。同时数据安全法明确规定，任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中国采取歧视性的禁止、限制措施的，中国可以对该国家或者地区采取对等措施。这表明我国既坚持数据自由流动，又对他国不正当的歧视行为作出了有力的回应。

4.信息基础设施依赖与数据安全的关系。随着云计算、大数据的快速普及，个人、企业、政务等各类系统开始日益依赖信息基础设施，然而这些信息基础设施大多由国内外大型信息技术企业运营维护的。部署于这些信息基础设施之上的系统及其数据控制权实际为这些大型企业所拥有。数据安全法规定，拥有国家机关数据控制权的企业必须履行数据保护义务。然而，目前对这些拥有国家机关数据控制权的企业很难进行有效监督，也很难有效追究其数据泄露责任。因此，国家还需要进一步明确信息基础设施运营者的数据安全责任，同时针对信息基础设施运营者建立行之有效的数据安全监管机制，以切实保障数据安全。

对保密工作的启示

首先，可借鉴数据安全法统筹发展和安全的理念，在涉密的政务、军工、科研等领域，引进和研发新型数据处理基础设施，推动数据的高效利用与开发，同时构建新型安全保密技术体系，保障重要数据的安全保密。

其次，鉴于当前在线数据处理全面采用云计算或大数据等信息基础设施，传统基于网络和终端的监管能力已力不从心，建议系统性构建面向新型信息基础设施的数据安全保密监管体系，提升对网络空间的安全保密监管能力。

最后，随着“一带一路”倡议的推进，以及我国各个领域的全球影响力提升，我国涉密数据处理也必然要实现全球化布局，在这样的格局下，域外数据处理的保密管理也需要从法律、法规到技术体系的有力支撑。

**机关单位内部信息外泄案件观察**

来源：《保密工作》 2019年第5期

**典型案例**

案例1：2018年12月，某市发改局事业单位工作人员程某，在办公期间擅自将机关协同办公系统中有关会议纪要的内容通过手机拍摄的方式发送到“业务通联”微信群中，群内成员闫某、张某、杨某分别将手机照片转发至同事、同学微信群内，短时间内在该市范围内大幅扩散，对相关工作的正常开展造成一定干扰。事件发生后，纪检部门、市发改局对程某诫勉谈话，责令作出书面检查，并在全市范围通报，闫某、张某、杨某所属单位也分别对三人进行提醒谈话。

案例2：2017年11月，某镇信访办副主任林某，从县政府办公室领取该县《维稳专班人员名录及工作分解表》（该文件首页标注“内部，注意保存”等字样），返回单位后将该文件放置于本人办公桌，恰逢有大量人员集中来访，遂与其他同事一起在大厅维持信访秩序。期间，信访人员唐某窜入林某办公室并发现桌上的文件，便使用手机拍摄了文件的全部内容，并立即发布于信访人员微信群。经过多次转发，文件照片迅速在微信群和QQ群中大范围传播，导致在全县范围内造成了不良影响，严重干扰了地区信访维稳工作。事件发生后，县委、县政府责令镇党委、镇政府作出深刻检查，镇政府给予林某行政警告处分。

以智能手机为代表的各种新型智能通信设备和以微信为代表的各种社交软件平台，为机关单位内部信息的泄露、扩散提供了极大的便利条件，信息化迅猛发展的时代背景进一步拓展了各种外泄渠道，给机关单位内部信息的保护提出新的课题。

案例3：2015年10月，保密检查发现，某国有企业集团公司干部左某使用的非涉密计算机中存储4份标密文件。经鉴定，4份文件均不属于国家秘密，但属于不应公开的内部资料。事件发生后，有关部门给予左某行政降级处分，扣除其半年绩效奖励，调离项目组且3年内不得从事涉密工作，同时给予其党内警告处分。负有监管责任的集团公司保密办主任葛某等4人向集团公司保密委作出深刻检查，并给予通报批评。

案例4：2016年2月，某研究院所属产业规划研究所互联网产业研究部主任刘某，违反研究院保密及科研管理相关制度和要求，将该院承担某中央国家机关规划编制过程文件发送无关人员，经评估确认未造成实际外泄后果。此外，核查中发现，刘某名下的笔记本电脑和移动硬盘中存有10余份涉及内部会议的记录，具有一定敏感性。事件发生后，有关部门给予刘某全院通报批评，责令作出深刻检查，取消评优资格等处理。

以上两起都是机关单位工作人员因违规存储、处理内部信息而被追责的典型案例，共同特征是违反了机关单位有关内部信息的管理制度，对机关单位的正常工作秩序造成干扰或影响。

案例5：2013年12月,某县农牧局决定将近年来中央、农业部以及省、市农牧部门涉及业务工作的有关文件及领导讲话汇编成册，供干部职工学习。办公室按照要求编印了《农牧工作学习资料汇编（2013年）》(以下简称《汇编》)，发至机关全体干部学习参考。为进一步扩大宣贯范围，宣传科责任人陆某从办公室要来《汇编》的电子版，上传到该县政务公开网站。2014年4月，业务部门反映该《汇编》内含两份标注“内部文件”的材料，不宜置于互联网站对外公开，该县农牧局当即从网站撤下《汇编》。事件发生后，有关部门给予直接责任人陆某通报批评，责成本人作出深刻检查，并取消当年的评优评先资格。

这是一起在汇编文件资料过程中外泄机关单位内部信息的案件，涉案机关在互联网发布信息之前，没有正常履行政府信息公开保密审查义务，导致公布的《汇编》中夹杂了不应公开的内部文件。

**加强对机关单位内部信息的保护**

机关单位内部信息是机关单位在职务、业务活动和内部管理中产生的，限于机关单位相关工作人员内部掌握的信息。内部信息与国家秘密存在着一些相似之处，如内部信息与国家秘密都是由机关单位产生的，都具有秘密的一般属性，也就是说两者具有类似的时空要素，即在一定时间内只限于一定范围的人员知悉、掌握。国家秘密与机关单位内部信息的区别也是非常明显的：一是实质要素不同。前者关系国家安全和利益，后者在于机关单位的内部管理和工作秩序。二是确定方式不同。前者严格依照法定程序，包括明确的定密依据、权限、方法和步骤来进行定密，后者主要由机关单位自行确定。三是标识不同。前者必须使用法定的文字与符号标识，标记于相应载体、设备或产品之上，后者没有统一的标识要求，“内部”“内部文件”“内部资料”等多种标识不一而足。四是管理体制不同。前者由国家法律法规以及党内法规进行系统规范，后者没有统一的制度规范，现阶段由各地方、部门或机关单位自行确定。五是法律责任不同。情节或后果严重的泄露国家秘密行为，可能会被追究刑事责任，而泄露机关单位内部信息的行为，法律责任形式主要还是行政责任。

当前的主要问题是尚未有全国统一、系统的内部信息管理制度规范，少数机关单位基于本地方、本系统的职责要求和业务需要的考虑，自行研究确定了内部信息管理体制、方法和措施，但大部分机关单位还没有这方面的专门规定，实际工作中对内部信息的保护和管理还存在空白地带和薄弱环节，导致机关单位内部信息外泄事件时有发生，给相关工作造成一定的损失和延误。特别要注意的是，境外情报机构高度关注我特定、重要机关单位产生的内部信息，将其作为重要的情报来源进行多方窃取、全面搜集，现行刑法也设定了为境外窃取、刺探、收买、非法提供国家秘密、情报罪，将关系国家安全和利益、尚未公开或者依照有关规定不应公开的事项明确为情报加以保护。

有鉴于此，机关单位要把加大内部信息的管理和保护提升到牢固树立总体国家安全观意识的高度，在全面强化、规范信息安全管理的整体框架下，将机关单位内部信息纳入以国家秘密为主体的信息安全保密整体工作中统筹考虑、集中部署、分类监管，杜绝各种内部信息外泄事件的发生。