



www.GOV.cn

中华人民共和国中央人民政府

The Central People's Government of the People's Republic of China



[Home](#) | [China Today](#) | [China Overview](#) | [Laws and Regulations](#) | [Official Bulletin](#) | [Government Interaction](#) | [Government Construction](#) | [Work Dynamics](#) | [Personnel Appointment and Removal](#) | [Press Releases](#)

Current Location: [Home](#) >> [Law and Regulation](#) >> [Law](#)

Central government portal www.gov.cn April 30, 2010 Source: Xinhua News Agency

[Font: [large](#),
[medium](#) and [small](#)]

[print this page](#)

[close the window](#)

Order of the President of the People's Republic of China

No. 28

The Law of the People's Republic of China on Guarding State Secrets was revised and adopted by the 14th meeting of the Standing Committee of the 11th National People's Congress of the People's Republic of China on April 29, 2010. The Secret Law was promulgated and came into force on October 1, 2010.

President of the People's

Republic of China Hu Jintao

April 29, 2010

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 fourteenth meeting of the Standing Committee of the Eleventh National People's Congress on April 29, 2010)

Table of contents

Chapter 1 General Provisions Chapter

2 Scope and Classes of State Secrets

Chapter 3 Secrecy System

Chapter 4 Supervision and Administration

Chapter 5 Legal Responsibilities

Chapter 6 Supplementary Provisions

Chapter 1 General Provisions

Article 1 This Law is formulated for the purpose of keeping state secrets, safeguarding national security and interests, and ensuring the smooth progress of reform and opening up and socialist construction.

Article 2 State secrets are matters related to national security and interests, determined in accordance with legal procedures, and only known to a certain range of persons within a certain period of time.

Article 3 State secrets are protected by law.

All state organs, armed forces, political parties, social organizations, enterprises, institutions and citizens have the obligation to keep state secrets.

Any acts that endanger the security of state secrets must be prosecuted by law.

Article 4 The work of keeping state secrets (hereinafter referred to as “secrecy work”) follows the policy of active prevention, highlighting key points, and lawful management, which not only ensures the security of state secrets, but also facilitates the rational use of information resources.

Matters that are required to be disclosed by laws and administrative regulations shall be disclosed in accordance with the law.

Article 5 The state administrative department for secrecy is in charge of secrecy work nationwide. Local secrecy administrative departments at or above the county level shall be in charge of the secrecy work in their respective administrative regions.

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

Central state organs, within the scope of their functions and powers, manage or guide the confidentiality work of the system.

Article 7: Organs and units shall implement a confidentiality work responsibility system, improve confidentiality management systems, improve

confidentiality protection measures, carry out confidentiality publicity and education, and strengthen confidentiality inspections.

Article 8 The state shall reward units or individuals that have made outstanding achievements in keeping and protecting state secrets and improving secrecy technologies and measures.

Chapter II Scope and Class of State Secrets

Article 9 The following matters involving national security and interests, which may damage the country's security and interests in the fields of politics, economy, national defense, diplomacy, etc., shall be determined as state secrets:

- (1) Secret matters in major decision-making on state affairs ;
- (2) Secret matters in national defense construction and armed forces activities;
- (3) Secret matters in diplomatic and foreign affairs activities and secret matters that are obliged to keep secret;
- (4) Secret matters in national economic and social development;
- (5)) secret matters in science and technology;
- (6) secret matters in safeguarding national security activities and investigating criminal crimes;
- (7) other secret matters determined by the state administrative department for secrecy.

The secret matters of political parties that meet the provisions of the preceding paragraph are state secrets.

Article 10 State secrets are classified into three levels: top secret, secret and secret.

Top-secret state secrets are the most important state secrets, and their disclosure will cause particularly serious damage to national security and interests; top-secret state secrets are important state secrets, and their disclosure will cause serious damage to national security and interests; secret-level state secrets It is a general state secret, and its disclosure will damage national security and interests.

Article 11 The specific scope of state secrets and their classification levels shall be prescribed by the state secrets administration department in conjunction with the foreign affairs, public security, national security and

other relevant central authorities.

The specific scope of military state secrets and their classification levels shall be prescribed by the Central Military Commission.

The provisions on the specific scope of state secrets and their classification levels shall be announced within the relevant scope and adjusted in a timely manner according to changes in the situation.

Article 12 The person in charge of an organ or unit and the person designated by it shall be the person responsible for classification and shall be responsible for the determination, modification and removal of state secrets of the organ or unit.

When an organ or unit determines, changes or removes its own state secrets, the undertaker shall put forward specific opinions, which shall be reviewed and approved by the person responsible for classification.

Article 13 When determining the classification level of state secrets, the authority for classification shall be abided by.

Central state organs, provincial organs and their authorized organs and units may determine top secret, secret and secret state secrets; organs at the level of districted cities and autonomous prefectures and their authorized organs and units may determine secret and secret state secrets. level state secrets. The specific classification authority and scope of authorization shall be stipulated by the state secrecy administrative department.

Organs and units that implement state secret matters determined by their superiors and need to be classified shall be determined according to the classification level of the state secret matters they execute. A lower-level organ or unit believes that the classification-related matters generated by this organ or unit are within the authority of the higher-level organ or unit, and should take security measures first, and immediately report it to the higher-level organ or unit for confirmation; if there is no higher-level organ or unit, it should immediately It shall be submitted to the competent business department or the confidentiality administrative department with the corresponding authority for classification.

The public security and state security organs shall, within the scope of their work, determine the classification level of state secrets within the scope of their work.

Article 14: Organs and units shall determine the level of state secrets in accordance with the regulations on the specific scope of state secrets and their level of state secrets, and at the same time determine the duration of confidentiality and the scope of knowledge.

Article 15: The confidentiality period of state secrets shall be limited to a necessary period according to the nature and characteristics of the matter and the needs of safeguarding national security and interests; if the period cannot be determined, the conditions for declassification shall be determined.

Unless otherwise stipulated, the confidentiality period of state secrets shall not exceed 30 years at the top secret level, 20 years at the secret level and 10 years at the secret level.

Organs and units shall determine the specific confidentiality period, decryption time or decryption conditions according to the needs of the work.

If an organ or unit decides to disclose a matter that needs to be kept secret in the process of deciding and handling relevant matters, it will be deemed to be declassified when it is officially announced.

Article 16 The scope of knowledge of state secrets shall be limited to the minimum scope according to the needs of the work.

If the scope of knowledge of state secrets can be limited to specific personnel, it is limited to specific personnel; if it cannot be limited to specific personnel, it is limited to organs and units, and organs and units are limited to specific personnel.

Persons outside the scope of knowledge of state secrets who need to know state secrets for work shall obtain approval from the person in charge of the organ or unit.

Article 17: Organs and units shall make state secret marks on paper media, optical media, electromagnetic media and other carriers that carry state secrets (hereinafter referred to as state secret carriers), as well as equipment and products that are state secrets.

If it is not a state secret, it should not be marked as a state secret.

Article 18: The classification level, confidentiality period, and scope of knowledge of state secrets shall be changed in a timely manner according to changes in circumstances. Changes to the secrecy level, confidentiality period, and scope of knowledge of state secrets shall be decided by the

original secrecy organization or unit, or by its higher-level organization.

When the classification level, confidentiality period and scope of knowledge of state secrets are changed, the organs, units or persons within the scope of knowledge shall be notified in writing in a timely manner.

Article 19: State secrets shall be decrypted by themselves if the period of confidentiality has expired.

Organs and units shall regularly review the determined state secrets. Those that are no longer classified as state secrets due to the adjustment of the scope of confidential matters within the confidentiality period, or the disclosure will not harm national security and interests, and do not need to continue to be kept confidential, they shall be declassified in a timely manner; if the confidentiality period needs to be extended, it shall be before the expiration of the original confidentiality period. Redefine the confidentiality period. Declassification in advance or extension of the confidentiality period shall be decided by the original classification organ or unit, and may also be decided by the higher-level organ.

Article 20 : Where an organ or unit is unclear or has disputes as to whether it is a state secret or what classification it belongs to, it shall be determined by the state secrecy administrative department or the secrecy administrative department of a province, autonomous region, or municipality directly under the Central Government.

Chapter III Confidentiality System

Article 21 : The production, dispatch, transmission, use, reproduction, preservation, maintenance and destruction of state secret carriers shall comply with state secrets regulations.

Top-secret-level state secret carriers shall be kept in facilities and equipment that meet the state's secrecy standards, and shall be managed by a designated person; no copying or excerpting is allowed without the approval of the original secrecy-classifying organ, unit, or its higher-level organ; Designate personnel to be responsible and take necessary safety measures.

Article 22 The development, production, transportation, use, preservation, maintenance and destruction of equipment and products that are state secrets shall comply with state secrets regulations.

Article 23 The computer information system that stores and handles

state secrets (hereinafter referred to as the “secret-related information system”) shall be protected by grades according to the degree of confidentiality.

Secret-related information systems shall be equipped with secret-guarding facilities and equipment in accordance with national secret-guarding standards. Secrecy facilities and equipment shall be planned, constructed and operated synchronously with the classified information system.

The classified information system shall be put into use only after passing the inspection according to the regulations.

Article 24 : Organs and units shall strengthen the management of secret-related information systems, and no organization or individual shall do the following:

(1) Connect secret-related computers and secret-related storage devices to the Internet and other public information networks;

(2) Exchange information between classified information systems and the Internet and other public information networks without taking protective measures;

(3) Use non-classified computers and non-classified storage devices to store and process state secret information;

(4) Uninstalling or modifying the security technology programs and management programs of the classified information system without authorization

;

Article 25 : Organs and units shall strengthen the management of state secret carriers, and no organization or individual shall conduct the following acts:

(1) Illegal acquisition and possession of state secret carriers;

(2) Buying, selling, forwarding or privately destroying state secret carriers;

(3) Transmitting state secret carriers through ordinary postal, express delivery and other channels without security measures;

(4) Mailing or consignment (5) Carrying or passing the state secret carrier out

of the country without the approval of the relevant competent authorities.

Article 26 It is prohibited to illegally reproduce, record and store state secrets.

It is forbidden to transmit state secrets in the Internet and other public information networks or in wired and wireless communications without security measures.

Involvement of state secrets in personal interactions and correspondence is prohibited.

Article 27 The editing, publishing, printing and distribution of newspapers, books, audio-visual products and electronic publications; the production and broadcasting of radio programs, television programs and movies; The editing and publishing of information shall abide by the relevant confidentiality regulations.

Article 28 Internet and other public information network operators and service providers shall cooperate with public security organs, state security organs, and procuratorial organs to investigate cases of leakage of secrets; if it is found that the information released by the use of the Internet and other public information networks involves leakage of state secrets, The transmission shall be stopped immediately, relevant records shall be kept, and reports shall be made to the public security organs, state security organs or secrecy administrative departments; information involving the disclosure of state secrets shall be deleted according to the requirements of the public security organs, state security organs or secrecy administrative departments.

Article 29 When organs and units publicly release information and purchase projects, goods and services involving state secrets, they shall abide by the confidentiality regulations.

Article 30 If an organ or unit needs to provide state secrets in its foreign exchanges and cooperation, or if the foreign personnel appointed or hired need to know state secrets due to their work, they shall report to the relevant competent department of the State Council or the relevant competent department of the people's government of a province, autonomous region or municipality directly under the Central Government. Approved and signed a non-disclosure agreement with the other party.

Article 31 Where state secrets are involved in holding a conference or other activities, the sponsoring unit shall take confidentiality measures,

conduct confidentiality education for the participants, and put forward specific confidentiality requirements.

Article 32: Organs and units shall identify institutions that involve top-secret or more secret or secret-level state secrets as key secrecy departments, and special places for centralized production, storage and custody of state secret carriers as key secrecy departments, Equip and use necessary technical protection facilities and equipment in accordance with national confidentiality regulations and standards.

Article 33: Military restricted areas and other places and parts that are state secrets and not open to the outside world shall take measures to keep them secret, and without the approval of the relevant departments, no decision shall be made to open to the outside world or expand the scope of opening.

Article 34: Enterprises and institutions that engage in the production, reproduction, maintenance, and destruction of state secret carriers, the integration of classified information systems, or the scientific research and production of weapons and equipment, and other businesses that involve state secrets, shall undergo a confidentiality review, and the specific measures shall be prescribed by the State Council.

Organs and units entrusting enterprises and institutions to engage in the business specified in the preceding paragraph shall sign a confidentiality agreement with them, put forward confidentiality requirements, and take confidentiality measures.

Article 35 Personnel working in secret-related positions (hereinafter referred to as secret-related personnel) are classified into core secret-related personnel, important secret-related personnel, and general secret-related personnel according to the degree of secret-related involvement, and are subject to classified management.

The appointment and employment of secret-related personnel shall be reviewed in accordance with relevant regulations.

Personnel involved in secrets shall have good political quality and conduct, and have the ability to be competent for the jobs required by secrets.

The legitimate rights and interests of personnel involved in secrets are protected by law.

Article 36 Personnel involved in secrets shall go through confidentiality education and training, master confidentiality knowledge and skills, sign confidentiality commitments, strictly abide by confidentiality rules and regulations, and shall not disclose state secrets in any way.

Article 37 The departure of secret-related personnel shall be approved by the relevant departments. If the relevant organs believe that the departure of secret-related personnel will cause harm to national security or cause heavy losses to national interests, the exit shall not be approved.

Article 38 The secret-disclosure period management shall be implemented for personnel involved in secrets who leave their posts and leave their posts. During the period of declassification, personnel involved in secrets shall perform their confidentiality obligations in accordance with regulations, shall not violate the regulations for employment, and shall not disclose state secrets in any way.

Article 39: Organs and units shall establish and improve the management system for secret-related personnel, clarify the rights, post responsibilities and requirements of secret-related personnel, and conduct regular supervision and inspection of the performance of duties by secret-related personnel.

Article 40 : When state functionaries or other citizens discover that state secrets have been leaked or may be leaked, they shall immediately take remedial measures and report to relevant organs and units in a timely manner. After receiving the report, the organ or unit shall deal with it immediately and report it to the secrecy administrative department in a timely manner.

Chapter IV Supervision and Management

Article 41 : The state secrecy administrative department shall formulate secrecy rules and national secrecy standards in accordance with the provisions of laws and administrative regulations.

Article 42: The secrecy administrative department shall organize and carry out secrecy publicity and education, secrecy inspection, secrecy technology protection, and investigation and handling of leaked cases in accordance with the law, and guide and supervise the secrecy work of organs and units.

Article 43: Where the secrecy administrative department finds that the

determination, modification or removal of state secrets is improper, it shall promptly notify the relevant organs and units to make corrections.

Article 44: The secrecy administrative department shall inspect the compliance of organs and units with the secrecy system, and the relevant organs and units shall cooperate. If the secrecy administrative department finds that an organ or unit has hidden dangers of leaking secrets, it shall require it to take measures and make rectification within a time limit; for facilities, equipment, and places with hidden dangers of leaking secrets, it shall order it to stop using; Relevant organs and units shall impose sanctions and be transferred from secret-related positions; if they are found to be suspected of leaking state secrets, they shall urge and guide relevant organs and units to investigate and deal with them. Those suspected of committing a crime shall be transferred to judicial organs for handling.

Article 45: The secrecy administrative department shall confiscate the carriers of state secrets illegally obtained or held during secrecy inspections.

Article 46: Where an organ handling a case suspected of divulging state secrets needs to conduct appraisal on whether the relevant matter is a state secret and what classification it belongs to, the appraisal shall be conducted by the state administrative department for secrecy or the administrative department for secrecy of a province, autonomous region, or municipality directly under the Central Government.

Article 47 If an organ or unit fails to impose sanctions on persons who violate the confidentiality provisions, the administrative department for confidentiality shall suggest corrections, and if it refuses to make corrections, it shall be submitted to the higher-level organ or supervisory organ to be held accountable by the organ or unit. The responsible leaders and directly responsible personnel shall be dealt with in accordance with the law.

Chapter V Legal Liability

Article 48 Anyone who violates the provisions of this Law and commits any of the following acts shall be punished according to law; if a crime is constituted, criminal responsibility shall be investigated according to law:

(1) Illegal acquisition or

possession of state secret carriers;

Destroying the carrier of state secrets without permission;

(3) Passing the carrier of state secrets through ordinary post, express delivery and other channels without security measures;

(4) Posting or consigning the carrier of state secrets out of the country, or carrying or delivering the carrier of state secrets without the approval of the relevant competent authorities

(5) Illegal copying, recording and storage of state secrets; (

6) State secrets are involved in private exchanges and communications;

(7) Wired and unsecured Internet or other public information networks or without security measures. Passing state secrets in wireless communication;

(8) Connecting secret-related computers and secret-related storage devices to

the Internet and other public information networks; (10) Using non-confidential computers or non-confidential storage devices to store and process state secret information;

(11) Uninstalling or modifying security technical procedures, (12)

Giving away, selling, discarding, or repurposing classified computers or storage devices that have been withdrawn from use without security technology

treatment for other purposes. Those who have committed the acts in the

preceding paragraph that do not constitute a crime and are not subject to

punishment, shall be supervised by the administrative department of

confidentiality to urge their organs and units to deal with them. Article

49: Where an organ or unit violates the provisions of this Law and has a

major case of leaking secrets, the relevant organ or unit shall impose

sanctions on the directly responsible person in charge and other directly

responsible personnel in accordance with the law; for those who do not apply

the sanctions, the secrecy administrative department shall Urge its competent

authorities to deal with it.

If an organ or unit violates the provisions of this Law by not

classifying the matters that should be classified, or classifying the matters that should not be classified, causing serious consequences, the relevant organs or units shall, in accordance with the law, take responsibility for the directly responsible person in charge and other directly responsible personnel. Punishment.

Article 50 : Internet and other public information network operators and service providers that violate the provisions of Article 28 of this Law shall be punished according to law by public security organs or state security organs, and competent departments of the information industry according to their respective responsibilities.

Article 51 : Where staff members of the secrecy administrative department abuse their powers, neglect their duties, or practice favoritism and fraud in the performance of secrecy management duties, they shall be punished according to law; if a crime is constituted, they shall be investigated for criminal responsibility according to law.

Chapter VI Supplementary Provisions

Article 52 The Central Military Commission formulates the Confidentiality Regulations of the Chinese People's Liberation Army in accordance with this Law.

Article 53 This Law shall come into force on October 1, 2010.

[【E-mail
recommendation](#)

】 [【Error Correction】](#)

Copyright©2013 www.gov.cn
All Rights Reserved

Copyright: China Government Network