

# 成人继续教育学院

# 教职工政治学习

# 资料汇编

教师工作部 编发

2020 年第一期（4 月）

---

## 全民国家安全教育日专辑

### 目 录

1. 习近平谈总体国家安全：把生物安全纳入国家安全体系 ..... 2
2. 习近平：《为打赢疫情防控阻击战提供强大科技支撑》※ ... 9
3. 中华人民共和国国家安全法 ..... 15
4. 中华人民共和国反间谍法 ..... 26
5. 中华人民共和国反恐怖主义法 ..... 32
6. 中华人民共和国网络安全法 ..... 54
7. 中华人民共和国保密法 ..... 69
8. 中华人民共和国保守国家秘密法实施条例 ..... 78

# 习近平谈总体国家安全：把生物安全纳入国家安全体系

## 坚持总体国家安全观

### 1、要坚持党对国家安全工作的绝对领导

要坚持党对国家安全工作的绝对领导，实施更为有力的统领和协调。中央国家安全委员会要发挥好统筹国家安全事务的作用，抓好国家安全方针政策贯彻落实，完善国家安全工作机制，着力在提高把握全局、谋划发展的战略能力上下功夫，不断增强驾驭风险、迎接挑战的本领。

——2018年4月17日，习近平在十九届中央国家安全委员会第一次会议上发表重要讲话

### 2、人民安全是国家安全的宗旨，政治安全是国家安全的根本

坚持人民安全、政治安全、国家利益至上的有机统一，人民安全是国家安全的宗旨，政治安全是国家安全的根本，国家利益至上是国家安全的准则，实现人民安居乐业、党的长期执政、国家长治久安……

——2018年4月17日，习近平在十九届中央国家安全委员会第一次会议上发表重要讲话

### 3、国家安全是安邦定国的重要基石

有效维护国家安全。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。要完善国家安全战略和国家安全政策，坚决维护国家政治安全，统筹推进各项安全工作。健全国家安全体系，加强国家安全法治保障，提高防范和抵御安全风险能力。严密防范和坚决打击各种渗透颠覆破坏活动、暴力恐怖活动、民族分裂活动、宗教极端活动。加强国家安全教育，增强全党全国人民国家安全意识，推动全社会形成维护国家安全的强大合力。

——2017年10月18日，习近平在中国共产党第十九次全国代表大会上作报告

#### **4、要坚持国家安全一切为了人民、一切依靠人民**

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，防范化解各类安全风险，不断提高人民群众的安全感、幸福感。

——2016年4月，习近平在首个全民国家安全教育日到来之际作出重要指示

#### **5、下好先手棋，打好主动仗，做好应对任何形式的矛盾风险挑战的准备**

推动创新发展、协调发展、绿色发展、开放发展、共享发展，前提都是国家安全、社会稳定。没有安全和稳定，一切都无从谈起。“明者防祸于未萌，智者图患于将来。”我们必须积极主动、未雨绸缪，见微知著、防微杜渐，下好先手棋，打好主动仗，做好应对任何形式的矛盾风险挑战的准备，做好经济上、政治上、文化上、社会上、外交上、军事上各种斗争的准备，层层负责、人人担当。

——2016年1月18日，习近平在省部级主要领导干部学习贯彻党的十八届五中全会精神专题研讨班上发表重要讲话

#### **6、安而不忘危，存而不忘亡，治而不忘乱**

改革开放以来，我们党始终高度重视正确处理改革发展稳定关系，始终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。我们保持了我国社会大局稳定，为改革开放和社会主义现代化建设营造了良好环境。“安而不忘危，存而不忘亡，治而不忘乱。”同时，必须清醒地看到，新形势下我国国家安全和社会安定面临的威胁和挑战增多，特别是各种威胁和挑战联动效应明显。我们必须保持清醒头脑、强化底线思维，有效防范、管理、处理国家安全风险，有力应对、处置、化解社会安定挑战。

——2014年4月25日，习近平在十八届中央政治局第十四次集体学习时发表讲话

#### **7、保证国家安全是头等大事**

增强忧患意识，做到居安思危，是我们治党治国必须始终坚持的一个重大原则。我们党要巩固执政地位，要团结带领人民坚持和发展中国特色社会主义，保证国家安全是头等大事。

——2014年4月15日，习近平在中央国家安全委员会第一次会议上发表重要讲话

## **8、以人民安全为宗旨，以政治安全为根本，走出一条中国特色国家安全道路**

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，必须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，走出一条中国特色国家安全道路。

——2014年4月15日，习近平在中央国家安全委员会第一次会议上发表重要讲话

## **维护重点领域国家安全**

### **1、政治安全**

办好中国的事情，关键在党。中国特色社会主义最本质的特征是中国共产党领导，中国特色社会主义制度的最大优势是中国共产党领导。坚持和完善党的领导，是党和国家的根本所在、命脉所在，是全国各族人民的利益所在、幸福所在。

——2016年7月1日，习近平在庆祝中国共产党成立九十五周年大会上发表重要讲话

### **2、国土安全**

维护国家主权和领土完整，实现祖国完全统一，是全体中华儿女共同愿望，是中华民族根本利益所在。在这个民族大义和历史潮流面前，一切分裂祖国的行径和伎俩都是注定要失败的，都会受到人民的谴责和历史的惩罚！中国人民有坚定的意志、充分的信心、足够的力量挫败一切分裂国家的活动！中国人民和中华民族有一个共同信念，这就是：我们伟大祖国的每一寸领土都绝对不能也绝对不可能从中国分割出去！

——2018年3月20日，习近平在第十三届全国人民代表大会第一次会议上发表重要讲话

### 3、军事安全

我国正处在由大向强发展的关键阶段，前景十分光明，挑战也十分严峻，中华民族伟大复兴绝不是轻轻松松、敲锣打鼓就能实现的。军事斗争是进行伟大斗争的重要方面，打赢能力是维护国家安全的战略能力。全军要强化忧患意识、危机意识、打仗意识，全部心思向打仗聚焦，各项工作向打仗用劲，尽快把备战打仗能力搞上去。

——2017年11月3日，习近平在视察军委联合作战指挥中心时发表重要讲话

### 4、经济安全

建设现代化经济体系，必须把发展经济的着力点放在实体经济上，把提高供给体系质量作为主攻方向，显著增强我国经济质量优势。加快建设制造强国，加快发展先进制造业，推动互联网、大数据、人工智能和实体经济深度融合，在中高端消费、创新引领、绿色低碳、共享经济、现代供应链、人力资本服务等领域培育新增长点、形成新动能。支持传统产业优化升级，加快发展现代服务业，瞄准国际标准提高水平。促进我国产业迈向全球价值链中高端，培育若干世界级先进制造业集群。加强水利、铁路、公路、水运、航空、管道、电网、信息、物流等基础设施网络建设。坚持去产能、去库存、去杠杆、降成本、补短板，优化存量资源配置，扩大优质增量供给，实现供需动态平衡。

——2017年10月18日，习近平在中国共产党第十九次全国代表大会上作报告

### 5、文化安全

牢牢掌握意识形态工作领导权。意识形态决定文化前进方向和发展道路。必须推进马克思主义中国化时代化大众化，建设具有强大凝聚力和引领力的社会主义意识形态，使全体人民在理想信念、价值理念、道德观念上紧紧团结在一起。要加强理论武装，推动新时代中国特色社会主义思想深入人心。深化马克思主义理论研究和建设，加快构建中国特色哲学社会科学，加强中国特色新型智库建设。坚持正确舆论导向，高度重视传播手段建设和创新，提高新闻舆论传播力、引导力、影响力、公信力。加强互联网内容建设，建立网络综合治理体系，营造清朗

的网络空间。落实意识形态工作责任制，加强阵地建设和管理，注意区分政治原则问题、思想认识问题、学术观点问题，旗帜鲜明反对和抵制各种错误观点。

——2017年10月18日，习近平在中国共产党第十九次全国代表大会上作报告

## 6、社会安全

发展是硬道理，稳定也是硬道理，抓发展、抓稳定两手都要硬。要坚定不移走中国特色社会主义社会治理之路，善于把党的领导和我国社会主义制度优势转化为社会治理优势，着力推进社会治理系统化、科学化、智能化、法治化，不断完善中国特色社会主义社会治理体系，确保人民安居乐业、社会安定有序、国家长治久安。

——2017年9月19日，习近平在会见全国社会治安综合治理表彰大会代表时发表重要讲话

## 7、科技安全

我们不拒绝任何新技术，新技术是人类文明发展的成果，只要有利于提高我国社会生产力水平、有利于改善人民生活，我们都不拒绝。问题是要搞清楚哪些是可以引进但必须安全可控的，哪些是可以引进消化吸收再创新的，哪些是可以同别人合作开发的，哪些是必须依靠自己的力量自主创新的。核心技术的根源问题是基础研究问题，基础研究搞不好，应用技术就会成为无源之水、无本之木。

——2016年4月19日，习近平在网络安全和信息化工作座谈会上发表重要讲话

## 8、网络安全

要理直气壮维护我国网络空间主权，明确宣示我们的主张。现在，各级领导干部特别是高级干部，如果不懂互联网、不善于运用互联网，就无法有效开展工作。各级领导干部要学网、懂网、用网，积极谋划、推动、引导互联网发展。要正确处理安全和发展、开放和自主、管理和服务的关系，不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力，把网络强国建设不断推向前进。

——2016年10月9日，习近平在十八届中央政治局第三十六次集体学习时发表讲话

## 9、核安全

中国将继续加强本国核安全，积极推进国际合作，分享技术和经验，贡献资源和平台。中国将构建核安全能力建设网络，推广减少高浓缩铀合作模式，实施加强放射源安全行动计划，启动应对核恐怖危机技术支持倡议，推广国家核电安全监管体系。只要我们精诚合作，持续加强核安全，核能造福人类的前景必将更加光明。

——2016年4月1日，习近平出席第四届核安全峰会并发表重要讲话

## 10、生态安全

生态环境没有替代品，用之不觉，失之难存。我讲过，环境就是民生，青山就是美丽，蓝天也是幸福，绿水青山就是金山银山；保护环境就是保护生产力，改善环境就是发展生产力。在生态环境保护上，一定要树立大局观、长远观、整体观，不能因小失大、顾此失彼、寅吃卯粮、急功近利。我们要坚持节约资源和保护环境的基本国策，像保护眼睛一样保护生态环境，像对待生命一样对待生态环境，推动形成绿色发展方式和生活方式，协同推进人民富裕、国家强盛、中国美丽。

——2016年1月18日，习近平在省部级主要领导干部学习贯彻党的十八届五中全会精神专题研讨班上发表重要讲话

## 11、资源安全

全面促进资源节约集约利用。生态环境问题，归根到底是资源过度开发、粗放利用、奢侈消费造成的。资源开发利用既要支撑当代人过上幸福生活，也要为子孙后代留下生存根基。要解决这个问题，就必须在转变资源利用方式、提高资源利用效率上下功夫。要树立节约集约循环利用的资源观，实行最严格的耕地保护、水资源管理制度，强化能源和水资源、建设用地总量和强度双控管理，更加重视资源利用的系统效率，更加重视在资源开发利用过程中减少对生态环境的损害，更加重视资源的再生循环利用，用最少的资源环境代价取得最大的经济社会效益。要全面推动重点领域低碳循环发展，加强高能耗行业能耗管理，强化建筑、交通节能，发展节水型产业，推动各种废弃物和垃圾集中处理和资源化利用。

——2017年5月26日，习近平在十八届中央政治局第四十一次集体学习时发表讲话

## **12、生物安全**

要从保护人民健康、保障国家安全、维护国家长治久安的高度，把生物安全纳入国家安全体系，系统规划国家生物安全风险防控和治理体系建设，全面提高国家生物安全治理能力。要尽快推动出台生物安全法，加快构建国家生物安全法律法规体系、制度保障体系。

——2020年2月14日，习近平在中央全面深化改革委员会第十二次会议上发表重要讲话

## 习近平：《为打赢疫情防控阻击战提供强大科技支撑》※

习近平

这次来军事医学研究院、清华大学医学院调研，主要是考察疫情防控科研攻关工作进展情况，看望奋战在疫情防控一线的科研工作者。

这次新冠肺炎疫情是新中国成立以来在我国发生的传播速度最快、感染范围最广、防控难度最大的一次重大突发公共卫生事件。党中央高度重视、迅速作出部署，把疫情防控作为头等大事来抓，把人民群众生命安全和身体健康摆在第一位，提出了坚定信心、同舟共济、科学防治、精准施策的总要求，明确了坚决遏制疫情蔓延势头、坚决打赢疫情防控阻击战的总目标。在党中央坚强领导下，经过各方面艰苦努力，目前疫情防控形势积极向好的态势正在拓展。

前不久，党中央召开了统筹推进新冠肺炎疫情防控和经济社会发展工作部署会议，我作了讲话。我还主持召开中央政治局常委会会议、中央政治局会议等，分析新冠肺炎疫情防控形势，研究防控重点工作。在这些场合，我都强调战胜疫情离不开科技支撑，要综合多学科力量加快科研攻关，在坚持科学性、确保安全性的基础上加快研发进度，力争早日取得突破，尽快拿出切实管用的研究成果。

疫情发生以来，全国科技战线积极响应党中央号召，科技、卫健等 12 个部门组成科研攻关组，确定临床救治和药物、疫苗研发、检测技术和产品、病毒病原学和流行病学、动物模型构建等五大主攻方向，组织跨学科、跨领域的科研团队，科研、临床、防控一线相互协同，产学研各方紧密配合，短短一个多月时间内就取得了积极进展。我们不到一周时间就确定了新冠病毒的全基因组序列并分离得到病毒毒株，及时向全球共享；适应疫情防控紧迫需求，面向全国揭榜，分阶段推出多种检测试剂产品；采取老药新用、研发新的治疗手段、

中西医结合等方式，迅速筛选了一批有效药物和治疗方案，推荐到临床一线救治；采取多条技术路线并行推进疫苗研发；通过对病毒生存环境、传播途径方面的研究，为制定完善防控策略提供了科学依据；在较短时间内构建了多个动物模型，为药物、疫苗研发提供了重要支撑。同时，专家学者及时发声、答疑解惑，稳定人心、坚定信心，为打赢疫情防控这场硬仗提供了有力科技支撑。



2020年3月10日，中共中央总书记、国家主席、中央军委主席习近平专门赴湖北省武汉市考察新冠肺炎疫情防控工作。这是习近平在火神山医院指挥中心视频连线感染科病房，与病房内患者和医务人员亲切交流。新华社记者 谢环驰/摄

在这场重大斗争中，广大科技工作者充分展示了拼搏奉献的优良作风、严谨求实的专业精神，涌现出一批先进典型。在这里，我代表党中央，向奋斗在疫情防控科研攻关一线的广大科技工作者表示衷心的感谢和诚挚的问候！

纵观人类发展史，人类同疾病较量最有力的武器就是科学技术，人类战胜大灾大疫离不开科学发展和技术创新。我国历史上有很多防治瘟疫的医疗著作和方法。《汉书·平帝纪》记载，元始二年，“民疾疫者，舍空邸第，为置医药”，提出了“隔离”是防疫的重要举措。

明代中期我国就出现了预防天花的“人痘”接种术。18 世纪末，英国科学家爱德华·琴纳发明了接种牛痘预防天花的方法，经过几代科学家不懈努力，最终研制出灭活天花病毒的疫苗。随着现代医学科技发展和公共卫生基础设施不断完善，霍乱、鼠疫、流感等这些曾经对人类造成巨大危害的传染病逐渐得到了有效控制。近些年来，在抗击严重急性呼吸综合征（SARS）、中东呼吸综合征（MERS）、甲型 H1N1 流感、埃博拉病毒等多次重大传染病中，科学技术都发挥了重要作用。新中国成立以来，我国通过传染病重大科技专项研发部署，在传染病防治领域的科研水平、技术能力、平台建设、人才队伍等方面都有了明显提升。



2020 年 3 月 2 日，中共中央总书记、国家主席、中央军委主席习近平在北京考察新冠肺炎防控科研攻关工作。这是习近平在军事医学研究院重大疫情应急防控药物研究室了解疫苗和抗体研制情况。新华社记者 丁海涛/摄

当前，打赢疫情防控人民战争、总体战、阻击战还需要付出艰苦努力。我们对新冠肺炎疫情的源头和宿主、传播途径、致病机理、危害性致命性、诊疗方案、救治药物以及患者康复后是否存在后遗症等，都还没有完全搞清楚。越是面对这种情况，越要坚持向科学要答案、要方法。希望广大科技工作者勇担责任、尽锐出战，尽快攻克疫情防

控的重点难点问题，为打赢疫情防控人民战争、总体战、阻击战提供强大科技支撑。下一步，要重点在以下几个方面下功夫。

**第一，加强药物、医疗装备研发和临床救治相结合，切实提高治愈率、降低死亡率。**3月1日，全国仍有7300多名重症和危重症患者，每天死亡人数还不少，主要是在湖北和武汉。尽最大努力挽救更多患者生命是当务之急、重中之重。科研攻关要把危重症患者救治当作头等大事，强化科研攻关支撑和服务前方一线救治的部署，坚持临床研究和临床救治协同，让科研成果更多向临床一线倾斜。要加快药物研发进程，坚持中西医结合、中西药并用，加快推广应用已经研发和筛选的有效药物，同时根据一线救治需要再筛选一批有效治疗药物，探索新的治疗手段，尽最大可能阻止轻症患者向重症转化，切实提高治愈率。要采取恢复期血浆、干细胞、单克隆抗体等先进治疗方式，提升重症、危重症救治水平，尽量降低死亡率。

**第二，推进疫苗研发和产业化链条有机衔接，为有可能出现的常态化防控工作做好周全准备。**疫苗作为用于健康人的特殊产品，对疫情防控至关重要，对安全性的要求也是第一位的。要加快推进已有的多种技术路线疫苗研发，同时密切跟踪国外研发进展，加强合作，争取早日推动疫苗的临床试验和上市使用。我们要立足当前、着眼长远，加快建立以企业为主体、产学研相结合的疫苗研发和产业化体系，建立国家疫苗储备制度。

**第三，统筹病毒溯源及其传播途径研究，搞清楚病源从哪里来、向哪里去。**正如专家所言，这次疫情病毒很狡猾，溯源工作面临很大困难。同时，新技术发展为病毒溯源提供了新的手段，可以利用病毒蛋白和不同受体的结合特征，评估可疑动物作为中间宿主的可能性，利用人工智能、大数据等新技术开展流行病学和溯源调查，提高精准度和筛查效率。病毒溯源和传播途径研究，对整个疫情防控至关重要，必须全力弄清楚。

**第四，做好患者康复和隔离群众的心理疏导工作。**病人心理康复需要一个过程，很多隔离在家的群众时间长了会产生这样那样的心理

问题，病亡者家属也需要心理疏导。这个问题解决不好，会带来社会稳定隐患。要高度重视他们的心理健康，动员各方面力量全面加强心理疏导工作。



2020年3月2日，中共中央总书记、国家主席、中央军委主席习近平在北京考察新冠肺炎防控科研攻关工作。这是习近平在清华大学医学院全球健康与传染病研究中心同科研人员交谈。新华社记者 燕雁/摄

**第五，完善平战结合的疫病防控和公共卫生科研攻关体系。**重大传染病和生物安全风险是事关国家安全和国家发展、事关社会大局稳定的重大风险挑战。要把生物安全作为国家总体安全的重要组成部分，坚持平时和战时结合、预防和应急结合、科研和救治防控结合，加强疫病防控和公共卫生科研攻关体系和能力建设。要统筹各方面科研力量，提高体系化对抗能力和水平。平时科研积累和技术储备是基础性工作，要加强战略谋划和前瞻布局，完善疫情防控预警预测机制，及时有效捕获信息，及时采取应对举措。要研究建立疫情蔓延进入紧急

状态后的科研攻关等方面指挥、行动、保障体系，平时准备好应急行动指南，紧急情况下迅速启动。

生命安全和生物安全领域的重大科技成果也是国之重器，疫病防控和公共卫生应急体系是国家战略体系的重要组成部分。要完善关键核心技术攻关的新型举国体制，加快推进人口健康、生物安全等领域科研力量布局，整合生命科学、生物技术、医药卫生、医疗设备等领域的国家重点科研体系，布局一批国家临床医学研究中心，加大卫生健康领域科技投入，加强生命科学领域的基础研究和医疗健康关键核心技术突破，加快提高疫病防控和公共卫生领域战略科技力量和战略储备能力。要加快补齐我国高端医疗装备短板，加快关键核心技术攻关，突破这些技术装备瓶颈，实现高端医疗装备自主可控。

**第六，坚持开展爱国卫生运动。**这不是简单的清扫卫生，更多应该从人居环境改善、饮食习惯、社会心理健康、公共卫生设施等多个方面开展工作，特别是要坚决杜绝食用野生动物的陋习，提倡文明健康、绿色环保的生活方式。

**第七，加强疫情防控科研攻关的国际合作。**公共卫生安全是人类面临的共同挑战，需要各国携手应对。当前，新冠肺炎疫情在多个国家出现，要加强同世卫组织沟通交流，同有关国家特别是疫情高发国家在溯源、药物、疫苗、检测等方面的科研合作，在保证国家安全的前提下，共享科研数据和信息，共同研究提出应对策略，为推动构建人类命运共同体贡献智慧和力量。

最后，希望广大科技工作者再接再厉，把疫情防控科研攻关作为科技战线的一项重大而紧迫任务，统一领导、协同推进科研攻关，拿出更多成果，不辜负党中央重托，不辜负人民期盼。

※这是习近平总书记 2020 年 3 月 2 日在同有关部门负责同志和专家学者就疫情防控科研攻关工作座谈时的讲话。

# 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)

## 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。

# 中华人民共和国反间谍法

《中华人民共和国反间谍法》由中华人民共和国第十二届全国人民代表大会常务委员会第十一次会议于2014年11月1日通过，自公布之日起施行。

## 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。

# 中华人民共和国反恐怖主义法

(2015年12月27日第十二届全国人民代表大会常务委员会第十八次会议通过)

## 第一章 总则

第一条 为了防范和惩治恐怖活动，加强反恐怖主义工作，维护国家安全、公共安全和人民生命财产安全，根据宪法，制定本法。

第二条 国家反对一切形式的恐怖主义，依法取缔恐怖活动组织，对任何组织、策划、准备实施、实施恐怖活动，宣扬恐怖主义，煽动实施恐怖活动，组织、领导、参加恐怖活动组织，为恐怖活动提供帮助的，依法追究法律责任。

国家不向任何恐怖活动组织和人员作出妥协，不向任何恐怖活动人员提供庇护或者给予难民地位。

第三条 本法所称恐怖主义，是指通过暴力、破坏、恐吓等手段，制造社会恐慌、危害公共安全、侵犯人身财产，或者胁迫国家机关、国际组织，以实现其政治、意识形态等目的的主张和行为。

本法所称恐怖活动，是指恐怖主义性质的下列行为：

(一)组织、策划、准备实施、实施造成或者意图造成人员伤亡、重大财产损失、公共设施损坏、社会秩序混乱等严重社会危害的活动的；

(二)宣扬恐怖主义，煽动实施恐怖活动，或者非法持有宣扬恐怖主义的物品，强制他人在公共场所穿戴宣扬恐怖主义的服饰、标志的；

(三)组织、领导、参加恐怖活动组织的；

(四)为恐怖活动组织、恐怖活动人员、实施恐怖活动或者恐怖活动培训提供信息、资金、物资、劳务、技术、场所等支持、协助、便利的；

(五)其他恐怖活动。

本法所称恐怖活动组织，是指三人以上为实施恐怖活动而组成的犯罪组织。

本法所称恐怖活动人员，是指实施恐怖活动的人和恐怖活动组织的成员。

本法所称恐怖事件，是指正在发生或者已经发生的造成或者可能造成重大社会危害的恐怖活动。

第四条 国家将反恐怖主义纳入国家安全战略，综合施策，标本兼治，加强反恐怖主义的能力建设，运用政治、经济、法律、文化、教育、外交、军事等手段，开展反恐怖主义工作。

国家反对一切形式的以歪曲宗教教义或者其他方法煽动仇恨、煽动歧视、鼓吹暴力等极端主义，消除恐怖主义的思想基础。

第五条 反恐怖主义工作坚持专门工作与群众路线相结合，防范为主、惩防结合和先发制敌、保持主动的原则。

第六条 反恐怖主义工作应当依法进行，尊重和保障人权，维护公民和组织的合法权益。

在反恐怖主义工作中，应当尊重公民的宗教信仰自由和民族风俗习惯，禁止任何基于地域、民族、宗教等理由的歧视性做法。

第七条 国家设立反恐怖主义工作领导机构，统一领导和指挥全国反恐怖主义工作。

设区的市级以上地方人民政府设立反恐怖主义工作领导机构，县级人民政府根据需要设立反恐怖主义工作领导机构，在上级反恐怖主义工作领导机构的领导和指挥下，负责本地区反恐怖主义工作。

第八条 公安机关、国家安全机关和人民检察院、人民法院、司法行政机关以及其他有关国家机关，应当根据分工，实行工作责任制，依法做好反恐怖主义工作。

中国人民解放军、中国人民武装警察部队和民兵组织依照本法和其他有关法律、行政法规、军事法规以及国务院、中央军事委员会的命令，并根据反恐怖主义工作领导机构的部署，防范和处置恐怖活动。

有关部门应当建立联动配合机制，依靠、动员村民委员会、居民委员会、企业事业单位、社会组织，共同开展反恐怖主义工作。

第九条 任何单位和个人都有协助、配合有关部门开展反恐怖主义工作的义务，发现恐怖活动嫌疑或者恐怖活动嫌疑人员的，应当及时向公安机关或者有关部门报告。

第十条 对举报恐怖活动或者协助防范、制止恐怖活动有突出贡献的单位和个人，以及在反恐怖主义工作中作出其他突出贡献的单位和个人，按照国家有关规定给予表彰、奖励。

第十一条 对在中华人民共和国领域外对中华人民共和国国家、公民或者机构实施的恐怖活动犯罪，或者实施的中华人民共和国缔结、参加的国际条约所规定的恐怖活动犯罪，中华人民共和国行使刑事管辖权，依法追究刑事责任。

## 第二章 恐怖活动组织和人员的认定

第十二条 国家反恐怖主义工作领导机构根据本法第三条的规定，认定恐怖活动组织和人员，由国家反恐怖主义工作领导机构的办事机构予以公告。

第十三条 国务院公安部门、国家安全部门、外交部门和省级反恐怖主义工作领导机构对于需要认定恐怖活动组织和人员的，应当向国家反恐怖主义工作领导机构提出申请。

第十四条 金融机构和特定非金融机构对国家反恐怖主义工作领导机构的办事机构公告的恐怖活动组织和人员的资金或者其他资产，应当立即予以冻结，并按照规定及时向国务院公安部门、国家安全部门和反洗钱行政主管部门报告。

第十五条 被认定的恐怖活动组织和人员对认定不服的，可以通过国家反恐怖主义工作领导机构的办事机构申请复核。国家反恐怖主义工作领导机构应当及时进行复核，作出维持或者撤销认定的决定。复核决定为最终决定。

国家反恐怖主义工作领导机构作出撤销认定的决定的，由国家反恐怖主义工作领导机构的办事机构予以公告；资金、资产已被冻结的，应当解除冻结。

第十六条 根据刑事诉讼法的规定，有管辖权的中级人民法院在审判刑事案件的过程中，可以依法认定恐怖活动组织和人员。对于在判决生效后需要由国家反恐怖主义工作领导机构的办事机构予以公告的，适用本章的有关规定。

### 第三章 安全防范

第十七条 各级人民政府和有关部门应当组织开展反恐怖主义宣传教育，提高公民的反恐怖主义意识。

教育、人力资源行政主管部门和学校、有关职业培训机构应当将恐怖活动预防、应急知识纳入教育、教学、培训的内容。

新闻、广播、电视、文化、宗教、互联网等有关单位，应当有针对性地面向社会进行反恐怖主义宣传教育。

村民委员会、居民委员会应当协助人民政府以及有关部门，加强反恐怖主义宣传教育。

第十八条 电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助。

第十九条 电信业务经营者、互联网服务提供者应当依照法律、行政法规规定，落实网络安全、信息内容监督制度和安全技术防范措施，防止含有恐怖主义、极端主义内容的信息传播；发现含有恐怖主义、极端主义内容的信息的，应当立即停止传输，保存相关记录，删除相关信息，并向公安机关或者有关部门报告。

网信、电信、公安、国家安全等主管部门对含有恐怖主义、极端主义内容的信息，应当按照职责分工，及时责令有关单位停止传输、删除相关信息，或者关闭相关网站、关停相关服务。有关单位应当立即执行，并保存相关记录，协助进行调查。对互联网上跨境传输的含

有恐怖主义、极端主义内容的信息，电信主管部门应当采取技术措施，阻断传播。

第二十条 铁路、公路、水上、航空的货运和邮政、快递等物流运营单位应当实行安全查验制度，对客户身份进行查验，依照规定对运输、寄递物品进行安全检查或者开封验视。对禁止运输、寄递，存在重大安全隐患，或者客户拒绝安全查验的物品，不得运输、寄递。

前款规定的物流运营单位，应当实行运输、寄递客户身份、物品信息登记制度。

第二十一条 电信、互联网、金融、住宿、长途客运、机动车租赁等业务经营者、服务提供者，应当对客户身份进行查验。对身份不明或者拒绝身份查验的，不得提供服务。

第二十二条 生产和进口单位应当依照规定对枪支等武器、弹药、管制器具、危险化学品、民用爆炸物品、核与放射物品作出电子追踪标识，对民用爆炸物品添加安检示踪标识物。

运输单位应当依照规定对运营中的危险化学品、民用爆炸物品、核与放射物品的运输工具通过定位系统实行监控。

有关单位应当依照规定对传染病病原体等物质实行严格的监督管理，严密防范传染病病原体等物质扩散或者流入非法渠道。

对管制器具、危险化学品、民用爆炸物品，国务院有关主管部门或者省级人民政府根据需要，在特定区域、特定时间，可以决定对生产、进出口、运输、销售、使用、报废实施管制，可以禁止使用现金、实物进行交易或者对交易活动作出其他限制。

第二十三条 发生枪支等武器、弹药、危险化学品、民用爆炸物品、核与放射物品、传染病病原体等物质被盗、被抢、丢失或者其他流失的情形，案发单位应当立即采取必要的控制措施，并立即向公安机关报告，同时依照规定向有关主管部门报告。公安机关接到报告后，应当及时开展调查。有关主管部门应当配合公安机关开展工作。

任何单位和个人不得非法制作、生产、储存、运输、进出口、销售、提供、购买、使用、持有、报废、销毁前款规定的物品。公安机

关发现的，应当予以扣押；其他主管部门发现的，应当予以扣押，并立即通报公安机关；其他单位、个人发现的，应当立即向公安机关报告。

第二十四条 国务院反洗钱行政主管部门、国务院有关部门、机构依法对金融机构和特定非金融机构履行反恐怖主义融资义务的情况进行监督管理。

国务院反洗钱行政主管部门发现涉嫌恐怖主义融资的，可以依法进行调查，采取临时冻结措施。

第二十五条 审计、财政、税务等部门在依照法律、行政法规的规定对有关单位实施监督检查的过程中，发现资金流入流出涉嫌恐怖主义融资的，应当及时通报公安机关。

第二十六条 海关在对进出境人员携带现金和无记名有价证券实施监管的过程中，发现涉嫌恐怖主义融资的，应当立即通报国务院反洗钱行政主管部门和有管辖权的公安机关。

第二十七条 地方各级人民政府制定、组织实施城乡规划，应当符合反恐怖主义工作的需要。

地方各级人民政府应当根据需要，组织、督促有关建设单位在主要道路、交通枢纽、城市公共区域的重点部位，配备、安装公共安全视频图像信息系统等防范恐怖袭击的技防、物防设备、设施。

第二十八条 公安机关和有关部门对宣扬极端主义，利用极端主义危害公共安全、扰乱公共秩序、侵犯人身财产、妨害社会管理的，应当及时予以制止，依法追究法律责任。

公安机关发现极端主义活动的，应当责令立即停止，将有关人员强行带离现场并登记身份信息，对有关物品、资料予以收缴，对非法活动场所予以查封。

任何单位和个人发现宣扬极端主义的物品、资料、信息的，应当立即向公安机关报告。

第二十九条 对被教唆、胁迫、引诱参与恐怖活动、极端主义活动，或者参与恐怖活动、极端主义活动情节轻微，尚不构成犯罪的人

员，公安机关应当组织有关部门、村民委员会、居民委员会、所在单位、就读学校、家庭和监护人对其进行帮教。

监狱、看守所、社区矫正机构应当加强对服刑的恐怖活动罪犯和极端主义罪犯的管理、教育、矫正等工作。监狱、看守所对恐怖活动罪犯和极端主义罪犯，根据教育改造和维护监管秩序的需要，可以与普通刑事罪犯混合关押，也可以个别关押。

第三十条 对恐怖活动罪犯和极端主义罪犯被判处徒刑以上刑罚的，监狱、看守所应当在刑满释放前根据其犯罪性质、情节和社会危害程度，服刑期间的表现，释放后对所居住社区的影响等进行社会危险性评估。进行社会危险性评估，应当听取有关基层组织和原办案机关的意见。经评估具有社会危险性的，监狱、看守所应当向罪犯服刑地的中级人民法院提出安置教育建议，并将建议书副本抄送同级人民检察院。

罪犯服刑地的中级人民法院对于确有社会危险性的，应当在罪犯刑满释放前作出责令其在刑满释放后接受安置教育的决定。决定书副本应当抄送同级人民检察院。被决定安置教育的人员对决定不服的，可以向上一级人民法院申请复议。

安置教育由省级人民政府组织实施。安置教育机构应当每年对被安置教育人员进行评估，对于确有悔改表现，不致再危害社会的，应当及时提出解除安置教育的意见，报决定安置教育的中级人民法院作出决定。被安置教育人员有权申请解除安置教育。

人民检察院对安置教育的决定和执行实行监督。

第三十一条 公安机关应当会同有关部门，将遭受恐怖袭击的可能性较大以及遭受恐怖袭击可能造成重大的人身伤亡、财产损失或者社会影响的单位、场所、活动、设施等确定为防范恐怖袭击的重点目标，报本级反恐怖主义工作领导小组备案。

第三十二条 重点目标的管理单位应当履行下列职责：

(一)制定防范和应对处置恐怖活动的预案、措施，定期进行培训和演练；

(二)建立反恐怖主义工作专项经费保障制度，配备、更新防范和处置设备、设施；

(三)指定相关机构或者落实责任人员，明确岗位职责；

(四)实行风险评估，实时监测安全威胁，完善内部安全管理；

(五)定期向公安机关和有关部门报告防范措施落实情况。

重点目标的管理单位应当根据城乡规划、相关标准和实际需要，对重点目标同步设计、同步建设、同步运行符合本法第二十七条规定的技防、物防设备、设施。

重点目标的管理单位应当建立公共安全视频图像信息系统值班监看、信息保存使用、运行维护等管理制度，保障相关系统正常运行。采集的视频图像信息保存期限不得少于九十日。

对重点目标以外的涉及公共安全的其他单位、场所、活动、设施，其主管部门和管理单位应当依照法律、行政法规规定，建立健全安全管理制度，落实安全责任。

第三十三条 重点目标的管理单位应当对重要岗位人员进行安全背景审查。对有不适合情形的人员，应当调整工作岗位，并将有关情况通报公安机关。

第三十四条 大型活动承办单位以及重点目标的管理单位应当依照规定，对进入大型活动场所、机场、火车站、码头、城市轨道交通站、公路长途客运站、口岸等重点目标的人员、物品和交通工具进行安全检查。发现违禁品和管制物品，应当予以扣留并立即向公安机关报告；发现涉嫌违法犯罪人员，应当立即向公安机关报告。

第三十五条 对航空器、列车、船舶、城市轨道车辆、公共电汽车等公共交通运输工具，营运单位应当依照规定配备安保人员和相应设备、设施，加强安全检查和保卫工作。

第三十六条 公安机关和有关部门应当掌握重点目标的基础信息和重要动态，指导、监督重点目标的管理单位履行防范恐怖袭击的各项职责。

公安机关、中国人民武装警察部队应当依照有关规定对重点目标进行警戒、巡逻、检查。

第三十七条 飞行管制、民用航空、公安等主管部门应当按照职责分工，加强空域、航空器和飞行活动管理，严密防范针对航空器或者利用飞行活动实施的恐怖活动。

第三十八条 各级人民政府和军事机关应当在重点国(边)境地段和口岸设置拦阻隔离网、视频图像采集和防越境报警设施。

公安机关和中国人民解放军应当严密组织国(边)境巡逻，依照规定对抵离国(边)境前沿、进出国(边)境管理区和国(边)境通道、口岸的人员、交通运输工具、物品，以及沿海沿边地区的船舶进行查验。

第三十九条 出入境证件签发机关、出入境边防检查机关对恐怖活动人员和恐怖活动嫌疑人员，有权决定不准其出境入境、不予签发出入境证件或者宣布其出境入境证件作废。

第四十条 海关、出入境边防检查机关发现恐怖活动嫌疑人员或者涉嫌恐怖活动物品的，应当依法扣留，并立即移送公安机关或者国家安全机关。

检验检疫机关发现涉嫌恐怖活动物品的，应当依法扣留，并立即移送公安机关或者国家安全机关。

第四十一条 国务院外交、公安、国家安全、发展改革、工业和信息化、商务、旅游等主管部门应当建立境外投资合作、旅游等安全风险评估制度，对中国在境外的公民以及驻外机构、设施、财产加强安全保护，防范和应对恐怖袭击。

第四十二条 驻外机构应当建立健全安全防范制度和应对处置预案，加强对有关人员、设施、财产的安全保护。

#### 第四章 情报信息

第四十三条 国家反恐怖主义工作领导机构建立国家反恐怖主义情报中心，实行跨部门、跨地区情报信息工作机制，统筹反恐怖主义情报信息工作。

有关部门应当加强反恐怖主义情报信息搜集工作，对搜集的有关线索、人员、行动类情报信息，应当依照规定及时统一归口报送国家反恐怖主义情报中心。

地方反恐怖主义工作领导机构应当建立跨部门情报信息工作机制，组织开展反恐怖主义情报信息工作，对重要的情报信息，应当及时向上级反恐怖主义工作领导机构报告，对涉及其他地方的紧急情报信息，应当及时通报相关地方。

第四十四条 公安机关、国家安全机关和有关部门应当依靠群众，加强基层基础工作，建立基层情报信息工作力量，提高反恐怖主义情报信息工作能力。

第四十五条 公安机关、国家安全机关、军事机关在其职责范围内，因反恐怖主义情报信息工作的需要，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。

依照前款规定获取的材料，只能用于反恐怖主义应对处置和对恐怖活动犯罪、极端主义犯罪的侦查、起诉和审判，不得用于其他用途。

第四十六条 有关部门对于在本法第三章规定的安全防范工作中获取的信息，应当根据国家反恐怖主义情报中心的要求，及时提供。

第四十七条 国家反恐怖主义情报中心、地方反恐怖主义工作领导机构以及公安机关等有关部门应当对有关情报信息进行筛查、研判、核查、监控，认为有发生恐怖事件危险，需要采取相应的安全防范、应对处置措施的，应当及时通报有关部门和单位，并可以根据情况发出预警。有关部门和单位应当根据通报做好安全防范、应对处置工作。

第四十八条 反恐怖主义工作领导机构、有关部门和单位、个人应当对履行反恐怖主义工作职责、义务过程中知悉的国家秘密、商业秘密和个人隐私予以保密。

违反规定泄露国家秘密、商业秘密和个人隐私的，依法追究法律责任。

## 第五章 调查

第四十九条 公安机关接到恐怖活动嫌疑的报告或者发现恐怖活动嫌疑，需要调查核实的，应当迅速进行调查。

第五十条 公安机关调查恐怖活动嫌疑，可以依照有关法律规定对嫌疑人员进行盘问、检查、传唤，可以提取或者采集肖像、指纹、虹膜图像等人体生物识别信息和血液、尿液、脱落细胞等生物样本，并留存其签名。

公安机关调查恐怖活动嫌疑，可以通知了解有关情况的人员到公安机关或者其他地点接受询问。

第五十一条 公安机关调查恐怖活动嫌疑，有权向有关单位和个人收集、调取相关信息和材料。有关单位和个人应当如实提供。

第五十二条 公安机关调查恐怖活动嫌疑，经县级以上公安机关负责人批准，可以查询嫌疑人员的存款、汇款、债券、股票、基金份额等财产，可以采取查封、扣押、冻结措施。查封、扣押、冻结的期限不得超过二个月，情况复杂的，可以经上一级公安机关负责人批准延长一个月。

第五十三条 公安机关调查恐怖活动嫌疑，经县级以上公安机关负责人批准，可以根据其危险程度，责令恐怖活动嫌疑人员遵守下列一项或者多项约束措施：

(一) 未经公安机关批准不得离开所居住的市、县或者指定的处所；

(二) 不得参加大型群众性活动或者从事特定的活动；

(三) 未经公安机关批准不得乘坐公共交通工具或者进入特定的场所；

(四) 不得与特定的人员会见或者通信；

(五) 定期向公安机关报告活动情况；

(六) 将护照等出入境证件、身份证件、驾驶证件交公安机关保存。

公安机关可以采取电子监控、不定期检查等方式对其遵守约束措施的情况进行监督。

采取前两款规定的约束措施的期限不得超过三个月。对不需要继续采取约束措施的，应当及时解除。

第五十四条 公安机关经调查，发现犯罪事实或者犯罪嫌疑人的，应当依照刑事诉讼法的规定立案侦查。本章规定的有关期限届满，公安机关未立案侦查的，应当解除有关措施。

## 第六章 应对处置

第五十五条 国家建立健全恐怖事件应对处置预案体系。

国家反恐怖主义工作领导机构应当针对恐怖事件的规律、特点和可能造成的社会危害，分级、分类制定国家应对处置预案，具体规定恐怖事件应对处置的组织指挥体系和恐怖事件安全防范、应对处置程序以及事后社会秩序恢复等内容。

有关部门、地方反恐怖主义工作领导机构应当制定相应的应对处置预案。

第五十六条 应对处置恐怖事件，各级反恐怖主义工作领导机构应当成立由有关部门参加的指挥机构，实行指挥长负责制。反恐怖主义工作领导机构负责人可以担任指挥长，也可以确定公安机关负责人或者反恐怖主义工作领导机构的其他成员单位负责人担任指挥长。

跨省、自治区、直辖市发生的恐怖事件或者特别重大恐怖事件的应对处置，由国家反恐怖主义工作领导机构负责指挥；在省、自治区、直辖市范围内发生的涉及多个行政区域的恐怖事件或者重大恐怖事件的应对处置，由省级反恐怖主义工作领导机构负责指挥。

第五十七条 恐怖事件发生后，发生地反恐怖主义工作领导机构应当立即启动恐怖事件应对处置预案，确定指挥长。有关部门和中国人民解放军、中国人民武装警察部队、民兵组织，按照反恐怖主义工作领导机构和指挥长的统一领导、指挥，协同开展打击、控制、救援、救护等现场应对处置工作。

上级反恐怖主义工作领导机构可以对应对处置工作进行指导，必要时调动有关反恐怖主义力量进行支援。

需要进入紧急状态的，由全国人民代表大会常务委员会或者国务院依照宪法和其他有关法律规定的权限和程序决定。

第五十八条 发现恐怖事件或者疑似恐怖事件后，公安机关应当立即进行处置，并向反恐怖主义工作领导机构报告；中国人民解放军、中国人民武装警察部队发现正在实施恐怖活动的，应当立即予以控制并将案件及时移交公安机关。

反恐怖主义工作领导机构尚未确定指挥长的，由在场处置的公安机关职级最高的人员担任现场指挥员。公安机关未能到达现场的，由在场处置的中国人民解放军或者中国人民武装警察部队职级最高的人员担任现场指挥员。现场应对处置人员无论是否属于同一单位、系统，均应当服从现场指挥员的指挥。

指挥长确定后，现场指挥员应当向其请示、报告工作或者有关情况。

第五十九条 中华人民共和国在境外的机构、人员、重要设施遭受或者可能遭受恐怖袭击的，国务院外交、公安、国家安全、商务、金融、国有资产监督管理、旅游、交通运输等主管部门应当及时启动应对处置预案。国务院外交部门应当协调有关国家采取相应措施。

中华人民共和国在境外的机构、人员、重要设施遭受严重恐怖袭击后，经与有关国家协商同意，国家反恐怖主义工作领导机构可以组织外交、公安、国家安全等部门派出工作人员赴境外开展应对处置工作。

第六十条 应对处置恐怖事件，应当优先保护直接受到恐怖活动危害、威胁人员的人身安全。

第六十一条 恐怖事件发生后，负责应对处置的反恐怖主义工作领导机构可以决定由有关部门和单位采取下列一项或者多项应对处置措施：

(一)组织营救和救治受害人员，疏散、撤离并妥善安置受到威胁的人员以及采取其他救助措施；

(二)封锁现场和周边道路，查验现场人员的身份证件，在有关场所附近设置临时警戒线；

(三)在特定区域内实施空域、海(水)域管制，对特定区域内的交通运输工具进行检查；

(四)在特定区域内实施互联网、无线电、通讯管制；

(五)在特定区域内或者针对特定人员实施出境入境管制；

(六)禁止或者限制使用有关设备、设施，关闭或者限制使用有关场所，中止人员密集的活动或者可能导致危害扩大的生产经营活动；

(七)抢修被损坏的交通、电信、互联网、广播电视、供水、排水、供电、供气、供热等公共设施；

(八)组织志愿人员参加反恐怖主义救援工作，要求具有特定专长的人员提供服务；

(九)其他必要的应对处置措施。

采取前款第三项至第五项规定的应对处置措施，由省级以上反恐怖主义工作领导机构决定或者批准；采取前款第六项规定的应对处置措施，由设区的市级以上反恐怖主义工作领导机构决定。应对处置措施应当明确适用的时间和空间范围，并向社会公布。

第六十二条 人民警察、人民武装警察以及其他依法配备、携带武器的应对处置人员，对在现场持枪支、刀具等凶器或者使用其他危险方法，正在或者准备实施暴力行为的人员，经警告无效的，可以使用武器；紧急情况下或者警告后可能导致更为严重危害后果的，可以直接使用武器。

第六十三条 恐怖事件发生、发展和应对处置信息，由恐怖事件发生地的省级反恐怖主义工作领导机构统一发布；跨省、自治区、直辖市发生的恐怖事件，由指定的省级反恐怖主义工作领导机构统一发布。

任何单位和个人不得编造、传播虚假恐怖事件信息；不得报道、传播可能引起模仿的恐怖活动的实施细节；不得发布恐怖事件中残忍、不人道的场景；在恐怖事件的应对处置过程中，除新闻媒体经负

责发布信息的反恐怖主义工作领导小组批准外，不得报道、传播现场应对处置的工作人员、人质身份信息和应对处置行动情况。

第六十四条 恐怖事件应对处置结束后，各级人民政府应当组织有关部门帮助受影响的单位和个人尽快恢复生活、生产，稳定受影响地区的社会秩序和公众情绪。

第六十五条 当地人民政府应当及时给予恐怖事件受害人员及其近亲属适当的救助，并向失去基本生活条件的受害人员及其近亲属及时提供基本生活保障。卫生、民政等主管部门应当为恐怖事件受害人员及其近亲属提供心理、医疗等方面的援助。

第六十六条 公安机关应当及时对恐怖事件立案侦查，查明事件发生的原因、经过和结果，依法追究恐怖活动组织、人员的刑事责任。

第六十七条 反恐怖主义工作领导小组应当对恐怖事件的发生和应对处置工作进行全面分析、总结评估，提出防范和应对处置改进措施，向上一级反恐怖主义工作领导小组报告。

## 第七章 国际合作

第六十八条 中华人民共和国根据缔结或者参加的国际条约，或者按照平等互惠原则，与其他国家、地区、国际组织开展反恐怖主义合作。

第六十九条 国务院有关部门根据国务院授权，代表中国政府与外国政府和有关国际组织开展反恐怖主义政策对话、情报信息交流、执法合作和国际资金监管合作。

在不违背我国法律的前提下，边境地区的县级以上地方人民政府及其主管部门，经国务院或者中央有关部门批准，可以与相邻国家或者地区开展反恐怖主义情报信息交流、执法合作和国际资金监管合作。

第七十条 涉及恐怖活动犯罪的刑事司法协助、引渡和被判刑人移管，依照有关法律规定执行。

第七十一条 经与有关国家达成协议，并报国务院批准，国务院公安部门、国家安全部门可以派员出境执行反恐怖主义任务。

中国人民解放军、中国人民武装警察部队派员出境执行反恐怖主义任务，由中央军事委员会批准。

第七十二条 通过反恐怖主义国际合作取得的材料可以在行政处罚、刑事诉讼中作为证据使用，但我方承诺不作为证据使用的除外。

## 第八章 保障措施

第七十三条 国务院和县级以上地方各级人民政府应当按照事权划分，将反恐怖主义工作经费分别列入同级财政预算。

国家对反恐怖主义重点地区给予必要的经费支持，对应对处置大规模恐怖事件给予经费保障。

第七十四条 公安机关、国家安全机关和有关部门，以及中国人民解放军、中国人民武装警察部队，应当依照法律规定的职责，建立反恐怖主义专业力量，加强专业训练，配备必要的反恐怖主义专业设备、设施。

县级、乡级人民政府根据需要，指导有关单位、村民委员会、居民委员会建立反恐怖主义工作力量、志愿者队伍，协助、配合有关部门开展反恐怖主义工作。

第七十五条 对因履行反恐怖主义工作职责或者协助、配合有关部门开展反恐怖主义工作导致伤残或者死亡的人员，按照国家有关规定给予相应的待遇。

第七十六条 因报告和制止恐怖活动，在恐怖活动犯罪案件中作证，或者从事反恐怖主义工作，本人或者其近亲属的人身安全面临危险的，经本人或者其近亲属提出申请，公安机关、有关部门应当采取下列一项或者多项保护措施：

- (一)不公开真实姓名、住址和工作单位等个人信息；
- (二)禁止特定的人接触被保护人员；
- (三)对人身和住宅采取专门性保护措施；

(四)变更被保护人员的姓名，重新安排住所和工作单位；

(五)其他必要的保护措施。

公安机关、有关部门应当依照前款规定，采取不公开被保护单位的真实名称、地址，禁止特定的人接近被保护单位，对被保护单位办公、经营场所采取专门性保护措施，以及其他必要的保护措施。

第七十七条 国家鼓励、支持反恐怖主义科学研究和技术创新，开发和推广使用先进的反恐怖主义技术、设备。

第七十八条 公安机关、国家安全机关、中国人民解放军、中国人民武装警察部队因履行反恐怖主义职责的紧急需要，根据国家有关规定，可以征用单位和个人的财产。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。

因开展反恐怖主义工作对有关单位和个人的合法权益造成损害的，应当依法给予赔偿、补偿。有关单位和个人有权依法请求赔偿、补偿。

## 第九章 法律责任

第七十九条 组织、策划、准备实施、实施恐怖活动，宣扬恐怖主义，煽动实施恐怖活动，非法持有宣扬恐怖主义的物品，强制他人在公共场所穿戴宣扬恐怖主义的服饰、标志，组织、领导、参加恐怖活动组织，为恐怖活动组织、恐怖活动人员、实施恐怖活动或者恐怖活动培训提供帮助的，依法追究刑事责任。

第八十条 参与下列活动之一，情节轻微，尚不构成犯罪的，由公安机关处十日以上十五日以下拘留，可以并处一万元以下罚款：

(一)宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；

(二)制作、传播、非法持有宣扬恐怖主义、极端主义的物品的；

(三)强制他人在公共场所穿戴宣扬恐怖主义、极端主义的服饰、标志的；

(四)为宣扬恐怖主义、极端主义或者实施恐怖主义、极端主义活动提供信息、资金、物资、劳务、技术、场所等支持、协助、便利的。

第八十一条 利用极端主义，实施下列行为之一，情节轻微，尚不构成犯罪的，由公安机关处五日以上十五日以下拘留，可以并处一万元以下罚款：

(一)强迫他人参加宗教活动，或者强迫他人向宗教活动场所、宗教教职人员提供财物或者劳务的；

(二)以恐吓、骚扰等方式驱赶其他民族或者有其他信仰的人员离开居住地的；

(三)以恐吓、骚扰等方式干涉他人与其他民族或者有其他信仰的人员交往、共同生活的；

(四)以恐吓、骚扰等方式干涉他人生活习俗、方式和生产经营的；

(五)阻碍国家机关工作人员依法执行职务的；

(六)歪曲、诋毁国家政策、法律、行政法规，煽动、教唆抵制人民政府依法管理的；

(七)煽动、胁迫群众损毁或者故意损毁居民身份证、户口簿等国家法定证件以及人民币的；

(八)煽动、胁迫他人以宗教仪式取代结婚、离婚登记的；

(九)煽动、胁迫未成年人不接受义务教育的；

(十)其他利用极端主义破坏国家法律制度实施的。

第八十二条 明知他人有恐怖活动犯罪、极端主义犯罪行为，窝藏、包庇，情节轻微，尚不构成犯罪的，或者在司法机关向其调查有关情况、收集有关证据时，拒绝提供的，由公安机关处十日以上十五日以下拘留，可以并处一万元以下罚款。

第八十三条 金融机构和特定非金融机构对国家反恐怖主义工作领导机构的办事机构公告的恐怖活动组织及恐怖活动人员的资金或者其他资产，未立即予以冻结的，由公安机关处二十万元以上五十万元以下罚款，并对直接负责的董事、高级管理人员和其他直接责任人员处十万元以下罚款；情节严重的，处五十万元以上罚款，并对直

接负责的董事、高级管理人员和其他直接责任人员，处十万元以上五十万元以下罚款，可以并处五日以上十五日以下拘留。

第八十四条 电信业务经营者、互联网服务提供者有下列情形之一的，由主管部门处二十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款；情节严重的，处五十万元以上罚款，并对其直接负责的主管人员和其他直接责任人员，处十万元以上五十万元以下罚款，可以由公安机关对其直接负责的主管人员和其他直接责任人员，处五日以上十五日以下拘留：

（一）未依照规定为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助的；

（二）未按照主管部门的要求，停止传输、删除含有恐怖主义、极端主义内容的信息，保存相关记录，关闭相关网站或者关停相关服务的；

（三）未落实网络安全、信息内容监督制度和安全技术防范措施，造成含有恐怖主义、极端主义内容的信息传播，情节严重的。

第八十五条 铁路、公路、水上、航空的货运和邮政、快递等物流运营单位有下列情形之一的，由主管部门处十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款：

（一）未实行安全查验制度，对客户身份进行查验，或者未依照规定对运输、寄递物品进行安全检查或者开封验视的；

（二）对禁止运输、寄递，存在重大安全隐患，或者客户拒绝安全查验的物品予以运输、寄递的；

（三）未实行运输、寄递客户身份、物品信息登记制度的。

第八十六条 电信、互联网、金融业务经营者、服务提供者未按规定对客户身份进行查验，或者对身份不明、拒绝身份查验的客户提供服务的，主管部门应当责令改正；拒不改正的，处二十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款；情节严重的，处五十万元以上罚款，并对其直接负

责的主管人员和其他直接责任人员，处十万元以上五十万元以下罚款。

住宿、长途客运、机动车租赁等业务经营者、服务提供者有前款规定情形的，由主管部门处十万元以上五十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处十万元以下罚款。

第八十七条 违反本法规定，有下列情形之一的，由主管部门给予警告，并责令改正；拒不改正的，处十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处一万元以下罚款：

(一)未依照规定对枪支等武器、弹药、管制器具、危险化学品、民用爆炸物品、核与放射物品作出电子追踪标识，对民用爆炸物品添加安检示踪标识物的；

(二)未依照规定对运营中的危险化学品、民用爆炸物品、核与放射物品的运输工具通过定位系统实行监控的；

(三)未依照规定对传染病病原体等物质实行严格的监督管理，情节严重的；

(四)违反国务院有关主管部门或者省级人民政府对管制器具、危险化学品、民用爆炸物品决定的管制或者限制交易措施的。

第八十八条 防范恐怖袭击重点目标的管理、营运单位违反本法规定，有下列情形之一的，由公安机关给予警告，并责令改正；拒不改正的，处十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处一万元以下罚款：

(一)未制定防范和应对处置恐怖活动的预案、措施的；

(二)未建立反恐怖主义工作专项经费保障制度，或者未配备防范和处置设备、设施的；

(三)未落实工作机构或者责任人员的；

(四)未对重要岗位人员进行安全背景审查，或者未将有不适合情形的人员调整工作岗位的；

(五)对公共交通运输工具未依照规定配备安保人员和相应设备、设施的；

(六)未建立公共安全视频图像信息系统值班监看、信息保存使用、运行维护等管理制度的。

大型活动承办单位以及重点目标的管理单位未依照规定对进入大型活动场所、机场、火车站、码头、城市轨道交通站、公路长途客运站、口岸等重点目标的人员、物品和交通工具进行安全检查的，公安机关应当责令改正；拒不改正的，处十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员处一万元以下罚款。

第八十九条 恐怖活动嫌疑人员违反公安机关责令其遵守的约束措施的，由公安机关给予警告，并责令改正；拒不改正的，处五日以上十五日以下拘留。

第九十条 新闻媒体等单位编造、传播虚假恐怖事件信息，报道、传播可能引起模仿的恐怖活动的实施细节，发布恐怖事件中残忍、不人道的场景，或者未经批准，报道、传播现场应对处置的工作人员、人质身份信息和应对处置行动情况的，由公安机关处二十万元以下罚款，并对其直接负责的主管人员和其他直接责任人员，处五日以上十五日以下拘留，可以并处五万元以下罚款。

个人有前款规定行为的，由公安机关处五日以上十五日以下拘留，可以并处一万元以下罚款。

第九十一条 拒不配合有关部门开展反恐怖主义安全防范、情报信息、调查、应对处置工作的，由主管部门处二千元以下罚款；造成严重后果的，处五日以上十五日以下拘留，可以并处一万元以下罚款。

单位有前款规定行为的，由主管部门处五万元以下罚款；造成严重后果的，处十万元以下罚款；并对其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。

第九十二条 阻碍有关部门开展反恐怖主义工作的，由公安机关处五日以上十五日以下拘留，可以并处五万元以下罚款。

单位有前款规定行为的，由公安机关处二十万元以下罚款，并对其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。

阻碍人民警察、人民解放军、人民武装警察依法执行职务的，从重处罚。

第九十三条 单位违反本法规定，情节严重的，由主管部门责令停止从事相关业务、提供相关服务或者责令停产停业；造成严重后果的，吊销有关证照或者撤销登记。

第九十四条 反恐怖主义工作领导机构、有关部门的工作人员在反恐怖主义工作中滥用职权、玩忽职守、徇私舞弊，或者有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；尚不构成犯罪的，依法给予处分。

反恐怖主义工作领导机构、有关部门及其工作人员在反恐怖主义工作中滥用职权、玩忽职守、徇私舞弊或者有其他违法违纪行为的，任何单位和个人有权向有关部门检举、控告。有关部门接到检举、控告后，应当及时处理并回复检举、控告人。

第九十五条 对依照本法规定查封、扣押、冻结、扣留、收缴的物品、资金等，经审查发现与恐怖主义无关的，应当及时解除有关措施，予以退还。

第九十六条 有关单位和个人对依照本法作出的行政处罚和行政强制措施决定不服的，可以依法申请行政复议或者提起行政诉讼。

## 第十章 附则

第九十七条 本法自2016年1月1日起施行。2011年10月29日第十一届全国人民代表大会常务委员会第二十三次会议通过的《全国人民代表大会常务委员会关于加强反恐怖工作有关问题的决定》同时废止。

# 中华人民共和国网络安全法

(2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过)

中华人民共和国主席令  
第五十三号

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。

中华人民共和国主席 习近平  
2016年11月7日

## 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 and 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。

单位有欠款行为的，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。

## 中华人民共和国保密法

### 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

## 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。