Democratic People's Republic of Korea

State Secret Protection Law

Adopted by Decree No. 1215 of the Standing Committee of the Supreme People's Assembly on February 2, 2023

Amended by Decree No. 1665 of the Standing Committee of the Supreme People's Assembly on June 11, 2024

Chapter 1: Basics of the State Secret Protection Law

Article 1 (Mission of the State Secret Protection Law) The State Secret Protection Law of the Democratic People's Republic of Korea contributes to ensuring the safety and interests of the state and the successful advancement of socialist construction by strictly establishing systems and order in the state secret protection business.

Article 2 (Definition of State Secret) A state secret refers to content related to the safety and interests of the state, which is known only to a certain range of people within a specified period.

Article 3 (State Secret Objects) State secret objects include paper, optical media, electronic media, or equipment, products, and materials containing secret content.

Article 4 (Principles for Determining the Scope and Grades of State Secrets) Determining the scope and grades of state secrets is a priority process in the state secret protection business. The state shall determine the scope and grades of state secrets based on the principle of ensuring the safety and interests of the state.

Article 5 (Principles for Establishing the State Secret Protection Management System) Establishing the state secret protection management system is an important requirement of the state secret protection business. The state shall establish the state secret protection management system based on the principle of responsibility by sector, region, and unit.

Article 6 (Principles for Voluntary Compliance with State Secret Protection) Protecting state secrets is the duty of institutions, enterprises, organizations, and citizens. The state shall strengthen education among citizens to ensure their voluntary participation in the state secret protection business.

Article 7 (Application of Relevant Regulations) Matters not regulated by this law regarding state secret protection shall be governed by relevant regulations.

Chapter 2: Content and Grades of State Secrets

Article 8 (Content of State Secrets) State secrets include content related to the safety and interests of the state, such as:

1. Content related to the safety of our supreme leadership
2. Content related to the execution of party and state policies
3. Content related to military and munitions sectors
4. Content related to national defense sectors
5. Content related to national diplomacy
6. Content related to science and technology
7. Content related to codes for secret protection
8. Statistical data
9. Content related to the formation and management of strategic reserves
10. Content related to foreign economy
11. Content related to criminal cases
12. Content designated as state secrets by relevant authorities

Article 9 (Grades of State Secrets) State secrets are classified into top secret, absolute secret, and secret based on their importance.

Article 10 (Top Secret) Top secret is the highest grade of state secret, which, if leaked, can create extremely serious risks to the safety and interests of the state. Top secret includes extremely important data related to the safety of our supreme leadership, military, munitions, diplomacy, major policy execution, important science and technology, transformation codes, national statistics, and other data of utmost significance for national security and strategic implementation.

Article 11 (Absolute Secret) Absolute secret is a high-grade state secret related to the safety and interests of the state. Absolute secret includes data that, while not top secret, is of significant importance for national security and strategic implementation and must not be disclosed beyond the permitted range.

Article 12 (Secret) Secret is a lower-grade state secret related to the safety and interests of the state. Secret includes data that, while not top secret or absolute secret, must not be disclosed beyond the permitted range.

Article 13 (Marking of State Secrets) Paper, optical media, memory media, and equipment, materials, and products containing state secrets shall be marked according to their grades.

Article 14 (Selection of Grades, Users, and Protection Periods for State Secrets) The unit that designates the object as a state secret shall select the grade, users, and protection period of the state secret. The unit shall determine the grade, users, and protection period of the state secret from the perspective of ensuring the safety and interests of the state.

Article 15 (Confirmation of State Secret Grades) State secret grades shall be determined according to Articles 10, 11, and 12 of this law. If necessary, the grades of state secrets may be determined in agreement with the higher authorities of the relevant sector or region or the relevant authorities.

Article 16 (Determination of State Secret Users) The range of users of state secrets shall be determined as a very limited number of members who need to know the state secrets for their tasks. If the range of users cannot be determined as specific members, it shall be determined as units, and the units shall determine the specific members.

Article 17 (Designation of State Secret Protection Periods) State secrets shall be protected for 50 years for top secret, 30 years for absolute secret, and 10 years for secret according to their grades. If the protection period of state secrets cannot be determined, they may be designated as conditions for declassification.

Article 18 (Change of State Secret Users and Protection Periods) Changes in state secret users and protection periods shall be made by the unit that designated the state secret. If the state secret can be disclosed within the protection period without harming the safety and interests of the state, the secret shall be declassified, and if the protection period needs to be extended, the new protection period shall be determined before the end of the current protection period.

Chapter 3: Protection and Management of State Secret Objects

Article 19 (Registration of State Secret Objects) State secrets shall be registered as top secret, absolute secret, and secret. Depending on the importance of the business, items such as business notebooks used by personnel utilizing state secret objects shall also be registered. Specific matters related to the dispatch, receipt, and registration of state secret objects shall be governed by relevant regulations.

Article 20 (Prohibited Acts in Handling State Secret Objects) The following acts are prohibited in handling state secret objects:

1. Disseminating or illegally acquiring or possessing state secret objects
2. Recording, duplicating, copying, storing, viewing, or watching without approval
3. Selling or destroying or deleting without approval
4. Transmitting or dispatching through routes without secret protection measures
5. Taking state secret objects outside the borders without approval

Article 21 (Secret Management Departments and Secret Management Personnel) The dispatch, receipt, registration, and storage of state secret objects shall be handled by the department or personnel managing state secret objects. Institutions, enterprises, and organizations shall determine management personnel by grade and strictly comply with the established order in managing state secret objects to prevent the leakage of state secrets.

Article 22 (Storage Facilities and Locations for State Secret Objects) Storage facilities and locations for state secret objects shall be installed and arranged according to the grades of state secrets. Only designated personnel shall have access to the storage locations of state secret objects.

Article 23 (Protection Measures for State Secret Protection Zones) State secret protection zones, such as military restricted areas and places and regions not open to the public, shall have secret protection measures. Without the approval of the relevant authorities, state secret protection zones shall not be opened or expanded.

Article 24 (Secret Protection Measures for Equipment, Products, and Materials) When researching, producing, utilizing, transporting, or disposing of equipment, products, and materials containing state secrets, it shall be done in accordance with the requirements of relevant regulations.

Article 25 (Operation and Utilization of State Secret Handling Information Systems) State secret handling information systems shall be operated and utilized according to the security standards set for the grades of state secrets. Equipment used in state secret handling information systems shall be inspected according to the set standards. Security and management programs of state secret handling information systems shall not be deleted or changed without approval.

Article 26 (Secret Protection in Handling Data through State Secret Handling Information Systems) Secret protection measures shall be established for data transmitted through state secret handling information systems.

Article 27 (Prohibited Acts in Operating and Utilizing Computers and Memory Media for State Secret Handling) The following acts are prohibited in operating and utilizing computers and memory media for state secret handling:

1. Connecting computers and memory media for state secret handling to general information networks
2. Storing or processing state secrets on computers and memory media not designated for state secret handling
3. Failing to handle the storage, transfer, disposal, and destruction of computers for state secret handling according to the set standards

Article 28 (Ensuring State Secrets in Meetings or Gatherings) Institutions, enterprises, and organizations shall determine participants in advance when conducting meetings or gatherings to convey or discuss content related to state secrets. Participants shall strictly comply with the state secrets handled in meetings or gatherings. Participants in meetings or gatherings discussing important state secrets shall not carry devices capable of photography, recording, or transmitting data without approval.

Article 29 (Prohibition of Exhibiting Products, Inventions, and Papers Containing State Secrets) Products, inventions, papers, and statistical data containing state secrets shall not be exhibited at exhibitions, academic discussions, or other events without approval.

Article 30 (Organization and Binding of State Secret Documents) Institutions, enterprises, and organizations shall annually organize and bind state secret documents to be stored in national document facilities, provincial (directly governed city), city (district), county document facilities, and document facilities of institutions, enterprises, and organizations. When organizing and binding state secret documents to be stored in the national document repository, it shall be done by designated units.

Article 31 (Inspection of State Secret Documents) Institutions, enterprises, and organizations shall periodically inspect state secret documents they store or use. State secret documents whose protection period has expired and documents used by units shall be processed according to the set procedures.

Article 32 (Handling of Secret Documents by Transferred, Dismissed, Retired, and Socially Secured Personnel) Institutions, enterprises, and organizations shall retrieve and process documents containing state secrets used by personnel who are transferred, dismissed, retired, or socially secured according to the set standards.

Article 33 (Transfer and Receipt of State Secret Protection Objects) The transfer and receipt of state secret protection objects shall be done by verifying and checking the

objects between units or personnel. Institutions, enterprises, and organizations that are dissolved or split shall transfer state secret protection objects to the unit responsible for related business, or if there is no unit, to the higher authorities.

Article 34 (Viewing Important State Secret Documents) Viewing important state secret documents shall be done only at designated locations by designated personnel.

Article 35 (Carrying State Secret Objects) When carrying state secret objects outside the unit, personnel shall obtain the relevant certification documents from the authorized institution. Personnel carrying state secret objects shall establish safety measures for state secret protection.

Article 36 (Protection of State Secrets in Literary and Artistic Works and Publications) When editing, printing, producing, publishing, or distributing various publications such as newspapers, magazines, books, sound broadcasts, TV broadcasts, and films, institutions, enterprises, and organizations shall comply with relevant regulations to prevent the leakage of state secrets.

Article 37 (Protection of State Secrets in National Networks and Information Technology Services) Units conducting information services using national networks shall stop data transmission and preserve relevant data if they discover state secret leakage during operation, and immediately notify the relevant institutions such as social security agencies and national defense agencies. Information technology service units shall not print or copy data containing state secrets.

Article 38 (Protection of State Secrets in Business Processes) Personnel conducting on-site inspections, audits, and supervision of institutions, enterprises, and organizations shall strictly comply with the state secrets they learn during their business processes and shall not request data unrelated to current business.

Article 39 (Protection of State Secrets in Foreign Affairs) Institutions, enterprises, organizations, and citizens shall ensure that state secrets are not leaked during foreign affairs. If it is necessary to use content containing state secrets due to the nature of foreign affairs, approval from the relevant institution shall be obtained, and an agreement on secret protection shall be made with the counterpart.

Article 40 (Reporting State Secret Leakage) Institutions, enterprises, organizations, and citizens shall establish preventive measures and promptly report to relevant institutions such as social security agencies and national defense agencies if state secrets are leaked or likely to be leaked. Institutions, enterprises, organizations, and citizens shall actively cooperate with the investigations of relevant institutions.

Chapter 4: Guidance and Control of State Secret Protection Business

Article 41 (Guidance of State Secret Protection Business) Guidance of the state secret protection business shall be conducted by the relevant central institution. The central institution shall regularly grasp and guide the state secret protection business of subordinate units.

Article 42 (Organization of State Secret Protection Business) Institutions, enterprises, and organizations shall establish systems to ensure state secrets are not leaked in their sectors, regions, and units. Units utilizing and managing state secret protection objects shall formulate detailed rules or regulations related to state secret protection and regularly understand and address compliance.

Article 43 (Supervision and Control of State Secret Protection Business) Supervision and control of state secret protection shall be conducted by the relevant supervision and control institution. The supervision and control institution shall regularly supervise and control institutions, enterprises, organizations, and citizens to ensure strict compliance with state secrets.

Article 44 (Measures for Secret Leakage Elements) If the supervision and control institution discovers elements that may lead to state secret leakage during supervision, it shall establish relevant protection measures. Objects containing illegally acquired state secrets shall be confiscated.

Article 45 (Warnings, Severe Warnings, Unpaid Labor, Labor Education, Demotion, Dismissal, and Removal) The following cases shall result in warnings, severe warnings, or punishment of unpaid labor for up to three months, labor education, demotion, dismissal, or removal:

1. Failure to determine the grade, user range, and protection period of state secrets from the perspective of ensuring the safety and interests of the state
2. Failure to dispatch, receive, and register state secret objects according to the set standards
3. Engaging in acts prohibited by Article 20
4. Failure to equip storage locations and facilities for state secret objects according to regulations
5. Failure to research, produce, utilize, transport, and dispose of equipment, products, and materials containing state secrets according to the requirements of regulations

6. Failure to operate and utilize state secret handling information systems according to set security standards
7. Violating the order of conveying and discussing content containing state secrets
8. Exhibiting objects containing state secrets at exhibitions, academic discussions, or other events without approval
9. Failure to organize, bind, and inspect state secret documents according to set standards
10. Failure to retrieve and process secret documents used by transferred, dismissed, retired, and socially secured personnel according to set standards
11. Failure to register, utilize, carry, dispose of, and destroy computers and memory media for secret handling according to set standards
12. Failure to comply with the order related to state secret protection in handling literary and artistic works and publications
13. Failure to comply with the order related to state secret protection in foreign affairs
14. Failure to establish preventive measures or promptly report state secret leakage or potential leakage
15. Leaking state secrets or losing state secret objects

Repeated violations of the above acts shall result in unpaid labor for more than three months, labor education, demotion, dismissal, or removal.

Article 46 (Criminal Responsibility) If acts violating this law reach the level of a crime, the responsible person shall bear criminal responsibility according to the relevant provisions of the criminal law.