ACT ON THE PROMOTION OF INFORMATION SECURITY INDUSTRY

[Enforcement Date 10. Jul, 2024.] [Act No.19990, 09. Jan, 2024., Amendment by Other Act]

과학기술정보통신부 (정보보호기획과)044-202-6448

ACT ON THE PROMOTION OF INFORMATION SECURITY INDUSTRY

[Enforcement Date 10. Jul, 2024.] [Act No.19990, 09. Jan, 2024., Amendment by Other Act]
과학기술정보통신부 (정보보호기획과) 044-202-6448
과학기술정보통신부 (정보보호산업과) 044-202-6453, 6452

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose) The purpose of this Act is to create infrastructure for the information security industry by providing for matters necessary for promoting the information security industry; and to contribute to creating the environment in which people can use information and communications safely, and to soundly developing the national economy by strengthening the competitiveness of the information security industry.

Article 2 (Definitions) (1) The terms used in this Act are defined as follows:

1. The term "information security" means establishing managerial, technological and physical means (hereinafter referred to as "information security system") for the following activities:
   (a) Preventing the destruction, modification, leakage, etc., of information which may occur while collecting, processing, storing, searching for, transmitting and receiving information, and recovering information;
   (b) Responding to accidents, disasters, crimes, etc. by utilizing security technology, such as cryptography, authentication, identification, and surveillance, or operating related equipment and facilities safely;
2. The term "information security industry" means the industry that develops, manufactures or distributes technology for information security (hereinafter referred to as "information security technology") and products to which information security technology applies (hereinafter referred to as "information security products"); or provides services related thereto (hereinafter referred to as "information security services");
3. The term "information security enterprise" means a person who conducts economic activities related to the information security industry (hereinafter referred to as "information security business");
4. The term "user" means a person who uses information security technology, information security products and information security services (hereinafter referred to as

"information security technology, etc.") provided by an information security enterprise;

5. The term "public institutions" means the following institutions:
   (a) Corporations, organizations or institutions established under Article 4 of the Act on the Management of Public Institutions;
   (b) Local public corporations and local industrial complexes established under the Local Public Enterprises Act;
   (c) Special corporations incorporated pursuant to special statutes;
   (d) Other corporations, organizations and institutions prescribed by Presidential Decree;
6. The term "evaluation of the level of information security preparedness" means evaluating the level of information security preparedness of enterprises and allocating a specific rating accordingly.

(2) Except as provided in paragraph (1), such statutes as the Framework Act on Intelligent Informatization; the Act on Promotion of Information and Communications Network Utilization and Information Protection; the Information and Communications Technology Industry Promotion Act; the Framework Act on Telecommunications; the Telecommunications Business Act; the Framework Act on Broadcasting Communications Development; the Internet Multimedia Broadcast Services Act shall apply to the definitions of the terms used in this Act. <Amended on Jun. 9, 2020>

Article 3 (Responsibility of the State and local governments) The State and local governments shall formulate and implement policies necessary to promote the information security industry, and prepare a plan to secure funds necessary therefor.

Article 4 (Relationship to other statutes) Except as otherwise expressly provided for in other statutes, the information security industry shall be governed by this Act.

Article 5 (Formulation of plan for promotion of information security industry) (1) The Minister of Science and ICT shall formulate and implement a plan for promoting the information security industry (hereinafter referred to as "promotion plan"), including the following, to set goals and directions for policies concerning the promotion of the information security industry: <Amended on Jul. 26, 2017; Jan. 9, 2024>

1. Matters concerning the basic direction-setting for policies to promote the information security industry;

2. Matters concerning creating infrastructure, such as training information security professionals, developing patented technology, and proliferating the use of information security services;
3. Matters concerning standardizing information security technology, etc., and protecting intellectual property rights;
4. Matters concerning nurturing and supporting information security enterprises;
5. Matters concerning providing support to strengthen the competitiveness of small and medium enterprises prescribed in Article 2 (1) of the Framework Act on Small and Medium Enterprises, venture businesses prescribed in Article 2 (1) of the Special Act on the Promotion of Venture Businesses, and self-employed creative enterprises prescribed in Article 2 of the Act on the Fostering of Self-Employed Creative Enterprises (hereinafter referred to as "small and medium-sized enterprises, etc.") with respect to information security;
6. Matters concerning information security policies based on developing convergence between the information security industry and other industries;
7. Matters concerning creating an environment for fair competition for the information security industry;
8. Matters concerning protecting rights and interests of users;
9. Matters concerning support for international cooperation and overseas expansion concerning the information security industry;
10. Matters concerning raising and allocating funds for promoting the information security industry;
11. Matters concerning improving laws and systems for promoting the information security industry;
12. Matters concerning business cooperation and coordination among central administrative agencies related to the information security industry;
13. Matters concerning linkages with a master plan referred to in Article 5 of the Special Act on Promotion of Information and Communications Technology and Vitalization of Convergence Thereof;
14. Other matters necessary to promote the information security industry.

(2) A promotion plan shall be formulated every five years, and the cycle of formulation may change where necessary.

(3) The Minister of Science and ICT may request the heads of related central administrative agencies, local governments and related public institutions to provide a plan or data in each competent field, to formulate a promotion plan. In such cases, agencies and institutions so requested shall comply in the absence of special circumstances. <Amended on Jul. 26, 2017>

(4) Other matters necessary to formulate, implement, etc. promotion plans shall be prescribed by Presidential Decree.

CHAPTER II REVITALIZATION OF INFORMATION SECURITY INDUSTRY

Article 6 (Provision of information on purchase demand) (1) The head of each administrative agency or public institution prescribed in subparagraph 2 of Article 2 of the Electronic Government Act (hereinafter referred to as "public institution, etc.") shall submit information on purchase demand (hereafter referred to as "information on purchase demand" in this Article) for information security technology, etc. to the Minister of Science and ICT annually to strengthen the information security level of the competent agency or institution. <Amended on Jul. 26, 2017>

(2) The Minister of Science and ICT may provide information security enterprises with information on purchase demand submitted pursuant to paragraph (1). <Amended on Jul. 26, 2017>

(3) Where the Minister of Science and ICT provides information security enterprises with information on purchase demand pursuant to paragraph (2), he or she shall convene meetings of a special deliberative committee within the Ministry Science and ICT to prevent information that has a significant impact on the national security and public interests from being provided to information security enterprises. <Amended on Jul. 26, 2017>

(4) Necessary matters concerning the specific number of times, period, methods, procedures, etc. for submitting and providing information on purchase demand under paragraphs (1) and (2) shall be prescribed by Presidential Decree.

Article 7 (Contract, etc. for establishment of information security system of public institutions) (1) Where the head of a public institution, etc. enters into a contract on a project for establishing an information security system, he or she shall enter into the contract

preferentially whereby a bidder prescribed in Article 10 (2) 3 of the Act on Contracts to Which the State Is a Party and Article 13 (2) 4 of the Act on Contracts to Which a Local Government Is a Party is selected as a successful bidder; provided, where it is deemed necessary in light of the characteristics of the information security system for which a contract is to be concluded, he or she may enter into the contract by other methods.

(2) The Minister of Science and ICT may determine criteria that may analyze and apply requirements for an information security system to enter into a contract under paragraph (1) and criteria for technical evaluation to select a business entity of the information security system. <Amended on Jul. 26, 2017>

(3) Where the head of a public institution, etc. enters into a contract for a project under paragraph (1) or conducts a technical evaluation to select a business entity, the Minister of Science and ICT may recommend him or her to apply criteria referred to in paragraph (2). <Amended on Jul. 26, 2017>

(4) The Minister of Science and ICT shall prescribe and publicly notify detailed procedures and criteria for contracting under paragraphs (1) through (3). <Amended on Jul. 26, 2017>

Article 8 (Approval of subcontracting) (1) Where an information security enterprise which has entered into a contract for a project to establish an information security system with a public institution, etc. intends to subcontract all or part of the project to another information security enterprise; or its subcontractor intends to again subcontract the work already subcontracted, the information security enterprise and the other information security enterprise shall obtain prior written approval from the head of the public institution, etc., respectively.

(2) Necessary matters concerning procedures, etc. for approval under paragraph (1) shall be prescribed by Decree of the Ministry of Science and ICT. <Amended on Jul. 26, 2017>

Article 9 (Defects warranty for information security system) (1) Where an information security enterprise has entered into a contract for a project to establish an information security system with a public institution, etc., it shall be liable to warranty any defects which arise within one year from the date it completes the project (referring to the date it delivers the final product after conducting tests and inspections on the project).

(2) Notwithstanding paragraph (1), no information security enterprise shall be liable to warranty defects which arise due to any of the following reasons; provided, the foregoing shall not apply where it fails to notify a person placing an order even though it is aware

that the goods provided by the person placing an order or his or her instructions are inappropriate:

1. Where the quality or standard of the goods provided by the person placing an order fails to meet the criteria referred to in Article 7 (2);
2. Where the information security enterprise has established the information security system in accordance with the instructions by the person placing an order;
3. Where the person placing an order causes a defect intentionally or negligently.

Article 10 (Price for information security products and information security services) (1) Where a public institution, etc. enters into a contract for an information security project, it shall endeavor to pay a reasonable price for the development of the information security industry and the quality assurance of information security products and information security services.

(2) Where a person placing an order falls under any of the following cases, the Minister of Science and ICT may conduct an investigation through public-private partnership monitoring, and disclose the result thereof or request the relevant person placing an order to take corrective action so that the practices for placing orders may be established reasonably: <Amended on Jul. 26, 2017>

1. Where the person violates any provision of this Act or other statutes in relation to placing an order for an information security project;
2. Where the person demands unreasonably low prices or long-term maintenance and management and maintenance of security performance compared to the ordinary business practices.

(3) The Minister of Science and ICT may prepare a standard-form contract through consultation with the Fair Trade Commission, and recommend public institutions, etc. to use such standard form contract for reasonable distribution and fair transactions in the information security industry. <Amended on Jul. 26, 2017>

(4) The Minister of Science and ICT may collect and analyse the following information about the information security project, and provide public institutions, etc, with the information so the head of each public institution, etc. may pay an appropriate price for an information security project under paragraph (1): <Amended on Jul. 26, 2017>

1. Environments for implementing the information security project;

2. Tools for implementing the information security project;
3. Costs, schedule, scale and the number of processes of the information security project;
4. Information about the characteristics of the quality of the information security project;
5. Other matters necessary for setting pricing standards for information security services for maintaining and managing information security products, and for maintaining the security performance thereof.

(5) The Minister of Science and ICT may request the heads of public institutions, etc. to submit necessary data to comprehensively manage information about information security projects under paragraph (4), and the heads of public institutions, etc. shall cooperate unless good cause exist. <Amended on Jul. 26, 2017>

(6) The cycle and method of disclosure of the findings of investigation under paragraph (2) and other necessary matters shall be prescribed by Presidential Decree.

Article 11 (Acceleration of convergence of information security industry) (1) The Government may formulate and implement policies necessary to accelerate researching and developing converged information security technology, etc. and developing various information security products and services based on development of convergence between the information security industry and other industries.

(2) The Minister of Science and ICT may implement the following projects to accelerate development of converged information security technology, etc.: <Amended on Jul. 26, 2017>

1. Researching and developing converged information security technology, etc.;
2. Trade and commercialization of converged information security technology;
3. Pilot projects concerning converged information security technology, etc.;
4. Training professionals concerning converged information security technology, etc.;
5. Policy research concerning converged information security technology, etc.;
6. Other support necessary to accelerate the development of converged information security technology, etc.

Article 12 (Support for evaluation of level of information security preparedness) (1) A person who provides, or intermediates to provide, information through an information and communications network may undergo evaluation of the level of information security preparedness by an evaluation agency registered with the Ministry of Science and ICT pursuant to paragraph (2) for the safety of persons who use information and

communications services under Article 2 (1) 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection. <Amended on Jul. 26, 2017>

(2) A person who intends to evaluate the level of information security preparedness shall register with the Minister of Science and ICT after preparing the following: <Amended on Jul. 26, 2017>

1. Articles of incorporation of a corporation or rules of an organization;
2. Plan for implementing a project to evaluate the level of information security preparedness;
3. Other matters prescribed by Presidential Decree, such as documents that may prove the human, technical and financial capability necessary to evaluate the level of information security preparedness.

(3) The Minister of Science and ICT may provide an evaluation agency registered pursuant to paragraph (2) with technical and financial support necessary to conduct evaluation of the level of information security preparedness, within the budgetary limits. <Amended on Jul. 26, 2017>

(4) The Government may provide enterprises that have undergone evaluation of the level of information security preparedness, with necessary support, such as awarding a prize, based on the findings of evaluation.

(5) Necessary matters concerning requirements and procedures for registration under paragraph (2), and support under paragraphs (3) and (4) shall be prescribed by Presidential Decree.

Article 13 (Information security disclosure) (1) A person who provides, or intermediates the provision of, information through an information communications network may disclose the status of information security, such as the status of investment in and human resources for information security, and authentication related to information security, to ensure that persons who use information and communications services under Article 2 (1) 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection use the Internet in a safe manner, as prescribed by Presidential Decree. In such cases, corporations subject to the submission of an annual report under Article 159 of the Financial Investment Services and Capital Markets Act may include in its disclosure the current status of authentication related to information security, such as the results of the

evaluation of the level of information security preparedness, pursuant to Article 391 of the aforesaid Act.

(2) Notwithstanding paragraph (1), a person who needs to adopt the information security disclosure system to ensure that persons who use information and communications services use the Internet in a safe manner and who also meets the standards prescribed by Presidential Decree in terms of business areas, sales, the number of users of such services, and other factors shall disclose the current status of information security under paragraph (1); provided, a person who discloses the current status of information security under other statutes shall be excluded herefrom. <Added on Jun. 8, 2021>

(3) Where a person who has disclosed the current status of information security pursuant to paragraph (1) intends to obtain authentication of an information security management system under Article 47 (1) of the Act on Promotion of Information and Communications Network Utilization and Information Protection, he or she may be granted a 30 percent discount on a fee required to be paid. <Amended on Jun. 8, 2021>

(4) The Minister of Science and ICT shall verify the disclosed information under paragraph (1) or (2) and may request that such information be corrected if it is inaccurate. <Added on Apr. 18, 2023>

(5) Methods and procedures for verifying the disclosed information under paragraph (4) and other details shall be prescribed by Decree of the Ministry of Science and ICT. <Added on Apr. 18, 2023>

CHAPTER III CREATION OF INFRASTRUCTURE FOR PROMOTION OF INFORMATION SECURITY INDUSTRY

Article 14 (Implementation of technological development and standardization) (1) The Minister of Science and ICT may implement the following projects to accelerate the development of and investment in information security technologies: <Amended on Jul. 26, 2017>

1. Surveying the levels of information security technologies and research and development of fundamental technologies;
2. Discovering and developing core patented technologies for information security in promising fields for future growth;

3. International joint research and development and support concerning information security technologies;
4. Commercializing information security technologies and establishing regional clusters of industries related to information security;
5. Projects to support joint research on information security technology among industry-academia-research;
6. Projects to revitalize trade in information security technology;
7. Other projects necessary to accelerate the development of and investment in information security technologies.

(2) The Minister of Science and ICT may establish and operate a system to comprehensively support the information security industry to strengthen the revitalization of the trade of information security technology and the competitiveness thereof, and to provide information related to the information security industry. <Amended on Jul. 26, 2017>

(3) The Minister of Science and ICT may establish and operate facilities for supporting information security enterprises in their commercialization efforts, such as technological testing and development, and may allow them to use the facilities or lend them such facilities. <Amended on Jul. 26, 2017>

(4) The Minister of Science and ICT may implement the following projects to revitalize the trade of information security technology and to secure the compatibility among information security products, as prescribed by Presidential Decree: <Amended on Jul. 26, 2017>

1. Establishing, revising, abolishing, and disseminating standards concerning information security technology, etc.; provided, where relevant Korean Industrial Standards prescribed in the Industrial Standardization Act have been established, the Korean Industrial Standards shall apply;
2. Conducting survey and research on, and development of, domestic and international standards related to information security technology, etc.;
3. Taking measures concerning international standardization of Korean standards related to information security technology, etc.;
4. Other projects necessary for standardization of information security technology, etc.

Article 15 (Training for professionals) (1) The Minister of Science and ICT may formulate and implement the following policy measures in consultation with the heads of related central administrative agencies, to train professionals necessary for the promotion of the information security industry: <Amended on Jul. 26, 2017>

1. Ascertaining the actual condition of demand for professionals and formulating a mid-term and long-term prospect of the supply and demand of professionals;
2. Designating, establishing and supporting institutions that train professionals;
3. Support to develop and disseminate educational programs to train professionals;
4. Support to establish a qualification system and for the supply and demand of professionals related to the information security industry;
5. Support for education related to the information security industry provided by schools at all levels and other educational institutions;
6. Other matters necessary to train professionals prescribed by Presidential Decree.

(2) The Minister of Science and ICT may implement a project to discover and nurture future talent and excellent foreign human resources related to information security, and an intern system that requires interns to earn credits. Articles 12 and 13 of the Special Act on Promotion of Information and Communications Technology and Vitalization of Convergence Thereof shall apply to matters necessary for the implementation of this project. <Amended on Jul. 26, 2017>

(3) The Minister of Science and ICT may establish and operate a management system of information security professionals for systematic training and management of information security professionals; and the range and details of support for professionals registered in the management system shall be prescribed by Decree of the Ministry of Science and ICT. <Amended on Jul. 26, 2017>

Article 16 (Promotion of international cooperation) (1) The Minister of Science and ICT shall understand international trends concerning the information security industry and may promote international cooperation. <Amended on Jul. 26, 2017>

(2) The Minister of Science and ICT may provide support for projects, such as international exchanges of information security technology and professionals, and international joint research and development, to promote international cooperation in the field of the information security industry. <Amended on Jul. 26, 2017>

(3) The Minister of Science and ICT may support the private sector related to the information security industry in its international cooperation. <Amended on Jul. 26, 2017>

Article 17 (Support for performance assessment) (1) The Minister of Science and ICT may assess performance of information security products to secure quality, accelerate the distribution and protect users of information security products, and to revitalize convergence industries. <Amended on Jul. 26, 2017>

(2) The Minister of Science and ICT may designate an assessment agency to professionally assess performance under paragraph (1). <Amended on Jul. 26, 2017>

(3) A person who intends to undergo performance assessment under paragraph (1) shall file an application for assessment with an assessment agency under paragraph (2). In such cases, an applicant shall bear the associated expenses, and the Minister of Science and ICT may provide necessary support, within budgetary limits. <Amended on Jul. 26, 2017>

(4) Necessary matters concerning methods of assessing performance under paragraph (1) and the designation of an assessment agency under paragraph (2) shall be prescribed by Presidential Decree.

Article 18 (Designation of excellent information security technology, etc.) (1) The Minister of Science and ICT may designate excellent information security technology, etc., and provide support therefor annually for the revitalization of the information security industry, as prescribed by Presidential Decree. <Amended on Jul. 26, 2017>

(2) Where the Minister of Science and ICT designates excellent information security technology, etc. under paragraph (1), he or she may request a person who provides the relevant information security technology, etc. to provide data necessary for the designation thereof. <Amended on Jul. 26, 2017>

(3) Where the Minister of Science and ICT makes a designation under paragraph (1), he or she shall publicly notify such designation, and necessary matters, such as methods of designation and details of support, shall be prescribed by Presidential Decree. <Amended on Jul. 26, 2017>

Article 19 (Designation of exemplary information security enterprises) (1) The Minister of Science and ICT may designate information security enterprises which have contributed to promoting the information security industry, such as the development and commercialization of excellent information security technology, etc. under Article 18 (1), as

exemplary information security enterprises and provide support for them. <Amended on Jul. 26, 2017>

(2) The Government shall preferentially provide the following support to exemplary information security enterprises under paragraph (1):

1. Concluding a contract on a project for establishing an information security system under Article 7 (1);
2. Providing support in training professionals under Article 15;
3. Providing loans under Article 20 (1);
4. Other matters prescribed by Presidential Decree to cultivate the information security industry.

(3) The Minister of Science and ICT may request the heads of public institutions, etc. to submit the details of support under paragraph (2) and the performance therein. In such cases, any institution or organization requested to submit the details of support and the relevant performance shall comply therewith, except under special circumstances. <Amended on Jul. 26, 2017>

(4) The Minister of Science and ICT shall publicly notify exemplary information security enterprises designated pursuant to paragraph (1), and necessary matters concerning methods, details, etc. of designation shall be prescribed by Presidential Decree. <Amended on Jul. 26, 2017>

Article 20 (Provision of loans) (1) Where it is necessary to cultivate the information security industry, the Minister of Science and ICT may lend to information security enterprises any of the following funds at a low interest rate, long-term (where an information security enterprise takes out a loan from a financial institution, this includes cases where a subsidy is granted to cover a difference between interest on the loan and that determined by the Minister of Science and ICT; hereinafter the same shall apply): <Amended on Jul. 26, 2017; Oct. 19, 2021>

1. Funds necessary to install, transfer, replace, complement or extend information security products and information security services;
2. Funds necessary to purchase and stockpile raw materials;
3. Development funds to localize information security products and information security services;

4. Funds to export information security products and information security services;
5. Funds necessary to develop core technologies and components for information security;
6. Funds necessary for research and development and the maintenance of idle facilities;
7. Other funds necessary to operate the information security industry.

(2) Necessary matters concerning procedures, methods, etc. for filing applications for loans under paragraph (1) shall be prescribed by Presidential Decree.

Article 21 (Support for exportation) (1) Where the Minister of Science and ICT deems it necessary to promote exporting in the information security industry, he or she may take measures necessary for the acceleration of investment in the information security industry and the expansion of export markets, as prescribed by Presidential Decree. <Amended on Jul. 26, 2017>

(2) Where the Minister of Science and ICT deems it necessary for the promotion of exportation under paragraph (1), he or she may provide any of the following persons with financial, material or personnel support, within budgetary limits, as prescribed by Presidential Decree: <Amended on Jul. 26, 2017>

1. A person who promotes exporting information security products and information security services;
2. A person who engages in business providing advice, guidance, publicity, exhibiting, training or mediating business talks for the promotion of exportation;
3. A person who installs and operates showrooms related to information security products, information security services, etc. or exhibits information security products, information security services, etc. at the exhibition centers both at home and abroad;
4. A person who promotes international cooperation to export information security products, information security services, etc.

Article 22 (Taxation support) (1) The Government may take necessary measures, such as granting tax credits, as prescribed by the Restriction of Special Taxation Act, the Restriction of Special Local Taxation Act, and other related taxation statutes for the promotion of the information security industry.

(2) The Government may provide financial support or other necessary support to develop the information security industry, and to expand investment in and to nurture small and medium enterprises related to information security, as prescribed by Presidential Decree.

Article 23 (Designation and management of enterprises specializing in information security services) (1) The Minister of Science and ICT may designate a person deemed capable of conducting the following affairs safely and reliably, as an enterprise specializing in information security services: <Amended on Jul. 26, 2017>

1. Affairs concerning the analysis and evaluation of vulnerabilities of important information and communications infrastructure designated pursuant to Article 8 of the Act on the Protection of Information and Communications Infrastructure (hereafter in this Article, referred to as "important information and communications infrastructure");
2. Affairs concerning the formulation of measures for the protection of important information and communications infrastructure;
3. Other affairs prescribed by Presidential Decree in relation to information security services.

(2) A person who can be designated as an enterprise specializing in information security services must be a corporation.

(3) The Minister of Science and ICT shall examine the post management of an enterprise specializing in information security services designated pursuant to paragraph (1) annually from the date it is designated as the enterprise specializing in information security services. <Amended on Jul. 26, 2017>

(4) Where an enterprise specializing in information security services transfers its business or merges with another enterprise specializing in information security services, it shall report thereon to the Minister of Science and ICT. In such cases, a transferee or a corporation merged shall succeed to the status of the enterprise specializing in information security services when the Minister of Science and ICT accepts the report. <Amended on Jul. 26, 2017>

(5) Where an enterprise specializing in information security services suspends, closes or resumes its business, it shall report thereon to the Minister of Science and ICT by no later than 30 days prior to the date it intends to suspend or close its business, or to resume its business after the suspension of business. <Amended on Jul. 26, 2017>

(6) Where an enterprise specializing in information security services falls under any of the following cases, the Minister of Science and ICT may revoke the designation of the enterprise specializing in information security services, or may order the suspension of all or part of its business for a specified period of up to three months after hearings;

provided, where it falls under any of subparagraphs 1, 2 and 4, he or she shall revoke the designation thereof: <Amended on Jul. 26, 2017>

1. Where it is designated by fraud or other improper means;
2. Where it fails to pass an examination of the post management under paragraph (3);
3. Where it fails to preserve records and data safely, in violation of paragraph (8);
4. Where it fails to meet criteria for designation under paragraph (10);
5. Where it causes difficulty in the operation of important information and communications infrastructure, by misusing or abusing information it has officially obtained.

(7) Where the Minister of Science and ICT deems it especially necessary for information security, he or she may require an enterprise specializing in information security services to submit related documents or data. <Amended on Jul. 26, 2017>

(8) An enterprise specializing in information security services shall preserve records and data it has prepared in relation to the affairs specified in the subparagraphs of paragraph (1), in a safe manner.

(9) Where the designation of an enterprise specializing in information security services under paragraph (1) is revoked or it closes its business, it shall return records and data related to the affairs referred to in the subparagraphs of paragraph (1) to the head of the relevant institution or enterprise, or destroy such records and data, and in the case of data unavailable or impossible to be returned, it shall specify the data to be destroyed and obtain approval therefor from the head of the relevant institution or enterprise before destroying such data.

(10) Necessary matters concerning designation under paragraph (1), examining post management under paragraph (3), transfer or merger under paragraph (4), reporting of suspension of business, etc. under paragraph (5), revocation of designation under paragraph (6), presentation of data under paragraph (7), procedures, methods, etc. for returning or destroying records and data under paragraph (9) shall be prescribed by Decree of the Ministry of Science and ICT. <Amended on Jul. 26, 2017>

Article 24 (Incorporation of Korea Information Security Industry Association) (1) Those who operate businesses related to the information security industry may incorporate the Korea Information Security Industry Association (hereinafter referred to as the "Association" in this Article) after obtaining approval from the Minister of Science and ICT for the sound development of the information security industry and improvement of the levels of

information security in overall national industries. <Amended on Jul. 26, 2017>

(2) The Association shall be a corporation.

(3) Necessary matters concerning procedures for authorization, business, supervision, etc. of the Association shall be prescribed by Presidential Decree.

(4) Except as otherwise provided for in this Act, the provisions concerning incorporated associations of the Civil Act shall apply mutatis mutandis to the Association.

CHAPTER IV DISPUTE MEDIATION COMMITTEE

Article 25 (Establishment of dispute mediation committee) (1) An information security industry dispute mediation committee (hereinafter referred to as the "Mediation Committee") shall be established to mediate disputes concerning developing, using, etc. information security products and information security services; provided, the Copyright Act shall apply to disputes related to copyrights, and disputes which become subject to mediation to settle disputes under Article 35-3 of the Broadcasting Act, disputes which become subject to arbitration under 45 of the Telecommunications Business Act and disputes which become subject to mediation under Article 40 of the Personal Information Protection Act among disputes related to broadcasting and communications shall be governed by the provisions of the relevant Act, respectively.

(2) The Mediation Committee shall be comprised of at least ten but not more than 30 members, including one chairperson.

(3) The Minister of Science and ICT shall appoint or commission members of the Mediation Committee from among the following persons: <Amended on Jul. 26, 2017>

1. Persons who hold or held the position of at least associate professor of law or in a department in a field related to information security at schools prescribed in Article 2 of the Higher Education Act;
2. Judges, public prosecutors or qualified attorneys-at-law;
3. Persons who have extensive knowledge and experience in the information security industry;
4. Persons who belong to user protection institutions or organizations;
5. Persons who hold or held the position of public official of at least Grade IV (including public officials in general service belonging to the Senior Executive Service) or equivalent

position at a public institution, who have experience in affairs concerning the promotion of the information security industry or affairs concerning consumer protection.

(4) The Chairperson of the Mediation Committee shall be elected by the Mediation Committee from among its members.

(5) Members shall be non-standing members, and the term of office of members who are not public officials shall be three years; such members may serve a second consecutive term only once: Provided That members who are public officials appointed pursuant to paragraph (3) 5 shall serve as members for a period during which they hold the position.

(6) No member shall be removed from office or dismissed against his or her will except in any of the following cases: <Amended on Feb. 21, 2018>

1. Where he or she is subjected to suspension of license or heavier punishment;
2. Where he or she is no longer capable of performing his or her duties due to a mental disorder;
3. Where he or she has committed a violation in connection with his or her duties;
4. Where he or she is deemed unfit as a member due to neglect of duties or injury to dignity; and
5. Where he or she fails to recuse himself or herself despite falling under any subparagraph of Article 27 (1) or under the former part of paragraph (2) of the same Article.

(7) The Secretariat shall be established in the Korea Internet and Security Agency under Article 52 of the Act on Promotion of Information and Communications Network Utilization and Information Protection to assist the Mediation Committee in performing its affairs.

Article 26 (Mediation to settle disputes) (1) A person who intends to obtain compensation for loss and to seeks mediation of a dispute in relation to the use, etc. of information security products and information security services may file an application for medication with the Mediation Committee; provided, the foregoing shall not apply where he or she has filed for mediation of the dispute or the dispute has been settled pursuant to another statute.

(2) The Mediation Committee shall prepare a proposed agreement within 60 days from the date on which it receives an application for dispute mediation under paragraph (1); provided, where it intends to extend the period in extenuating circumstances, it shall notify the parties to the dispute of the ground for extension and the extended period.

Article 27 (Exclusion, challenge and voluntary refrainment of members) (1) Where a member of the Mediation Committee falls under any of the following cases, he or she shall be excluded from deliberating and resolving on a case of dispute mediation (hereinafter referred to as "case") for which an application has been filed with the Mediation Committee pursuant to Article 26:

1. Where the member or his or her current or former spouse becomes a party to the case, or is a joint holder of any right or is in relationship with a person who is jointly liable for the case;
2. Where the member is or was a relative of a party to the case;
3. Where the member bears witness to, provides an expert opinion or legal advice on, the case;
4. Where the member participates or participated in the case as an agent of a party to the case.

(2) Where a party to a dispute has reasonable grounds to deem a member unlikely to be fair in the mediation of such dispute, he or she may explain the grounds in writing and file an application for challenge. In such cases, the Chairperson shall render a decision on the application for challenge without adopting a resolution of the Mediation Committee.

(3) Where a member falls under paragraph (1) or (2), he or she may voluntarily refrain from the deliberation and resolution on the case.

Article 28 (Request for data) (1) The Mediation Committee may request the parties to a dispute, information security enterprises or witnesses (hereafter in this Article, referred to as "parties to the dispute, etc." in this Article) to provide data necessary for dispute mediation. In such cases, none of the relevant parties to the dispute, etc. shall refuse a request to provide data without good cause.

(2) Where the Mediation Committee deems it necessary, it may require the parties to the dispute, etc. to attend its meetings to hear their opinions.

Article 29 (Validity of mediation) (1) Where the Mediation Committee prepares a proposed agreement pursuant to Article 26 (2), it shall immediately present the proposed agreement to each party to the dispute.

(2) Each party to the dispute to whom a proposed agreement is presented pursuant to paragraph (1) shall notify the Mediation Committee of whether he or she accepts the

proposed agreement within 15 days from the date the proposed agreement is presented to him or her. In such cases, where a party to the dispute fails to notify the Mediation Committee as to whether he or she accepts the proposed agreement, he or she shall be deemed to have refused the proposed agreement.

(3) Where the parties to the dispute accept a proposed agreement pursuant to paragraph (2), the Mediation Committee shall prepare the mediation agreement, stating the matters agreed by and between the parties to the dispute.

(4) Where the parties to the dispute accept a proposed agreement and the Mediation Committee prepares a mediation agreement and notify the parties to the dispute of the mediation agreement pursuant to paragraph (3), a settlement on the same terms as that of the proposed agreement shall be deemed reached by and between the parties to the dispute.

Article 30 (Refusal and suspension of mediation) (1) Where the Mediation Committee admits that it is inappropriate for the Mediation Committee to mediate a dispute due to the characteristics of the dispute or deems that an application for mediation has been filed vexatiously, it may refuse to mediate the relevant case. In such cases, it shall notify applicants of reasons for refusal of mediation, etc.

(2) Where one party files a suit during the mediation process of a dispute for which an application was filed, the Mediation Committee shall suspend the mediation to settle the dispute and notify both parties to the dispute of such fact.

Article 31 (Expenses incurred in mediating dispute) The Mediation Committee may require persons who have filed an application for dispute mediation to bear the associated expenses, as prescribed by Presidential Decree; provided, where a settlement has been reached, the Mediation Committee may require the parties to the dispute to apportion expenses incurred in mediating the dispute.

Article 32 (Confidentiality) No former or current facilitator of affairs concerning dispute mediation of the Mediation Committee shall divulge confidential information obtained in the course of performing his or her duties to any third person, or use confidential information for other than official purposes; provided, the foregoing shall not apply where special provisions are prescribed in other statutes.

Article 33 (Procedures for mediation) In addition to matters provided for in this Chapter, necessary matters concerning the organization and operation of the Mediation Committee, methods and procedures for dispute mediation, the management of affairs concerning mediation, etc., shall be prescribed by Presidential Decree.

CHAPTER V MEASURES TO PROTECT USERS

Article 34 (Measures to protect users) (1) The Government may implement the following projects to protect fundamental rights and interests of users:

1. Providing information on the information security industry to users and education of users;
2. Fact-finding research as to whether guidelines for protection of users under Article 36 are complied with;
3. Education concerning the protection of users intended for information security enterprises;
4. Providing support to institutions or organizations aiming at protecting users;
5. Formulating and implementing measures for preventing loss of users and providing users with relief;
6. Formulating and implementing other measures for protecting rights and interests of users.

(2) The Government shall formulate and implement necessary measures so that persons difficult to freely approach or use information security products or services due to economical, regional, physical or social circumstances can use information security products or services in a convenient manner.

Article 35 (Withdrawal of application) (1) In the case of information security products and information security services in which it is impracticable for users to withdraw an application or to cancel a contract pursuant to Article 17 (2) of the Act on the Consumer Protection in Electronic Commerce (excluding the proviso of the same paragraph), each information security enterprise shall take measures through any of the following means to ensure that the exercise of users' rights to withdraw an application and to cancel a contract is not interfered with; provided, where an information security enterprise fails to take such measures, withdrawing an application or cancelling a contract by a user shall not

be restricted:

1. Method, etc. for withdrawing applications shall be specified on information security products and information security services or the package thereof;
2. A pilot information security product shall be provided or it shall be possible to temporarily or partially use the same.

(2) Articles 17, 18, 31, 32, 40, 41 and 44 of the Act on the Consumer Protection in Electronic Commerce shall apply mutatis mutandis to withdrawing an application and cancelling a contract under paragraph (1). In such cases, "communications service providers" and "business entities" shall be construed as "information security enterprises," "goods, etc." as "information security products and information security services," "consumers" as "users," and the "Fair Trade Commission" as the "Minister of Science and ICT," respectively. <Amended on Jul. 26, 2017>

Article 36 (Formulation of guidelines for protection of users) (1) The Minister of Science and ICT may formulate guidelines with which information security enterprises may voluntarily comply for sound trade, establishment of healthy distribution, and protection for users in the information security industry (hereinafter referred to as "guidelines for the protection of users"). In such cases, the Minister of Science and ICT may take advice from business entities, institutions and organizations, and experts in related fields. <Amended on Jul. 26, 2017>

(2) Information security enterprises shall stipulate the terms and conditions, including, but not limited to the return of overpaid or erroneously paid amounts, the right to cancel or terminate a contract for using an information security product and information security service, compensation for loss to users which occurs due to a defect, etc. in the product, as prescribed by Presidential Decree.

(3) Where an information security enterprise enters into a contract concerning the use of an information security product and information security service, it shall explain to users, the details of the terms and conditions under paragraph (2); and where a user requests, it shall issue a copy of the terms and conditions to the user so that he or she may readily understand the details of the terms and conditions.

(4) The Minister of Science and ICT may stipulate the standard terms and conditions concerning trade in the information security industry and recommend information security enterprises to use the standard terms and conditions. <Amended on Jul. 26, 2017>

(5) Where the terms and conditions an information security enterprise uses are unfavorable to users compared to the details of guidelines for the protection of users, it shall indicate or announce the details of the terms and conditions stipulated differently from guidelines for the protection of users so that users may readily understand differences.
(6) Articles 31, 32, 40, 41 and 44 of the Act on the Consumer Protection in Electronic Commerce shall apply mutatis mutandis to recommendations for corrective action, measures to take corrective action and penalty provisions against cases where an information security enterprise violates paragraphs (2), (3) and (5). In such cases, the "Fair Trade Commission" shall be construed as "Minister of Science and ICT," "business entities" as "information security enterprises," and "consumers" as "users." <Amended on Jul. 26, 2017>

Article 37 (Information security measures of public institutions) The head of each public institution shall prepare a managerial, physical and technological plan for information security of the relevant institution, and the Government may investigate the current status of information security of public institutions and take measures for information security.

CHAPTER VI SUPPLEMENTARY PROVISIONS

Article 38 (Entrustment of duties) The Minister of Science and ICT may entrust part of his or her duties under this Act to a specialized institution designated, as prescribed by Presidential Decree. <Amended on Jul. 26, 2017>

Article 39 (Deemed public officials for purposes of penalty provisions) Executive officers and employees of an institution that engages in duties entrusted pursuant to this Act shall be deemed public officials for the purposes of the penalty provisions prescribed in Articles 129 through 132 of the Criminal Act.

CHAPTER VII PENALTY PROVISIONS

Article 40 (Penalty provisions) Any person who divulges confidential information obtained in the course of performing his or her duties, or uses such confidential information for purposes other than official purposes, in violation of Article 32, shall be punished by

imprisonment with labor for not more than three years or by a fine not exceeding 30 million won.

Article 41 (Administrative fines) (1) Any of the following persons shall be punished by an administrative fine not exceeding 10 million won: <Amended on Jun. 8, 2021; Apr. 18, 2023>

1. A person who fails to disclose the current status of information security, in violation of Article 13 (2);

1-2. A person who refuses or interferes with the verification of the disclosed information under Article 13 (4) or fails to comply with a request for correction;

2. A person who fails to make a report under Article 23 (5);

3. A person who fails to submit related documents or data under Article 23 (7), or submits false documents or data;

4. A person who fails to return or destroy records and data or destroys records and data without obtaining approval, in violation of Article 23 (9).

(2) The Minister of Science and ICT shall impose and collect administrative fines under paragraph (1), as prescribed by Presidential Decree. <Amended on Jul. 26, 2017>