Law of the People's Republic of China on Guarding State Secrets

(Adopted at the Third Meeting of the Standing Committee of the Seventh National People's Congress on September 5, 1988, and revised at the 14th Session of the Standing Committee of the 11th National People's Congress on April 29, 2010.)

***

Order of the President of People's Republic of China
No. 28

The *Law of the People's Republic of China on Guarding State Secrets* was revised and adopted at the 14th Session of the Standing Committee of the 11th National People's Congress on April 29, 2010. It is hereby promulgated, and effective as of October 1, 2010.

Hu Jintao, President of the People's Republic of China

April 29, 2010

[English translation by Human Rights in China]

Contents

Chapter One: General Provisions

Article 1. This law is formulated for the purpose of guarding state secrets, safeguarding state security and national interests, and ensuring the smooth progress of reform, of opening to the outside world, and of socialist construction.

Article 2. State secrets shall be matters that have a vital bearing on state security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time.

Article 3. State secrets shall be protected by law.

All state organs, armed forces, political parties, public organizations, enterprises, units, and citizens shall have the obligation to guard state secrets.

Any activities endangering the security of state secrets must be punishable by law.

Article 4. The work of guarding state secrets (hereinafter referred to as "the secret-guarding work ") shall be carried out in line with the principles of active prevention of leaks, emphasizing priorities, and management according to the law, so that the security of state secrets is protected while the rational use of information and resources is facilitated.

Matters requiring disclosure by laws or administrative regulations shall be disclosed in accordance with the law.

Article 5. The national department for the administration and management of state secret-guarding work shall be responsible for guarding state secrets throughout the country. The local departments for the administration and management of secret-guarding at or above the county level shall be responsible for guarding secrets in their own administrative areas.

Article 6. State organs and units involved with state secrets (hereinafter referred to as "organs and units") shall manage the work of guarding secrets in their own organs and units.

The central state organs shall, within the scope of their functions and powers, manage or guide the work of guarding state secrets in their own organs and in the departments subordinate to them.

Article 7. Organs and units shall implement a system of responsibility for the work of guarding secrets, strengthen the system of management of guarding secrets, perfect measures to safeguard secrets, launch publicity and education on secret-guarding, and reinforce inspections of secret-guarding.

Article 8. The state shall reward those units or individuals that have rendered meritorious service in guarding and protecting state secrets and improving techniques and measures in this field.

Chapter Two: Scope and Classification of State Secrets

Article 9. The following matters involving state security and national interests, the disclosure of which may harm the country in politics, the economy, defense, foreign affairs, or other such realms, shall be classified as state secrets:

1. Secret matters concerning major policy decisions on state affairs;
2. Secret matters in the building of national defense and in the activities of the armed forces;
3. Secret matters in diplomatic activities and in activities related to foreign countries and those to be kept secret through commitments to foreign countries;
4. Secret matters in national economic and social development;
5. Secret matters concerning science and technology;
6. Secret matters concerning activities for safeguarding state security and the investigation of criminal offenses; and
7. Other matters that are classified as state secrets by the national department for the administration and management of state secret-guarding.

Secrets of political parties that correspond with the stipulations in the preceding paragraph shall be treated as state secrets.

Article 10. State secrets are classified into three categories: "top secret," "highly secret," and "secret."

Secrets classified as "top secret" are the most vital state secrets, the divulgence of which will cause extremely serious harm to state security and national interests; secrets classified as "highly secret" are important state secrets, the divulgence of which will cause serious harm to state security and national interests; and secrets classified as "secret" are ordinary state secrets, the divulgence of which will cause harm to state security and national interests.

Article 11. The specific scope of state secrets and their classification levels shall be stipulated by the national department for the administration and management of state secret-guarding together with the Ministries of Foreign Affairs, Public Security, and State Security, and other relevant central organs.

The specific scope of state secrets related to military affairs, and their classification levels, shall be stipulated by the Central Military Commission.

Stipulations on the specific scope and classification levels of state secrets shall be made known within relevant quarters and promptly adjusted according to changes in circumstance.

Article 12. Individuals in charge of organs and units, and personnel appointed by them, shall be the people responsible for classifying secrets; they shall be responsible for the task of classifying, reclassifying, and declassifying state secrets in their own organs and units.

The classification, reclassification, and declassification of state secrets by organs and units shall be proposed with specific opinions by the person who handles the matter and reviewed and approved by the people responsible for classifying secrets.

Article 13. The classification of the level of state secrets shall abide by the jurisdiction for classification determination.

Central state organs, provincial organs, and organs and units authorized by them may classify state secrets as top secrets, highly secrets, and secrets; the organs of districted cities or autonomous prefectures and organs or units authorized by them may classify state secrets as highly secrets and secrets. The specific jurisdiction for classification determination and the scope of authorization shall be stipulated by the national department for the administration and management of state secret-guarding.

Whenever organs or units which implement state secrets items set by superior authorities need to classify those secrets, they shall determine the classification level based on the classification level of state secrets item being executed. When the subordinate organs or

units believe that the classified items generated by them fall under the classification jurisdiction of their superior agencies and units, they shall first adopt measures to protect the secrets and immediately report to the superior agencies or units for determination. When there are no superior agencies or units, they shall immediately submit such items to the business administrative department with relevant jurisdiction for classification determination or to the national department for the administration and management of state secret-guarding for determination.

Public security organs and national security organs shall determine the classification level of state secrets within their scope of work in accordance with their prescribed jurisdiction.

Article 14. Organs and units shall, in accordance with the stipulations on the specific scope and classification levels of state secrets, determine the classification level of any state secret that arises in said organs and units, and at the same time determine the length of time that the secret should be protected and the range of those with knowledge of it.

Article 15. The length of time during which state secrets should be protected shall be limited to a period required based on the nature and characteristics of the item in accordance with the requirements of safeguarding national security and interests; when a time limit cannot be determined, the conditions for declassification shall be determined .

The length of time during which state secrets should be protected shall be, unless otherwise specified, not more than 30 years for top secrets, not more than 20 years for highly secrets, and not more than ten years for secrets. Organs and units shall determine the specific length of time during which secrets should be protected, the time of declassification, and the conditions for declassification, in accordance with work requirements.

Items which organs and units have classified as state secrets during the course of determining and handling related matters shall be declassified upon being officially published if the disclosure is deemed necessary based on work requirements.

Article 16. The range of those with knowledge of state secrets shall be restricted to the smallest range possible as required by work.

If the range of those with knowledge of state secrets can be limited to specific people, it shall be limited to specific people; if it cannot be limited to specific people, it shall be limited to an organ or a unit, and the organ or unit shall limit it to specific people.

Personnel outside the range of those with knowledge of state secrets, whose work requires knowledge of state secrets, shall go through the approval of the people in charge of the organs or units that originally classified the secret.

Article 17. Organs and units shall mark as state secrets any item of paper, optical, or electromagnetic medium bearing state secrets (hereinafter referred to as "items bearing state secrets"), as well as equipment and products that are a part of state secrets.

Items that are not a part of state secrets shall not be marked as state secrets.

Article 18. The classification levels of state secrets, the length of time that they should be guarded, and the range of those with knowledge of them shall be altered in accordance with changing circumstances. Such alterations shall be decided on by the state organs or units that originally determined the classification level of the secrets and the time period for guarding them, or by a higher-level department.

If the classification level of a state secret, the length of time that it should be guarded, or the range of those with knowledge of it is altered, a written notification shall promptly be sent to the organs, units, or personnel within the range of those with knowledge of it.

Article 19. A state secret shall be automatically declassified when the time period for guarding it has expired.

Organs and units shall conduct periodic audits of all classified state secrets. They shall promptly declassify a secret when it, during the period of classification, is determined as no longer requiring classification due to an adjustment of the scope of items to be guarded or the classification is determined to be no longer necessary because the disclosure of the item will not harm state security and national interests; if the time period for guarding a secret needs to be extended, that time limit shall be re-determined before the original period has expired. The advance declassification or extension of classification time period shall be decided by the organ or unit that originally classified it, or by a higher-level department.

Article 20. If organs or units are unclear about or disagree with whether a certain matter is a state secret or its classification level, it shall be determined by the national department for the administration and management of state secret-guarding, or the department for the administration and management of secret-guarding at the level of the province, autonomous region, or directly-administered municipality.

Chapter Three: System for Guarding State Secrets

Article 21. The making, receiving, dispatch, transfer, use, duplication, storage, maintenance, and destruction of items bearing state secrets shall conform to the stipulations for state secret-guarding.

Items bearing information classified as top secret shall be stored within facilities or equipment that conform to state secret-guarding standards, and shall be managed by specifically-designated individuals; the items shall not be duplicated or excerpted without prior approval from the organ or unit that originally classified them or by a higher-level department; designated personnel shall be responsible for receiving, transferring, and carrying them outside, and necessary security measures shall be adopted.

Article 22. The manufacture, production, transportation, use, storage, maintenance, and destruction of equipment or products classified as state secrets shall conform to state secret-guarding provisions.

Article 23. Computer information systems that store and process state secrets (hereinafter referred to as "secrets information systems") shall be protected according to classification level based on the degree of involvement with secrets.

The secrets information systems shall be outfitted with secret-guarding facilities and equipment that conform to state secret-guarding standards. The secret-guarding facilities and equipment shall be planned, built, and operated in step with the secrets information systems.

Before a secrets information system is put to use, it shall be inspected and approved in accordance with regulations.

Article 24. Organs and units shall reinforce the management of the secrets information systems; no organization or individual shall engage in the following conduct:

1. Connect computers or storage devices dealing with secrets to the Internet or other public information networks;
2. Exchange information between a secrets information system and the Internet or other public information networks without adopting protective measures;
3. Use computers or storage devices that do not deal with state secrets to save or process state secrets information;
4. Uninstall or modify security technology programs or administrative programs from a secrets information system without authorization;
5. Give away, sell, or discard or modify to another use those decommissioned computers and storage devices that have dealt with state secrets but have not gone through security technology procedures.

Article 25. Organs and units shall reinforce the management of items bearing state secrets; no organization or individual shall engage in the following conduct:

1. Illegally obtain or hold items bearing state secrets;
2. Buy, sell, transfer, or destroy items bearing state secrets without authorization;
3. Transfer items bearing state secrets through channels without secret-guarding measures, such as the ordinary postal service or express courier;
4. Mail or consign for shipment abroad items bearing state secrets;
5. Carry or transmit items bearing state secrets abroad without permission from the authorities in charge.

Article 26. Duplicating, recording, or storing state secrets in violation of the law is prohibited.

The transmission of state secrets through the Internet or other public information networks, or through wired or wireless communication, without first adopting secret-guarding measures is prohibited. Dealing with state secrets in private contact and correspondence is prohibited.

Article 27. The relevant secret-guarding regulations shall be complied with in editing, publishing, printing, and distributing newspapers and periodicals, books, audio- visual products, and electronic publications; in producing and broadcasting radio programs, television programs, and films; and in editing and releasing information through public

information networks such as the Internet and mobile communication networks, and through other media.

Article 28. Internet and other public information network operators and service providers must cooperate with public security, state security, and procuratorate organs in investigation of cases regarding leaking of secrets; when information involving leaking of state secrets is found to have been published through the Internet and other public information networks, transmission must stop immediately, relevant records must be kept, and reports must be made to public security organs, state security organs, or the departments for the administration and management of guarding state secrets; information involving leaking of state secrets must be deleted as required by public security organs, state security organs, or the departments for the administration and management of guarding state secrets.

Article 29. State organs and units shall comply with secret-guarding regulations when they publicly release information and purchase goods, or services or [any items] for projects involving state secrets.

Article 30. When organs and units have to provide state secrets in the course of maintaining foreign relations and cooperation, or when personnel appointed or hired abroad need to have knowledge of state secrets because it is required by their job, they shall report such information to the relevant supervising department in the State Council or to the relevant supervising department in the people's government of a province, autonomous region, or a directly-administered municipality for approval, and sign a confidentiality agreement with the concerned party.

Article 31. When holding meetings or conducting other activities that involve state secrets, the host unit shall adopt the appropriate secret-guarding measures, provide the participants with education on secret-guarding, and raise specific secret-guarding requirements.

Article 32. Organs and units shall designate as "key secret-guarding departments" the organizations that shall be involved with state secrets at the top-secret level or with relatively large amounts of highly secret or secret information; shall designate as "key secret-guarding positions" the specialized places that shall focus on the production, storage, or maintenance of items bearing state secrets; and shall outfit them in accordance with the state secret-guarding regulations and standards, and protect the facilities and equipment with the use of necessary techniques.

Article 33. Forbidden military zones and other places that involve state secrets and are not open to the public shall be protected by secret-guarding measures; no one may decide to open them to the public or enlarge the area that is open to the public without prior approval from the relevant authorities.

Article 34. Enterprises or public institutions whose business activities involve state secrets, including those who produce, reproduce, maintain, and destroy items bearing state secrets; those which are integrated into a secrets information system; and those which scientifically research or produce military equipment, shall be subject to secret-

guarding examinations. Specific measures for such examinations shall be stipulated by the State Council.

Organs and units that entrust enterprises and public institutes to engage in the operations stipulated in the above paragraph shall sign secret-guarding agreements with such enterprises and institutions; they shall make secret-guarding requirements, and security measures shall be adopted.

Article 35. Personnel working in jobs that involve secrets (hereinafter referred to as "personnel involved with secrets") shall be classified according to the degree of involvement with secrets into "core personnel involved with secrets," "important personnel involved with secrets," and "general personnel involved with secrets," and shall be managed by classification.

The employment or appointment of personnel involved with secrets shall be subject to examination in accordance with relevant regulations.

Personnel involved with secrets shall have good political awareness and characters and shall possess working ability qualified for positions involving secrets.
The lawful rights and interests of personnel involved with secrets shall be protected by law.

Article 36. When assuming a post, personnel involved with secrets shall receive education and training in secret-guarding, master the knowledge and skills of secret-guarding, sign a confidentiality agreement, strictly observe the rules and regulations for secret-guarding, and shall not divulge state secrets in any manner.

Article 37. If leaving the country, personnel involved with secrets shall receive approval from relevant departments; if the relevant department decides that the departure from the country by the personnel involved with secrets might endanger state security or cause serious damage to national interests, the exit approval shall not be granted.

Article 38. When leaving a post or resigning, personnel involved with state secrets shall undergo a period of release from secrets-management. During that period of release, personnel shall perform secret-guarding obligations in accordance with regulations and shall not obtain employment in violation of the regulations, nor shall they divulge state secrets in any manner.

Article 39. Organs and units shall establish a robust management system for personnel involved with secrets, specifying their rights and the responsibilities and requirements of their position, and shall regularly supervise and inspect the performance of their duties.

Article 40. If state employees and other citizens should find that state secrets have been divulged or are in danger of being divulged, they should immediately take measures to remedy the situation and promptly report the matter to the state organs and units concerned, which shall, upon receiving such reports, deal with the matter without delay and promptly report it to the department for the administration and management of state secret-guarding.

Chapter Four: Supervision and Management

Article 41. The national department for the administration and management of state secret-guarding shall, pursuant to the provisions of laws and administrative statutes, stipulate secret-guarding rules and regulations and set standards for state secret-guarding techniques.

Article 42. The department for the administration and management of state secret-guarding shall, in accordance with the law, undertake the task of secret-guarding publicity and education, secret-guarding inspection, defense of secret-guarding techniques, and investigation of secrecy leaks cases, and shall provide guidance and supervision of the secret-guarding work of organs and units.

Article 43. The department for the administration and management of state secret-guarding shall promptly notify relevant state organs and units of its discovery of improper classification, re-classification, or declassification of state secrets and shall correct it.

Article 44. The department for the administration and management of state secret-guarding shall conduct examinations into whether organs and units are complying with the secret-guarding system; the organs and units concerned shall cooperate with such examinations. The department for the administration and management of state secret-guarding, if it finds that there is a danger of secrecy leaks within an organ or unit, shall request that that organ or unit adopt measures and rectify the situation within a specified time; it shall order that the use of facilities, equipment, and locations where the danger of secrecy leaks exists be suspended; it shall suggest that the organ or unit in charge penalize personnel involved with secrets who gravely violate the secret-guarding regulations and remove them from positions that involve state secrets. If it discovers a suspected divulgence of state secrets, it shall urge and guide the organs or units concerned to investigate and handle the divulgence. If a crime is suspected, the case shall be transferred to the judicial organ for handling.

Article 45. The department for the administration and management of state secret-guarding shall seize any illegally obtained or held items bearing state secrets that it discovers in the course of a secret-guarding inspection.

Article 46. The organ that handles a case of a suspected leak of state secrets must carry out an appraisal of whether or not relevant matters are classified as state secrets and to which level of secret classification they belong; the national department for the administration and management of state secret-guarding or a department for the administration and management of state secret-guarding at the level of the province, autonomous region, or a directly-administered municipality shall [validate] the appraisal.

Article 47. If an organ or unit does not penalize personnel for violations of secret-guarding regulations in accordance with the law, the department for the administration and management of state secret-guarding shall recommend a correction; if the organ or unit refuses to make corrections, the department shall request that the organ at the next higher level or its supervisory organ penalize the responsible leaders and the personnel directly responsible in the organs or units in accordance with the law.

Chapter Five: Legal Responsibility

Article 48. Anyone who violates the provisions of this Law with any [form of] the conduct listed below shall be punished in accordance with the law; if the violation constitutes a crime, the individual shall be prosecuted and held criminally responsible in accordance with the law.

1. Illegally obtaining or possessing any items bearing state secrets;
2. Buying, selling, transferring, or destroying without authorization items bearing state secrets;
3. Transferring items bearing state secrets through channels without secret-guarding measures, such as the ordinary postal service and express delivery;
4. Mailing or consigning for shipment abroad items bearing state secrets, or carrying or transferring items bearing state secrets abroad without permission from the relevant departments;
5. Copying, recording, or storing state secrets illegally;
6. Touching on state secrets in private contact or correspondence;
7. Transmitting state secrets through the internet or other public information networks or in wired or wireless communications without having first adopted secret-guarding measures;
8. Connecting computers or other storage devices dealing with state secrets to the Internet or other public information networks;
9. Exchanging information between a secrets information system and the Internet or other public information network without having first adopted protective measures;
10. Using a computer or other storage device that do not deal with state secrets to store or process state secret information;
11. Uninstalling or modifying the security technology programs or administrative programs of a secrets information system without authorization;
12. Giving away, selling, discarding, or converting to other uses decommissioned computers and storage devices that have dealt with state secrets but not gone through security technology procedures.

Personnel who commit conduct in the above categories that does not constitute a crime and for whom disciplinary measures are not applicable shall be penalized by the organ or unit to which such personnel belong under the supervision of the department for the administration and management of state secret-guarding.

Article 49. If any organ or unit violates the provisions of this Law and causes a major divulgence of state secrets, the organ or unit shall penalize the person in charge who is directly responsible and other directly responsible personnel in accordance with the law; the personnel for whom disciplinary measures are not applicable shall be handled by the competent departments under the supervision of the administration and management of state secret-guarding.

If any organ or unit violates the provisions of this Law, either by not classifying items which should be classified as state secrets or by classifying items which should not be classified, and such violation leads to serious consequences, the organ or unit shall

penalize the chief person in charge who is directly responsible and other directly responsible persons.

Article 50. Internet and other public information network operators and service providers in violation of Article 28 of this Law shall be penalized in accordance with the law by the public security organ, the state security organ, or the relevant information industry department according to their respective authority conferred.

Article 51. Any personnel involved in the administrative management of state secrets who, in the course of performing their duty of managing state secrets abuse their authority, neglect their duty, or engage in bribery or fraud, shall be penalized in accordance with the law; those whose conduct constitutes a crime shall be legally prosecuted and held criminally responsible.

Chapter Six: Additional Provisions

Article 52. The Central Military Commission shall, in accordance with this Law, formulate the regulations of the Chinese People's Liberation Army on the protection of state secrets.

Article 53. This law shall take effect as of October 1, 2010.

中华人民共和国保守国家秘密法

中华人民共和国主席令
第二十八号

《中华人民共和国保守国家秘密法》已由中华人民共和国第十一届全国人民代表大会常务委员会第十四次会议于 2010 年 4 月 29 日修订通过，现将修 订后的《中华人民共和国保守国家秘密法》公布，自 2010 年 10 月 1 日起施行。

中华人民共和国主席　胡锦涛
2010 年 4 月 29 日

中华人民共和国保守国家秘密法（1988 年 9 月 5 日第七届全国人民代表大会常务委员会第三次会议通过 2010 年 4 月 29 日第十一届全国人民代表大会常务委员会第十四次会议 修订）

目　录

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：

（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；
（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；
（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；
（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；
（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。

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：

（十三） 非法获取、持有国家秘密载体；
（十四） 买卖、转送或者私自销毁国家秘密载体；
（十五） 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；
（十六） 邮寄、托运国家秘密载体出境；
（十七） 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。