ENFORCEMENT DECREE OF THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND

[Enforcement Date 20. May, 2025.] [Presidential Decree No.35533, 20. May, 2025., Partial Amendment]

방송미디어통신위원회 (디지털이용자기반과 - 본인확인제 관련)02-2110-1521

ENFORCEMENT DECREE OF THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION

[Enforcement Date 20. May, 2025.] [Presidential Decree No.35533, 20. May, 2025., Partial Amendment]

방송미디어통신위원회 (디지털이용자기반과 - 본인확인제 관련) 02-2110-1521
방송미디어통신위원회 (디지털이용자기반과 - 스팸) 02-2110-1514
방송미디어통신위원회 (이용자정책총괄과) 02-2110-1514
과학기술정보통신부 (통신자원정책과 - 통신과금관련) 044-202-6669
과학기술정보통신부 (사이버침해대응과 - 해킹 등 침해대응 관련) 044-202-6461, 6462
과학기술정보통신부 (디지털기반안전과- 집적정보통신시설 관련) 044-202-6777, 6778
방송미디어통신위원회 (디지털유해정보대응과 - 불법정보 및 청소년보호 관련) 02-2110-1567, 1549

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose) The purpose of this Decree is to prescribe matters mandated by the Act on Promotion of Information and Communications Network Utilization and Information Protection and those necessary for enforcing said Act.

Article 2 (Code of ethics) (1) The providers of information and communications services, defined under Article 2 (1) 3 of the Act on Promotion of Information and Communications Network Utilization and Information Protection (hereinafter referred to as the "Act"), and an association of such providers may establish and enforce a code of ethics in order to protect users and to ensure soundness and safety in providing information and communications services. <Amended on Jan. 28, 2009; Aug. 4, 2020>

(2) An association of users defined under Article 2 (1) 4 of the Act may establish and enforce a users' code of ethics for the establishment of a sound information society.

(3) The Government may provide assistance to activities for the establishment and enforcement of the code of ethics under paragraph (1) or (2).

Article 3 Deleted. <Aug. 4, 2020>

CHAPTER II PROMOTION OF UTILIZATION OF INFORMATION AND COMMUNICATIONS NETWORKS

Article 4 Deleted. <Aug. 18, 2009>

Article 5 Deleted. <Aug. 18, 2009>

Article 6 (Policy measures for establishment of system for sharing information) (1) Pursuant to Article 12 of the Act, the head of a central administrative agency may formulate and provide a public notice of a plan for sharing information about matters under his or her jurisdiction. <Amended on May 4, 2010>

(2) If the head of a central administrative agency deems it necessary to efficiently implement a plan for sharing information pursuant to paragraph (1), he or she may assist a person in conducting the following business activities:

1. Selection of information to be shared, among the information possessed and managed;
2. Establishment and operation of a system for interconnecting different information and communications networks;
3. Adjustment of expenses allotted to each agency in connection with the interconnection of different information and communications networks;
4. Other activities necessary for the establishment of the system for sharing information.

Article 7 (Implementation of projects for promoting utilization of information and communications networks) Projects that the Minister of Science and Information Communications Technology (ICT) may implement pursuant to Article 13 (1) of the Act are as follows: <Amended on Mar. 23, 2013; Jul. 26, 2017>

1. Pilot projects for the establishment and operation of information and communications networks;
2. Pilot projects for the commercialization of new media;
3. Advanced application projects for nurturing the informatization industry and projects for supporting related research projects;
4. Projects to lay a foundation for the development of technologies for electronic transactions and the invigoration of electronic transactions;
5. Supportive projects for the improvement of statutes and systems for promoting the utilization of information and communications networks;

6. Other pilot projects for the efficient utilization and dissemination of technologies, devices, and application services.

CHAPTER III Deleted.

Article 8 Deleted. <Dec. 22, 2015>

Article 9 Deleted. <Dec. 22, 2015>

CHAPTER IV CREATION OF SAFE ENVIRONMENT FOR USE OF INFORMATION AND COMMUNICATIONS SERVICES

Article 9-2 (Extent of access authority) (1) A case where a provider of information and communications services shall obtain consent from the users pursuant to Article 22-2 (1) of the Act means a case where such provider needs authority of access to the following information and functions (hereafter referred to as "access authority" in this Article) through the software of mobile devices; provided, this shall not apply to the information and functions accessed by any software, which has been installed in mobile devices in the course of manufacturing and supplying them, to perform their intrinsic functions such as communications, photography, and audio and video replay:

1. Information stored by the users on their mobile devices such as contact points, schedules, videos, communications, biometric information (referring to information concerning physical or behavioral characteristics with which an individual can be identified, such as fingerprints, iris, voice, and handwriting; hereinafter the same shall apply);
2. Information automatically stored on mobile devices in the course of using them, such as location information, communication logs, authentication information, and physical activity records;
3. Unique information assigned to identify mobile devices, including unique international identification number under Article 60-2 (1) of the Telecommunications Business Act;
4. Input and output functions, such as photography, speech recognition, and biometric or health information detecting sensor.

(2) A provider of information and communications services shall, in the course in which the users install or run a software of mobile devices, inform the users of the matters referred to in each subparagraph of Article 22-2 (1) of the Act in a manner displaying such matters on a software's guidance information screen or other separate screen and shall obtain consent of the users according to the following classifications in the same manner:

1. Where the basic operating system of mobile devices (referring to the based environment in which the software can be executed in mobile devices; hereinafter referred to as "operating system") is an operating system in which the users can individually choose whether to consent to the access authority: A method by which, after the provider of information and communications services informs the users about the both access authorities under Article 22-2 (1) 1 and 2 of the Act separately from each other, the users choose whether to consent when for the first time they access any information or function the access authority for which is set;
2. Where the operating system of mobile devices is an operating system by which the users cannot individually choose whether to consent to the access authority: A method by which, after the provider of information and communications services only sets the access authority under Article 22-2 (1) 1 of the Act and informs the users thereof, the users choose whether to consent to the access authority when they install the software;
3. Where the method referred to in subparagraph 1 or 2 is impossible though the operating system of mobile devices falls within the operating system described in subparagraph 1 or 2: A method similar to the method referred to in subparagraph 1 or 2, by which the provider of information and communications services informs the users of the content of consent so that they can definitely acknowledge such content and choose whether to give consent.

(3) When determining whether a matter requiring consent of the users pursuant to Article 22-2 (1) of the Act falls under any access authority under subparagraph 1 or 2 of that Article, the following shall be taken into consideration: The extent of information and communications services as disclosed through the terms of service, the privacy policy prescribed in Article 30 (1) of the Personal Information Protection Act, or any separate guidelines; whether such information and communications services are actually provided; the users' reasonable foreseeability for the relevant information and communications services; and technical relevance between the relevant information and communications

services and the access authority, and other factors. <Amended on Aug. 4, 2020>

(4) Persons manufacturing and supplying the operating system of mobile devices, manufacturers of mobile devices, and persons manufacturing and supplying software of mobile devices shall take necessary measures according to the following classifications in order to protect information on the users referred to in Article 22-2 (3) of the Act:

1. Persons manufacturing and supplying the operating system of mobile devices: They shall manufacture and provide the operating system in which there are embedded functions by which the providers of information and communications services can obtain the consent of the users by the methods classified in the subparagraphs of paragraph (2) and the users can revokes their consent, and they also shall prepare and disclose operating standards for the access authority set in the operating system so that the persons manufacturing and supplying the software of mobile devices can easily understand such standards;
2. Manufacturers of mobile devices: They shall install on mobile devices the operating system in which functions to give and revoke the consent under subparagraph 1 are embedded;
3. Persons manufacturing and providing software of mobile devices: They shall embed in the software the operating system for which the measures under subparagraphs 1 and 2 are taken and the methods for giving and revoking consent which are suitable for mobile devices.

[This Article Added on Mar. 22, 2017]

Article 9-3 (Detailed examination criteria for each examination item) (1) Detailed examination criteria for each item of under Article 23-3 (1) of the Act shall be as follows: <Amended on Aug. 17, 2012; Aug. 4, 2020>

1. A plan for physical, technical, and administrative measures: A plan to take measures regarding the following shall be formulated:
   (a) The management and operation of facilities related to the identity verification service under Article 23-3 (1) of the Act (hereinafter referred to as "identity verification service");
   (b) The prevention of a breach on information and communications networks;
   (c) The operation, security, and management of systems and networks;

(d) The protection of users and the settlement of complaints;

(e) The response to urgency and emergency;

(f) The formulation and implementation of internal regulations on the identity verification service;

(g) The securement of safety of an alternative means under Article 23-2 (2) of the Act (hereinafter referred to as "alternative means");

(h) The prevention of fabrication and alteration of access records;

(i) Other matters determined and publicly notified by the Korea Communications Commission for the identity verification service;

2. Technical capability: An identification service agency shall have at least 8 persons who meet any of the following requirements:

(a) Each person shall have a national technical qualification of information and communications engineer, information processing engineer, or electronic computer system application engineer or higher, or a qualification recognized by the Korea Communications Commission as equivalent or higher;

(b) Each person shall have work experience of at least 2 years in the field of information protection or information and communications operation and management as prescribed and publicly notified by the Korea Communications Commission;

3. Financial capability: An identification service agency's equity capital shall be at least 8 billion won (excluding national agencies and local governments);

4. Adequacy of the size of facilities: An identification service agency shall possess the following facilities that shall be at least the size necessary to properly provide identity verification services:

(a) Facilities for the verification, management, and protection of users' personal information (referring to personal information defined in subparagraph 1 of Article 2 of the Personal Information Protection Act; hereafter in Article 9-6 the same shall apply);

(b) Facilities for the generation, issuance, and management of alternative means;

(c) Security facilities for controlling and restricting access;

(d) Facilities for the protection of systems and networks;

(e) Facilities for the prevention of fire, flood, power failure, and other disasters.

(2) Matters necessary for guidelines and methods for the evaluation of criteria for each standard subject to the review under paragraph (1) shall be prescribed and publicly

notified by the Korea Communications Commission.

[This Article Added on Aug. 29, 2011]

Article 9-4 (Procedures for designation of identity verification agencies) (1) A person who seeks to be designated as an identity verification agency under Article 23-3 (1) of the Act shall file an application for the designation of an identity verification agency (including in electronic form) with the Korea Communications Commission, along with the following documents (including electronic documents):

1. A business plan describing the current conditions of its organization, human resources, facilities, etc.;
2. Documents certifying that criteria for each standard subject to the review under Article 9-3 are satisfied;
3. Articles of incorporation or bylaws of organization (applicable only if an applicant is a legal person or organization);
4. Other documents specified and publicly notified by the Korea Communications Commission as documents necessary for ascertaining the expertise in providing identity verification services, the soundness of the financial structure, etc.

(2) Upon receipt of an application for the designation of an identity verification agency under paragraph (1), the Korea Communications Commission shall verify the relevant corporate registration certificate (applicable only if such applicant is a corporation) through administrative data matching under Article 36 (1) of the Electronic Government Act.

(3) If the Korea Communications Commission deems it necessary to review an application under paragraph (1), it may request the applicant to submit data or may hear the applicant's opinion.

(4) Upon receipt of an application under paragraph (1), the Korea Communications Commission shall examine whether the application meets criteria for each standard subject to the review under Article 9-3 and shall notify the applicant of the outcomes of the review within 90 days from the date when such application is filed; provided, the period may be extended by up to 30 days in special circumstances by giving notice of the reasons therefor.

(5) Where the Korea Communications Commission designates an identity verification agency based on the results of the examination under paragraph (4), it shall issue a certificate of designation as an identity verification agency to the applicant and shall

publish a public notice of the details of designation, including the name, location, and date of designation of the identity verification agency, in the Official Gazette.

(6) Matters necessary for procedures and methods for the application for designation and the review on the designation under the provisions of paragraphs (1) through (5) shall be prescribed and publicly notified by the Korea Communications Commission.

[This Article Added on Aug. 29, 2011]

Article 9-5 (Identity verification agency's request for verification of electronic data on resident registration) When a person designated as an identity verification agency under Article 23-3 (1) of the Act (hereinafter referred to as "identity verification agency") needs to verify the identities of a child under 14 years of age and the legal representative of the child, it may request the Minister of the Interior and Safety to verify relevant electronic data on resident registration under Article 30 (1) of the Resident Registration Act.

[This Article Added on Jul. 17, 2018]

[Previous Article 9-5 moved to Article 9-6 <Jul. 17, 2018>]

Article 9-6 (Temporary or permanent discontinuation of identity verification service) (1) When an identity verification agency intends to disclose its service temporarily or permanently in accordance with Article 23-3 (2) or (3) of the Act, it shall notify users of the following matters:

1. The reasons for the temporary or permanent discontinuation;
2. The date and time of the temporary or permanent discontinuation (in the case of temporary discontinuation, including the date and time of resumption of the service);
3. Restrictions on the use of alternative means and personal information (only applicable to the temporary discontinuation);
4. The destruction of alternative means and personal information (applicable only to permanent discontinuation).

(2) When an identity verification agency reports the temporary or permanent discontinuation of its identity verification service in accordance with Article 23-3 (2) or (3) of the Act, it shall submit a report on the temporary or permanent discontinuation of identity verification service to the Korea Communications Commission, along with the following documents:

1. A notice of the matters under paragraph (1);
2. A document concerning a plan to restrict the use or to destroy alternative means and personal information;
3. A document regarding a plan for protective measures to be taken by users;
4. The certificate of designation as an identity verification agency (applicable only to permanent discontinuation).

(3) Detailed matters related to procedures, guidelines, methods, etc. for notification and reporting of temporary or permanent discontinuation under paragraph (1) or (2) shall be determined and publicly notified by the Korea Communications Commission.

[This Article Added on Aug. 29, 2011]

[Moved from Article 9-5; previous Article 9-6 Is moved to Article 9-7 <Jul. 17, 2018>]

Article 9-7 (Suspension of identity verification services or revocation of designation of identity verification agencies) (1) The criteria for suspension of the identity verification service or revocation of designation of an identity verification agency under Article 23-4 (1) of the Act are as shown in Appendix 1. (1) The criteria for suspension of the identity verification service or revocation of designation of the identity verification agency under Article 23-4 (1) of the Act are as shown in Appendix 1.

[This Article Added on Aug. 29, 2011]

[Moved from Article 9-6 <Jul. 17, 2018>]

Article 10 (Information and communication services requiring creation and processing of connecting information) "Information and communications services prescribed by Presidential Decree" in Article 25 (1) 4 of the Act means any of the following information and communication services:

1. The service of notifying users of matters to be notified in accordance with statutes and regulations through a certified electronic document intermediary under subparagraph 10 of Article 2 of the Framework Act on Electronic Documents and Transactions;
2. The service of transmitting personal credit information about an individual to the credit data subject himself or herself through a MyData company as defined in subparagraph 9-3 of Article 2 of the Credit Information Use and Protection Act upon a request for transmission under Article 33-2 (1) of that Act;

3. Other services similar to those under subparagraphs 1 and 2, which are publicly notified by the Korea Communications Commission as the Commission deems it essential to create, provide, use, compare, or link connecting information (hereinafter referred to as "connecting information") or perform other similar acts (hereinafter referred to as "processing") under the provisions, with the exception of the subparagraphs, of Article 23-5 (1) of the Act.

(2) Where the Korea Communications Commission intends to publicly notify the services under paragraph (1) 3, it shall reach an agreement with the Personal Information Protection Commission.

[This Article Added on May 20, 2025]

Article 11 (Approval procedures for creation and processing of connecting information) (1) Where an identity verification agency and a provider of information and communications services intend to obtain approval for the creation and processing of connecting information together under Article 23-5 (1) 4 of the Act, they shall submit to the Korea Communications Commission an application for approval for the creation and processing of connecting information as prescribed and publicly notified by the Korea Communications Commission, along with the following documents:

1. A business plan stating the current status of the organization, human resources, facilities, etc. of the identity verification agency and the provider of information and communications services;
2. Documents proving that detailed review criteria for each item subject to review under Article 9-3 are met;
3. Articles of incorporation or bylaws of organization (applicable only to corporations or organizations) of the identity verification agency and the provider of information and communications services;
4. Other documents prescribed and publicly notified by the Korea Communications Commission, which are necessary for ascertaining the expertise in creating and processing connecting information, the soundness of the financial structure, etc.

(2) Upon receipt of an application for approval for the creation and processing of connecting information under paragraph (1), the Korea Communications Commission shall verify the relevant corporation registration certificate (applicable only to corporations)

through administrative data matching under Article 36 (1) of the Electronic Government Act.

(3) If the Korea Communications Commission deems it necessary to review an application under paragraph (1), it may request the applicant to submit data or may hear the applicant's opinion.

(4) Upon receipt of an application under paragraph (1), the Korea Communications Commission shall examine whether the application meets the detailed examination criteria for each matter for approval under Article 12 within 90 days from the date of receipt of the application and notify the applicant of whether the application has been approved; provided, in the event of unavoidable circumstances, the period may be extended up to 30 days after informing the applicant of the reason.

(5) Except as provided in paragraphs (1) through (4), details necessary for approval for the creation and processing of connecting information shall be determined and publicly notified by the Korea Communications Commission.

[This Article Added on May 20, 2025]

Article 12 (Detailed review criteria for each items subject to review for approval) (1) The detailed review criteria for each items subject to review for approval under Article 23-5 (2) of the Act shall be as follows:

1. Appropriateness and innovativeness of the realization of services to be provided:
   (a) Necessity of creating and processing connecting information for the realization of services to be provided;
   (b) Differentiation from existing similar services;
2. Adequacy of procedures for creating and processing connecting information: Adequacy of procedures for creating and processing connecting information under relevant statutes, regulations, and internal regulations;
3. Plans for physical, technical, and administrative measures to ensure safety in creating and processing connecting information: Feasibility of plans for the measures under the subparagraphs of Article 13 (1);
4. Adequacy of measures to protect the rights of users:
   (a) Measures to protect users' rights, such as suspension of creation and processing of connecting information and deletion of connecting information;

(b) Procedures for receipt and handling of user complaints;

(c) Measures to prevent user damage and secure safety;

5. Impacts and effects on relevant markets and user benefits:

(a) Impacts and effects of services to be provided on the relevant markets, including the invigoration of relevant industries and the reduction of costs;

(b) Impacts and effects of services to be provided on user benefits, including convenience of use and economic benefits.

(2) Matters necessary for guidelines and methods for the evaluation of the detailed review criteria for each items subject to review for approval under paragraph (1) shall be prescribed and publicly notified by the Korea Communications Commission.

[This Article Added on May 20, 2025]

Article 13 (Physical, technical, and administrative measures by identity verification agencies)

(1) An identity verification agency shall take the following physical, technical and administrative measures to ensure the safety of the creation and processing of connecting information under Article 23-6 (1) of the Act;

1. Measures regarding the matters specified in the items of Article 9-3 (1) 1;
2. Formulation and implementation of internal regulations for the creation and processing of connecting information, such as designation of a person in charge of overall physical, technical and administrative measures;
3. Security control of connecting information creating software;
4. Measures to prevent forgery or falsification of connecting information;
5. Recording and storage of verification data on creation and processing of connecting information;
6. Other measures determined and publicly notified by the Korea Communications Commission in relation to ensuring safety in the creation and processing of connecting information.

(2) An entity using connecting information referred to in the main clause of Article 23-5 (4) of the Act (hereinafter referred to as "entity using connecting information") shall store and manage the connecting information separately from resident registration numbers under Article 23-6 (2) of the Act and shall take the following measures (hereinafter referred to as "security measures") to prevent the connecting information from being lost, stolen, leaked,

forged, falsified, or damaged:

1. Establishment and implementation of internal regulations for secure processing of connecting information, such as designation of a person in charge of general supervision and control of security measures;
2. Processing of connecting information within the scope of the purpose for which the connecting information is provided;
3. Separation, storage, and management of resident registration numbers and connecting information where storing resident registration numbers;
4. Application of encryption technology to safely store and transmit connecting information;
5. Formulation and implementation of a response plan in case of a cyber security incident, such as loss or theft of connecting information;
6. Recording and retention of data regarding entities providing connecting information, the time connecting information is provided, etc.;
7. Other measures determined and publicly notified by the Korea Communications Commission to prevent the loss, theft, leakage, forgery, falsification, or damage of connecting information.

(3) Except as provided in paragraphs (1) and (2), detailed matters necessary for the physical, technical, and administrative measures taken by identity verification agencies and for the security measures taken by entities using connecting information shall be determined and publicly notified by the Korea Communications Commission.

[This Article Added on May 20, 2025]

Article 14 (Entities subject to inspection of operational and managerial status) An identity verification agency or an entity using connecting information subject to inspection of current status under Article 23-6 (3) of the Act (hereinafter referred to as "inspection of current status") shall be as follows:

1. In the case of an identity verification agency: A person who has created or processed connecting information in accordance with Article 23-5 (1) of the Act and has created or processed 1,000 or more connecting information cases;
2. In the case of an entity using connecting information: A person who has received at least 1,000 connecting information cases from an identity verification agency under

Article 23-5 (1) of the Act.

[This Article Added on May 20, 2025]

Article 15 (Procedures for inspection of current status) A public official who inspects the current status with regard to the physical, technical, and administrative measures taken by an identity verification agency and the security measures taken by an entity using connecting information under Article 23-6 (3) of the Act shall notify the agency of the following matters by no later than 7 days prior to the inspection; provided, if it is deemed urgent or if it is deemed impractical to achieve the purpose of the inspection of the current status due to evidence destruction, etc., prior notice may be omitted:

1. Grounds for and purpose of the inspection;
2. Date and time of the inspection;
3. Personal information of the inspecting person;
4. Details of the inspection.

[This Article Added on May 20, 2025]

Article 16 (Specialized organization for inspection of current status) "Specialized organization prescribed by Presidential Decree" in Article 23-6 (4) of the Act means the Korea Internet and Security Agency under Article 52 of the Act (hereinafter referred to as the "Internet and Security Agency").

[This Article Added on May 20, 2025]

Article 16-2 Deleted. <Aug. 4, 2020>

Article 17 Deleted. <Aug. 4, 2020>

Article 17-2 Deleted. <Aug. 4, 2020>

Article 18 Deleted. <Aug. 4, 2020>

Article 18-2 Deleted. <Aug. 4, 2020>

Article 19 (Scope of persons required to designate domestic agents) (1) "Person who meets the criteria prescribed by Presidential Decree" in Article 32-5 (1) of the Act means any of the following persons: <Amended on Aug. 4, 2020>

1. A person whose sales for the preceding year (if the person is a corporation, referring to the preceding business year) reach or exceed 1 trillion won;
2. A person whose sales from information and telecommunications services for the preceding year (if the person is a corporation, referring to the preceding business year) reach or exceed 10 billion won;
3. Deleted; <Aug. 4, 2020>
4. A person who caused or is likely to cause an incident or accident significantly undermining security in using information and communication services in violation of this Act and has been consequently required by the Korea Communications Commission to submit relevant articles, documents, etc. under Article 64 (1) of the Act.

(2) Sales referred to in paragraphs (1) 1 and 2 shall be based on the amount determined by converting sales into Korean won at the average foreign exchange rate for the preceding year (if the person is a corporation, referring to the preceding business year). [This Article Added on Mar. 19, 2019]

Article 20 Deleted. <Sep. 29, 2011>

Article 21 Deleted. <Sep. 29, 2011>

Article 22 Deleted. <Sep. 29, 2011>

CHAPTER V PROTECTION OF USERS IN INFORMATION AND COMMUNICATIONS NETWORKS

Article 23 (Policy measures on protection of youths) "Matters prescribed by Presidential Decree" in Article 41 (1) 4 of the Act means the following measures: <Amended on Jan. 28, 2009; Aug. 29, 2011>

1. Promotion of the development and dissemination of information useful to youths;
2. Encouragement of and support for youths' voluntary activities for protecting themselves from harmful information, such as information of obscenity or violence, circulated through information and communications networks;
3. Encouragement of and support for voluntary activities conducted by parents, teachers, or nongovernmental organizations for surveillance, counseling, and remedial measures

for the protection of youths;

4. Assistance in the establishment of a system for the cooperation of providers of information and communications services for the protection of youths;
5. Other measures incidental to the implementation of policy measures under Article 41 (1) of the Act.

Article 24 (Labeling of media product harmful to youths) (1) A person who provides a media product harmful to youths, as defined under Article 42 of the Act, shall label it with an easily noticeable audio, text, or video warning stating that no person under 19 years shall use the same.

(2) If a person who shall put a label required by paragraph (1) provides information through the Internet, he or she shall also put an electronic label warning that it is a media product harmful to youths with symbols, marks, letters, or numbers.

(3) The Korea Communications Commission shall prescribe specific methods for labeling under paragraphs (1) and (2), taking into consideration the categories of information, etc., and shall publish a public notice of the methods in the Official Gazette.

Article 25 (Scope of persons obliged to designate persons responsible for protection of youths) "Who meets the criteria prescribed by Presidential Decree, such as the average number of daily users and sales" in Article 42-3 (1) of the Act means a person who meets all the following criteria: <Amended on Aug. 29, 2011; Sep. 14, 2012>

1. A person falling under either of the following:
   (a) A person in whose case the average number of users per day during 3 months immediately before the end of the immediately preceding year is at least 100,000 persons;
   (b) A person whose sales in the previous year (in the case of a corporation, the previous business year) in the information and communications service sector were at least one billion won;
2. A person who has at least 3 years of work experience (including work experience prior to obtaining a degree) in the field of information security or information technology, after obtaining a bachelor's degree in the field of information security or information technology in the Republic of Korea or abroad.

Article 26 (Duties of persons responsible for protection of youths) A person responsible for protection of youths under Article 42-3 (1) of the Act shall perform the following duties in order to protect youths from information harmful to youths on information and communications networks (hereinafter referred to as "harmful information"):

1. Formulation of a plan for protection of youths from harmful information;
2. Measures for restricting or controlling youths' access to harmful information;
3. Education of persons engaged in information and communications services for the protection of youths from harmful information;
4. Counseling on damage inflicted by harmful information and the settlement of grievances;
5. Other matters necessary to protect youths from harmful information.

Article 27 (Deadline for designation of persons responsible for protection of youths) A person responsible for protection of youths under Article 42-3 (1) of the Act shall be designated by no later than the end of April each year.

Article 28 (Preservation of video or audio information) (1) "Information provider prescribed by Presidential Decree" in Article 43 (1) of the Act means a person who distributes information through telecommunications lines; provided, broadcasting business operators, CATV relay broadcasting business operators, and electronic signboard broadcasting business operators under subparagraphs 3, 6, and 12 of Article 2 of the Broadcasting Act, among persons who distribute information according to a certain program schedule, using the word "broadcasting", "television" or "radio" in their names, shall be excluded herefrom. <Amended on Aug. 29, 2011>

(2) An information provider under Article 43 of the Act shall preserve relevant information for 6 months from the time when the information is provided for use.

Article 29 Deleted. <Nov. 28, 2014>

Article 30 Deleted. <Nov. 28, 2014>

Article 31 (Scope of user information that can be requested) "Minimum information prescribed by Presidential Decree" in Article 44-6 (1) of the Act means the following information: <Amended on Aug. 29, 2011>

1. Name;
2. Address;
3. Other information that the defamation dispute conciliation division under Article 44-10 of the Act (hereinafter referred to as "defamation dispute conciliation division") deems necessary for filing a civil or criminal complaint, including the contact information of users involved.

Article 32 (Procedures for requesting provision of information) (1) A person who intends to request the provision of the information of users involved pursuant to Article 44-6 (1) of the Act (hereinafter referred to as "claimant") may file a claim with the defamation dispute conciliation division, stating the following matters therein, along with supporting materials:

1. The claimant's name, address, and contact information (referring to telephone numbers, e-mail addresses, etc.);
2. The category of the lawsuit to be filed and remedies sought;
3. The type of violated rights and specific facts relevant to the violation of rights by users involved.

(2) Where the defamation dispute conciliation division finds it necessary to make a decision on whether to provide information under Article 44-6 (2) of the Act, it may permit the claimant to present his or her arguments.

Article 33 (Procedures for provision of information) (1) Upon receipt of a request from a claimant to provide information, the defamation dispute conciliation division shall make a decision on whether to provide the information of users involved and shall notify the claimant of its decision.

(2) When the defamation dispute conciliation division decides to provide information, it shall request the relevant provider of information and communications services to provide information under Article 31. In such cases, the provider of information and communications services shall comply with such request, unless there is a compelling reason not to do so. <Amended on Jan. 28, 2009>

(3) A provider of information and communications services shall notify the users involved of such provision of information under paragraph (2). <Amended on Jan. 28, 2009>

(4) The defamation dispute conciliation division shall keep documents relating to the provision of user information for 5 years.

Article 34 (Requests to order restrictions on handling unlawful information) (1) When the head of a related central administrative agency (including the head of an investigative agency with regard to a photograph or its duplicate (including duplicates of duplicates) under Article 14 of the Act on Special Cases concerning the Punishment of Sexual Crimes out of information provided in Article 44-7 (1) 9 of the Act; hereafter in this Article the same shall apply) intends to request the Korea Communications Commission pursuant to Article 44-7 (3) of the Act to order a provider of information and communications services or the manager or operator of a message board to refuse, suspend, or restrict the management of the information specified in Article 44-7 (1) 7 through 9 of the Act, he or she shall submit to the Korea Communications Commission a written request stating the following matters, along with evidentiary materials: <Amended on Jan. 28, 2009; Sep. 22, 2016; Jun. 11, 2019>

1. The purpose of and reasons for a request;
2. Relevant statutes or regulations and the details of violations;
3. A list of relevant information and a person by whom the relevant information is provided;
4. The titles or names and contact information, such as addresses, telephone numbers, and e-mail addresses, of the provider of information and communications services or the manager or operator of the message board and users involved.

(2) If the Korea Communications Commission finds any defect in the documents submitted pursuant to paragraph (1), it may request the head of a related central administrative agency to rectify the defect immediately. In such cases, at least 5 more days shall be given for rectification.

(3) If the head of a related central administrative agency fails to rectify a defect even until the end of a period given for the rectification requested under paragraph (2), the Korea Communications Commission may return the request and evidential materials submitted pursuant to paragraph (1) to the head of the related central administrative agency.

[Title Amended on Sep. 22, 2016]

Article 35 (Grounds for exception from submission of opinions) "Ground prescribed by Presidential Decree" in Article 44-7 (4) 2 of the Act means any of the following cases: <Amended on Aug. 29, 2011>

1. Where a user involved is not identifiable (limited to the submission of a user's opinion);
2. Where the facts relevant to an order have already been proved objective by a final judgment of a court or by other decisions and thus issuing the order to hear an opinion is unnecessary.

Article 35-2 (Technical and administrative measures to prevent circulation of unlawful information) (1) "Provider that ... meets the criteria prescribed by Presidential Decree" in the provisions, with the exception of the subparagraphs, of Article 44-7 (5) of the Act means a person who engages in the business of transmitting data to users by temporarily storing copies of data, received from an original server, on domestic servers in order to provide another party's information and communications services and whose sales in the information and communications service sector for the previous year (in the case of a corporation, referring to the previous fiscal year) were 1 billion won or more.

(2) "Period prescribed by Presidential Decree" in Article 44-7 (5) 3 of the Act means 2 years.

(3) "Measures prescribed by Presidential Decree" in Article 44-7 (5) 4 of the Act means the following measures:

1. Designation of a person in charge of preventing the circulation of information prescribed in each subparagraph of Article 44-7 (1) of the Act (hereafter referred to as "illegal information" in this paragraph);
2. Notifying the Korea Communications Commission of the circulation of illegal information, if he or she becomes aware thereof;
3. Stipulating matters regarding the prevention of circulation of illegal information in the terms and conditions of use or in contract documents.

[This Article Added on May 20, 2025]

[Previous Article 35-2 moved to Article 35-3 <May 20, 2025>]

Article 35-3 (Persons responsible for preventing circulation of illegally filmed materials or the like) (1) A provider of information and communications services obligated to designate a

person responsible for preventing the circulation of illegally filmed materials or the like pursuant to Article 44-9 (1) of the Act shall be the following persons:

1. A person who provides value-added telecommunications services defined in subparagraph 14 (a) of Article 2 of the Telecommunications Business Act among special value-added telecommunications business operators referred to in Article 22-3 (1) of that Act;
2. Any of the following persons, who has filed a report on the value-added telecommunications business under Article 22 (1) of the Telecommunications Business Act (including a person who falls under any of the subparagraphs of Article 22 (4) of that Act):
   (a) A person who provides information and communication services under Appendix 1-2, posting at least 10 billion won in sales of information and communication services over the preceding year (referring to the preceding business year, in the case of a corporation);
   (b) A person who provides information and telecommunications services under Appendix 1-2 with an average number of users per day of at least 100,000 during the immediately preceding 3 months as of the end of the previous year.

(2) A provider of information and communications services under the subparagraphs of paragraph (1) (hereinafter referred to as "person obligated to designate a person responsible for preventing the circulation of illegally filmed materials or the like") shall designate at least 1 person responsible for preventing the circulation of illegally filmed materials (hereinafter referred to as "illegally filmed materials or the like") under Article 44-9 (1) of the Act (hereinafter referred to as "person responsible for preventing the circulation of illegally filmed materials or the like").

(3) Persons responsible for preventing the circulation of illegally filmed materials or the like shall be any of the following persons:

1. An executive officer who belongs to the person obligated to designate a person responsible for preventing the circulation of illegally filmed materials or the like;
2. The head of the division in charge of preventing the circulation of illegally filmed materials or the like, that is under the control of the person obligated to designate a person responsible for preventing the circulation of illegally filmed materials or the like

(4) A person responsible for preventing the circulation of illegally filmed materials or the like shall receive education (including distance education using information and communications networks) for at least 2 hours every year, including the following, which is delivered by the Korea Communications Commission in cooperation with relevant agencies and organizations:

1. Matters regarding systems and statutes and regulations relating to preventing the circulation of illegally filmed materials or the like;
2. Matters regarding measures necessary to prevent circulation under Article 44-9 (2) of the Act;
3. Matters regarding the criteria for deliberation on illegally filmed materials or the like by the Korea Communications Standards Commission under Article 18 of the Act on the Establishment and Operation of Korea Communications Commission (hereinafter referred to as the "Korea Communications Standards Commission");
4. Other matters deemed by the Korea Communications Commission necessary for preventing the circulation of illegally filmed materials or the like

[This Article Added on Dec. 8, 2020]

[Moved from Article 35-2 <May 20, 2025>]

Article 36 (Establishment and management of defamation dispute conciliation division, and conciliation of disputes) (1) A meeting of the defamation dispute conciliation division shall be convened by the head of the defamation dispute conciliation division.

(2) When the head of the defamation dispute conciliation division intends to hold a meeting of the division, he or she shall determine the date, time, and place of meeting and items on the agenda and shall notify the conciliators thereof by no later than 7 days before the opening of the meeting, except in unavoidable circumstances.

(3) A majority of the conciliators of the defamation dispute conciliation division shall constitute a quorum, and any resolution thereof shall require the concurring votes of at least a majority of those present.

(4) The head of the defamation dispute conciliation division shall be appointed by the Chairman of the Korea Communications Standards Commission, from among conciliators. <Amended on Dec. 8, 2020>

(5) No meeting of the defamation dispute conciliation division shall be open to the public; provided, if it is deemed necessary, the defamation dispute conciliation division may resolve to permit parties to a dispute or interested parties to sit in on a meeting.
(6) Deleted. <Sep. 29, 2011>
(7) Except as provided in this Decree, the establishment, organization, and management of the defamation dispute conciliation division and other matters necessary for the conciliation of disputes shall be determined by the resolution of the Korea Communications Standards Commission.

CHAPTER VI SECURING OF STABILITY OF INFORMATION AND COMMUNICATIONS NETWORKS

Article 36-2 (Scope of devices and the like connected to information and communications networks) "Devices, equipment, and facilities prescribed by Presidential Decree" in Article 45 (1) 2 of the Act means the following devices, equipment, and facilities (hereinafter referred to as "devices and the like connected to information and communications networks") in any field specified in Appendix 1-3:

1. Devices, equipment, and facilities that have caused or are likely to cause a cyber security incident;
2. Devices, equipment, and facilities that pose a serious risk to ensuring the security of information and communications networks and the reliability of information, if a cyber security incident occurs.

[This Article Added on Dec. 8, 2020]
[Previous Article 36-2 moved to Article 36-3 <Dec. 8, 2020>]

Article 36-3 (Pre-inspection standards for information security) The pre-inspection standards for information security under Article 45-2 (2) of the Act shall be determined and publicly notified by the Minister of Science and ICT in consideration of the following matters: <Amended on Mar. 23, 2013; Jul. 26, 2017>

1. The structure and operating environment of the system for building information and communication networks or providing information and communication services;

2. Identification and risk of assets to be protected, such as hardware, programs, and content for the operation of the system under subparagraph 1;
3. Current status of establishment and implementation of countermeasures.

[This Article Added on Aug. 17, 2012]

[Moved from Article 36-2; Previous Article 36-3 moved to Article 36-4 <Dec. 8, 2020>]

Article 36-4 (Business subject to information security pre-inspection recommendation) (1) "Information and communications services or telecommunications business determined by Presidential Decree" in Article 45-2 (2) 1 of the Act means the information and communications services or telecommunications businesses that require at least 500 million won (referring to an amount exclusive of costs incurred in merely purchasing hardware and software) for investment in information systems.

(2) "Information and communications services or telecommunications business determined by Presidential Decree" in Article 45-2 (2) 2 of the Act means the information and communications services or the telecommunications businesses that the Minister of Science and ICT fully or partially subsidizes projects for searching for and nurturing new information and communications services or the telecommunications businesses. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Added on Aug. 17, 2012]

[Moved from Article 36-3; previous Article 36-4 moved to Article 36-5 <Dec. 8, 2020>]

Article 36-5 (Methods and procedures for information security pre-inspection) (1) The information security pre-inspection under Article 45-2 (2) of the Act shall be conducted by means of written inspection, on-site inspection, or remote inspection (referring to the inspection of security-related matters by accessing the system under subparagraph 1 of Article 36-3 through an information and communications network from the outside). <Amended on Dec. 8, 2020>

(2) The information security pre-inspection under Article 45-2 (2) of the Act shall be conducted in the following order:

1. Preparation for the pre-inspection;
2. Review on designs;

3. Application of countermeasures for protection;

3. Current status of establishment and implementation of countermeasures for protection.

5. Arrangement of results of the pre-inspection.

(3) Upon recommendation from the Minister of Science and ICT under Article 45-2 (2) of the Act, a person may conduct the information security pre-inspection by himself or herself or request the Korea Internet and Security Agency or an external specialized organization to conduct the information security pre-inspection on his or her behalf. In such cases, only persons who meet the qualification standards for technical human resources for information security shown in Appendix 2 may conduct the information security pre-inspection. <Amended on Mar. 23, 2013; Jul. 26, 2017; May 20, 2025>

(4) Except as provided in paragraphs (1) through (3), detailed matters related to methods and procedures for information security pre-inspection shall be determined and publicly notified by the Minister of Science and ICT. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Added on Aug. 17, 2012]

[Moved from Article 36-4; previous Article 36-5 moved to Article 36-6 <Dec. 8, 2020>]

Article 36-6 (Fees for information security pre-inspection) (1) Where a person who has received a recommendation from the Minister of Science and ICT under Article 45-2 (2) of the Act requests the Korea Internet and Security Agency or an external specialized organization to conduct the information security pre-inspection on his or her behalf, the person shall pay fees therefor to the Korea Internet and Security Agency or the external specialized organization. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(2) The Minister of Science and ICT shall determine and publicly notify the calculation criteria for information security pre-inspection in consideration of the following matters: <Amended on Mar. 23, 2013; Jul. 26, 2017>

1. The scale of information and communications services or telecommunications businesses subject to information security pre-inspection;

2. Expertise of persons participating in information security pre-inspection;

3. The period required for information security pre-inspection.

[This Article Added on Aug. 17, 2012]

[Moved from Article 36-5; previous Article 36-6 moved to Article 36-7 <Dec. 8, 2020>]

Article 36-7 (Designation of chief information security officers and prohibition on dual office holding) (1) "Executive officers and employees meeting the criteria prescribed by Presidential Decree" in the main clause of Article 45-3 (1) of the Act means persons categorized as follows: <Add on Dec. 7, 2021; Dec. 31, 2024>

1. Any of the following providers of information and telecommunications services: The business owner or its representative:
   (a) A person whose capital (referring to the paid-in capital in cases of a corporation and the appraised value of assets for business use if the person is not a corporation) is not more than 100 million won;
   (b) A small enterprise set forth in Article 2 (2) of the Framework Act on Small and Medium Enterprises;
   (c) A medium enterprise defined in Article 2 (2) of the Framework Act on Small and Medium Enterprises, which does not fall under any of the following:
   (i) A telecommunications business operator under the Telecommunications Business Act;
   (ii) A person required to obtain certification of an information security management system pursuant to Article 47 (2) of the Act;
   (iii) A personal information controller required to disclose its privacy policy under Article 30 (2) of the Personal Information Protection Act;
   (iv) A mail order distributor required to file a report under Article 12 of the Act on the Consumer Protection in Electronic Commerce;
2. Any of the following providers of information and communications services: Directors (including persons under Article 401-2 (1) 3 of the Commercial Act and executive directors under Article 408-2 of that Act):
   (a) A person whose total assets as of the end of the immediately preceding business year amount to at least 5 trillion won;
   (b) A person whose total assets as of the end of the immediately preceding business year amount to at least 500 billion won, among those required to obtain certification of an information security management system under Article 47 (2) of the Act;
3. A provider of information and communications services who does not fall under subparagraph 1 or 2: Any of the following persons:

(a) The business owner or representative;

(b) Directors (including persons prescribed in Article 401-2 (1) 3 of the Commercial Act and executive directors prescribed in Article 408-2 of that Act);

(c) The head of a department that has general supervision and control of information security-related affairs.

(2) "Provider of information and communications services whose total assets, sales, and the like meet the criteria prescribed by Presidential Decree" in the proviso of Article 45-3 (1) of the Act means a person referred to in any item of paragraph (1) 1 as a provider of information and communications services. <Amended on Dec. 7, 2021>

(3) Where a person falling under the proviso of Article 45-3 (1) of the Act fails to report his or her chief information security officer, he or she shall be deemed to have designated the business owner or representative as the chief information security officer. <Added on Dec. 7, 2021>

(4) A chief information security officer required to be designated and reported by a provider of information and communications services pursuant to Article 45-3 (1) and (7) of the Act shall have any of the following qualifications; in such cases, a degree in the field of information security or information technology refers to the completion of and graduation from courses offered by departments provided in the items of subparagraph 1 of the remarks of Appendix 1 of the Enforcement Decree of the Electronic Financial Transactions Act at a university or college defined in the subparagraphs of Article 2 of the Higher Education Act or other degrees recognized as equivalent to or higher than aforementioned degrees under other relevant statutes or regulations; and the duties in the field of information security or information technology refers to the duties provided in subparagraphs 3 and 4 of those remarks: <Amended on Dec. 7, 2021; Aug. 9, 2022>

1. A person who has obtained at least a master's degree in the field of information security or information technology in the Republic of Korea or abroad;
2. A person who has at least three years of work experience (including work experience prior to obtaining a degree) in the field of information security or information technology, after obtaining a bachelor's degree in the field of information security or information technology in the Republic of Korea or abroad;

3. A person who has at least 5 years of work experience (including work experience prior to obtaining a degree) in the field of information security or information technology, after obtaining an associate degree in the field of information security or information technology in the Republic of Korea or abroad;
4. A person who has at least 10 years of work experience in the field of information security or information technology;
5. A person who has obtained the qualification of a certification examiner of information security management systems under Article 47 (6) 5;
6. A person who has at least 1 year of work experience as the head of a department in charge of the information security-related affairs of the relevant provider of information and communications services.

(5) "Provider of information and communications services whose total assets, sales, and the like meet the criteria prescribed by Presidential Decree" in Article 45-3 (3) of the Act means a person specified in any item of paragraph (1) 2 as a provider of information and communications services; provided, a person who is a holding company under subparagraph 2 of Article 2 of the Act on Monopoly Regulation and Fair Trade and does not engage in any other business for profit than the management and administration of its subsidiaries and the business incidental thereto shall be excluded from those specified in paragraph (1) 2 (a). <Amended on Dec. 7, 2021; Dec. 26, 2022; Dec. 26, 2023>

(6) The chief information security officer required to be designated and reported by a provider of information and communications services under paragraph (5) shall be a full-time worker with the qualifications prescribed in paragraph (4) together with any of the following qualifications; in such cases, the duties in the field of information security or information technology refer to the duties under subparagraphs 3 and 4 of the remarks of Appendix 1 of the Enforcement Decree of the Electronic Financial Transactions Act: <Amended on Dec. 7, 2021; Aug. 9, 2022>

1. A person who has at least 4 years of work experience in the field of information security (including work experience prior to obtaining any of the degrees under paragraph (4) 1 through 3 or the qualification prescribed in subparagraph 5 of that paragraph);
2. A person who has at least 5 years of work experience (including work experience prior to obtaining any of the degrees under paragraph (4) 1 through 3 or the qualification

prescribed in subparagraph 5 of that paragraph) in the field of information security or information technology (out of the 5 years, at least 2 years of work experience in the field of information security are required).

[This Article Wholly Amended on Jun. 11, 2019]

[Moved from Article 36-6; previous Article 36-7 moved to Article 36-8 <Dec. 8, 2020>]

Article 36-8 (Methods and procedures for reporting on chief information security officers) Any information and communications service provider obligated to designate and report a chief information security officer under the proviso of Article 45-3 (1) of the Act shall submit to the Minister of Science and ICT a report on the designation of the chief information security officer prescribed by Decree of the Ministry of Science and ICT within 180 days from the date he or she becomes obligated to report such officer. <Amended on Jul. 26, 2017; Jun. 11, 2019; Dec. 7, 2021>

[This Article Added on Nov. 28, 2014]

[Moved from Article 36-7; previous Article 36-7 moved to Article 36-8 <Dec. 8, 2020>]

Article 36-9 (Scope of programs of Council of Chief Information Security Officers) "Joint programs prescribed by Presidential Decree" in Article 45-3 (5) of the Act means the following programs: <Amended on Nov. 28, 2014; Jun. 11, 2019>

1. Assistance in policy research, studies, and formulation to enable information and communications service providers to strengthen the protection of information;
2. Analysis on a cyber security incident and the study of measures following the use of information and communications services;
3. Improvement of information and communications service providers' ability and expertise of the protection of information, including education of chief information security officers;
4. International exchange and cooperation in relation to information and communications services security;
5. Other programs necessary for the security of information and communications systems and the safe management of information.

[This Article Added on Aug. 17, 2012]

[Moved from Article 36-8 <Dec. 8, 2020>]

Article 37 (Protective measures by integrated information and communication facility operators, etc.) (1) "Person who meets the standards prescribed by Presidential Decree" in the provisions, with exception of the subparagraphs, of Article 46 (1) of the Act means a person specified in any of the following subparagraphs; provided, the foregoing shall not apply to public institutions under Article 3 of the Enforcement Decree of the Public Archives Act. <Added on Jul. 3. 2023>

1. A person specified in Article 46 (1) 1 of the Act whose computer room floor area in the integrated and communications facilities that the person operates and manages is at least 500 square meters;
2. A person specified in Article 46 (1) 2 of the Act satisfies all the following requirements:
   (a) A person whose computer room floor area in the integrated information and communications facilities that the person operates and manages shall be at least 500 square meters;
   (b) A person whose sales from information and telecommunications services for the preceding year (if the person is a corporation, referring to the preceding business year) shall reach or exceed 10 billion won;
   (c) The average number of domestic users per day for 3 months immediately before the end of the preceding year shall be at least 1 million;

(2) A data integrated information and communication facility operators, etc. under the provisions, with the exception of the subparagraphs, of Article 46 (1) of the Act (hereinafter referred to as "integrated information and communication facility operators, etc.") shall take the following protective measures to ensure the stable operation of information and communications facilities: <Amended on Jan. 28, 2009; Jun. 11, 2019; Dec. 7, 2021; Jul. 3, 2023>

1. Technical and administrative measures for controlling and monitoring access by persons who have no authority to access information and communications facilities;
2. Physical and technical measures for uninterrupted and stable operation of information and communications facilities and for protecting information and communications facilities from various disasters and threats, such as fire, earthquake, flood, and terrorism;

3. Measures for selecting and placing personnel for the stable management of information and communications facilities;
4. Formulation and implementation of an internal control plan for the stable operation of information and communications facilities (including an emergency plan);
5. Preparation and implementation of technical and administrative measures to contain the spread of cyber security incidents.

(3) The Minister of Science and ICT shall collect opinions from related business operators and determine and publicly notify detailed guidelines for protective measures under paragraph (2). <Amended on Mar. 23, 2013; Jul. 26, 2017; Jul. 3, 2023>

[Title Amended on Jul. 3, 2023]

Article 38 (Insurance) (1) A integrated information and communication facility operator under Article 46 (1) 1 of the Act (hereinafter referred to as "integrated information and communication facility operator") shall take out a liability insurance policy simultaneously with the commencement of his or her business under Article 46 (2) of the Act. <Amended on Jul. 3. 2023>

(2) The amount of liability insurance that a business operator is obligated to purchase under paragraph (1) shall be as specified in Appendix 3. <Amended on Aug. 29, 2011; Jun. 11, 2019; Dec. 8, 2020>

Article 39 (Frequency and method of inspection of implementation of protective measures) (1) The Minister of Science and ICT shall conduct an annual inspection of the implementation of protective measures pursuant to Article 46 (3) of the Act (hereinafter referred to as the "inspection of implementation").

(2) If the inspection of implementation is related to the field of work of another administrative agency, the Minister of Science and ICT shall consult in advance with the head of that agency.

[This Article Added on Jul. 3, 2023]

Article 40 (Method of report by integrated information and communication facility operator, etc. on service interruption) (1) "Period prescribed by Presidential Decree" in Article 46 (6) of the Act means the period falling under any of the following:

1. For 30 or more minutes consecutively;
2. If there are 2 or more service interruptions within a 24-hour period, the sum of the interruptions is 45 minutes or more.

(2) A report under Article 46 (6) of the Act shall include the following matters:

1. The date, time, and place where the provision of information and communications services is interrupted;
2. Cause for the interruption of information and communication services and the details of damage;
3. Emergency measures taken;
4. Response and recovery plans;
5. Plan for future measures;
6. Other matters necessary to cope with and recover from the interruption of the provision of information and communications services.

(3) When the provision of information and communications services is interrupted as described in Article 46 (6) of the Act, the integrated information and communication facility operator, etc. shall make a report in writing to the Minister of Science and ICT.

[This Article Added on Jul. 3, 2023]

Article 41 (Obligation of lessees of integrated information and communication facilities to take measures) A provider of information and communication services that leases and exclusively operates and manages integrated information and communication facilities shall take the following measures in accordance with Article 46 (7) of the Act:

1. The provider shall implement protective measures in accordance with Article 37 (2);
2. Where information and communications services are interrupted for the period specified in each subparagraph of Article 40 (1) due to a disaster, etc., the provider shall report thereon to the Minister of Science and ICT and notify the integrated information and communication facility operator who has leased the facilities thereof. In this case, Article 40 (2) and (3) shall apply mutatis mutandis to the reporting method.

[This Article Added on Jul. 3, 2023]

Article 42 (Specialized organization for protective measures and technical support)

"Specialized organization prescribed by Presidential Decree" in Article 46 (8) of the Act

means any of the following organizations:

1. Public institutions established under Article 4 of the Act on the Management of Public Institutions;
2. A non-profit corporation established with the permission of the Minister of Science and ICT pursuant to Article 32 of the Civil Act that performs tasks related to securing the stability of integrated information and communication facilities;
3. Any other institution or organization recognized by the Minister of Science and ICT as having expertise in the stability of integrated information and communication facilities.

(2) Where the Minister of Science and ICT entrusts the affairs pursuant to Article 46 (8) of the Act, he or she shall give public notice of the specialized organization to be entrusted with the affairs and the details of said affairs.

[This Article Added on Jul. 3, 2023]

Article 43 Deleted. <Aug. 17, 2012>

Article 44 Deleted. <Aug. 17, 2012>

Article 45 Deleted. <Aug. 17, 2012>

Article 46 Deleted. <Aug. 17, 2012>

Article 47 (Methods and procedures for, and scope of, certification of information security management systems) (1) A person who intends to have his or her information security management system certified under Article 47 (1) or (2) of the Act shall file an application for the certification of the information security management system (or an application in an electronic form) with the Korea Internet and Security Agency, an institution designated pursuant to Article 47 (6) of the Act (hereinafter referred to as "certification body for information security management systems"), or an institution designated pursuant to Article 47 (7) of the Act (hereinafter referred to as "examination institution for information security management systems"), along with a statement of the information security management system (or a statement in an electronic format) containing explanations about the following matters: <Amended on Mar. 23, 2013; May 31, 2016>

1. The scope of the information security management system;

2. A list of major information and communications facilities included in the information security management system and the system diagram;
3. The method and procedure for the establishment and operation of the information security management system;
4. A list of major documents related to the information security management system;
5. Details of domestic and foreign certifications obtained for the quality management system in connection with the information security management system.

(2) Where the Korea Internet and Security Agency, a certification body for information security management systems, or an examination institution for information security management systems in receipt of an application referred to in paragraph (1) conducts an examination for certification under Article 47 (6) 1 of the Act (hereinafter referred to as "examination for certification"), it shall consult with the applicant about the scope, time schedule, etc. of certification in accordance with the certification standards, etc. including countermeasures for administrative, technical, and physical protection, determined and publicly notified by the Minister of Science and ICT for certification of information security systems under paragraph (4) of that Article (hereinafter referred to as "public notice of certification of management systems"). <Amended on Mar. 23, 2013; May 31, 2016; Jul. 26, 2017>

(3) The Korea Internet and Security Agency, a certification body for information security management systems, or an examination institution for information security management systems shall, in the case of conducting an examination for certification, examine whether the information security management system established by the applicant for certification meets requirements for public notice of certification of management systems. In such cases, the examination for certification shall be conducted by means of a written examination or on-site examination. <Amended on May 31, 2016>

(4) An examination for certification may be administered only by a certification examiner under Article 53 (1) 1. <Amended on May 31, 2016>

(5) An examination institution for information security management systems shall submit the results of an examination for certification to the Korea Internet and Security Agency or a certification body for information security management systems. <Added on May 31, 2016>

(6) The Korea Internet and Security Agency or a certification body for information security management systems shall establish and operate a certification committee composed of members having abundant knowledge and experience in the information protection field to deliberate on the results of examinations for certification. <Amended on May 31, 2016>

(7) Where an information security management system is found to comply with the requirements of the public notice of certification of management systems as a result of deliberation by the certification committee under paragraph (6), the Korea Internet and Security Agency or the certification body for information security management systems shall issue a certificate of information security management system to the person who applied for certification. <Amended on May 31, 2016>

(8) Except as provided in paragraphs (1) through (7), detailed matters required for application for certification, examination for certification, establishment and operation of the certification committee, issuance of certificates, and others shall be determined and publicly notified by the Minister of Science and ICT. <Amended on Mar. 23, 2013; May 31, 2016; Jul. 26, 2017>

[This Article Wholly Amended on Aug.17, 2012]

[Moved from Article 50; previous Article 47 moved to Article 53 <Aug. 17, 2012>]

Article 48 (Fees for certification of information security management systems) (1) A person who intends to apply for certification pursuant to Article 47 (1) shall pay fees to the Korea Internet and Security Agency, a certification body for information security management systems, or an examination institution for information security management systems. <Amended on May 31, 2016>

(2) The Minister of Science and ICT shall determine and give a public notice of detailed guidelines for the determination of fees for the certification of information security management systems, taking into consideration the number of certification examiners assigned to an examination for certification, the number of days required for the examination for certification, etc. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Added on Aug. 17, 2012]

[Previous Article 48 moved to Article 53-2 <Aug. 17, 2012>]

Article 49 (Scope of persons subject to certification of information security management systems) (1) "Person who renders information and communications network services, as prescribed by Presidential Decree" in Article 47 (2) 1 of the Act means a person who provides information and communications network services in Seoul Special Metropolitan City or any Metropolitan City.

(2) "Person meeting the standards prescribed by Presidential Decree" in Article 47 (2) 3 of the Act means any of the following persons: <Amended on May 31, 2016; Jul. 23, 2024>

1. A person whose sales or revenues in the preceding year were at least 150 billion won and falls under any of the following categories:
   (a) A superior general hospital under Article 3-4 of the Medical Service Act;
   (b) A university or college under Article 2 of the Higher School Act, the number of the enrolled students of which is at least 1000 as of December 31 of the immediately preceding year;
2. A person whose sales in the information and communication service sector amounted to at least 10 billion won in the previous year (referring to the previous business year in the case of a corporation) are least 10 billion won: excluding, however, financial companies under subparagraph 3 of Article 2 of the Electronic Financial Transactions Act;
3. A person whose average daily number of users during the preceding year is at least 1 million; provided, excluding financial companies under subparagraph 3 of Article 2 of the Electronic Financial Transactions.

[This Article Added on Aug. 17, 2012]

[Previous Article 49 moved to Article 53-3 <Aug. 17, 2012>]

Article 49-2 (Scope of persons eligible for special cases concerning certification of information security management systems) (1) Any of the following persons that are medium enterprises defined in Article 2 (2) of the Framework Act on Small and Medium Enterprises shall be eligible for the special cases concerning certification of information security management systems under Article 47-7 (1) 2 of the Act:

1. A person whose sales from information and telecommunications services for the preceding year (if the person is a corporation, referring to the preceding business year) are less than 30 billion won;

2. A person that does not directly install and operate major information and communications facilities and uses any of the following services (limited to services provided by a person who has obtained certification under Article 47 (1) of the Act, certification under Article 32-2 (1) of the Personal Information Protection Act, or certification under Article 23-2 (1) of the Act on the Development of Cloud Computing and Protection of Its Users) from among persons whose sales from the information and communications service sector amount to at least 30 billion won in the preceding year (referring to the preceding business year in cases of a corporation):

(a) Hosting services (referring to services for building websites, maintaining web servers, etc.)

(b) Cloud computing services under subparagraphs 2 and 3 of Article 3 of the Enforcement Decree of the Act on the Development of Cloud Computing and Protection of Its Users;

(2) Notwithstanding paragraph (1), any of the following persons shall be excluded from those eligible for special cases concerning the certification of information security management systems under Article 47-7 (1) 2 of the Act:

1. A person falling within Article 47 (2) 1 or 2 of the Act;
2. A person falling within Article 49 (2) 1 or 3;
3. A virtual asset service provider defined in subparagraph 1 (n) of Article 2 of the Act on Reporting and Using Specified Financial Transaction Information;
4. A financial company defined in subparagraph 3 of Article 2 of the Electronic Financial Transactions Act.

[This Article Added on Jul. 23, 2024]

Article 50 [Moved to Article 47 <Aug. 17, 2012>]

Article 51 (Follow-up management of certification) (1) Follow-up management under Article 47 (8) of the Act shall be conducted by means of written examination or on-site examination. <Amended on May 31, 2016>

(2) Where an examination institution for information security management systems finds, as a result of conducting follow-up management pursuant to Article 47 (8) of the Act, that there is any of the grounds under the subparagraphs of paragraph (10) of that Article, it

shall immediately submit the results of the follow-up management so conducted to the Korea Internet and Security Agency or the certification body for information security management systems. <Added on May 31, 2016>

(3) The Korea Internet and Security Agency or the certification body for information security management systems shall, after deliberation by the certification committee under Article 47 (6), notify the results thereof to the Minister of Science and ICT in any of the following cases: <Amended on May 31, 2016; Jul. 26, 2017>

1. Where follow-up management conducted pursuant to Article 47 (8) of the Act finds any of the grounds under the subparagraph of paragraph (10) of that Article;
2. Where the Korea Internet and Security Agency or the certification body for information security management systems receives the results of follow-up management from the examination institution for information security management systems pursuant to paragraph (2).

[This Article Wholly Amended on Aug.17, 2012]

[Moved from Article 52; previous Article 51 is deleted <Aug. 17, 2012>]

Article 52 (Indication and publicity of certification) A person who obtains certification of his or her information security management system pursuant to Article 47 (1) or (2) of the Act may use the information security management system certification mark determined and publicly notified by the Minister of Science and ICT when he or she indicates or publicizes the content of certification in a document, invoice, advertisement, etc. in accordance with Article 47 (9) of the Act. In such cases, the scope and validity period of certification shall be indicated together with the mark. <Amended on Mar. 23, 2013; May 31, 2016; Jul. 26, 2017>

[This Article Wholly Amended on Aug.17, 2012]

[Moved from Article 53; previous Article 52 moved to Article 51 <Aug. 17, 2012>]

Article 53 (Standards for designation of certification bodies for information security management systems and examination institutions for information security management systems) (1) Standards for designating certification bodies for information security management systems and examination institutions for information security management systems shall be as follows: <Amended on Mar. 23, 2013; May 31, 2016; Jul. 26, 2017>

1. A certification body shall have at least 5 persons who meet the requirements for the qualification determined and publicly notified by the Minister of Science and ICT (hereinafter referred to as "certification examiners");
2. A certification body shall be approved as competent in an examination administered by the Minister of Science and ICT on the requirements and competence for the performance of the duties.

(2) The Minister of Science and ICT shall determine and publicly notify matters related to the education and qualification management of certification examiners and detailed standards for the examination on the requirements and competence for the performance of the duties under paragraph (1) 2. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Wholly Amended on Aug.17, 2012]

[Title Amended on May 31, 2016]

[Moved from Article 47; previous Article 53 moved to Article 52 <Aug. 17, 2012>]

Article 53-2 (Procedures for designation of certification bodies for information security management systems and examination institutions for information security management systems) (1) A person who intends to have his or her business designated as a certification body for information security management systems or an examination institution for information security management systems pursuant to Article 47 (6) or (7) of the Act shall file an application (including in electronic form) for the designation of a certification body for information security management systems or an examination institution for information security management systems with the Minister of Science and ICT, along with the following documents (or electronic documents): <Amended on Aug. 17, 2012; Mar. 23, 2013; May 31, 2016; Jul. 26, 2017>

1. Articles of incorporation, or bylaws of an association;
2. A statement of the current status of certification examiners employed and a document certifying the current status;
3. Documents determined and publicly notified by the Minister of Science and ICT as those necessary for the examination on the requirements and competence for the performance of duties, including work experience in performing duties for the protection of information and the level of expertise.

(2) Upon receipt of an application for the designation under paragraph (1), the Minister of Science and ICT shall verify the relevant corporate registration by sharing administrative information under Article 36 (1) of the Electronic Government Act, if the applicant is a corporation.<Amended on May 4, 2010; Nov. 2, 2010; Mar. 23, 2013; Jul. 26, 2017>

(3) Upon receipt of an application for designation under paragraph (1), the Minister of Science and ICT shall examine whether the application meets the standards for designation under Article 53 (1), notify the applicant of the result within 3 months from the date of receipt of the application, and issue a certificate of designation as a certification body for information security management systems or a certificate of designation as an examination institution for information security management systems to the applicant who is designated as a certification body for information security management systems or an examination institution for information security management systems. <Amended on Aug. 17, 2012; Mar. 23, 2013; May 31, 2016; Jul. 26, 2017>

(4) When the Minister of Science and ICT examines whether an application meets the standards for the designation under paragraph (3), he or she may require the applicant to submit data or may conduct an on-site inspection within the necessary extent. In such cases, a person who conducts the on-site inspection shall present identification verifying his or her qualification to the applicant. <Amended on Aug. 17, 2012; Mar. 23, 2013; Jul. 26, 2017>

(5) Deleted. <Jun. 25, 2012>

[Title Amended on May 31, 2016]

[Moved from Article 48 <Aug. 17, 2012>]

Article 53-3 (Validity period of designation of certification body for information security management systems and examination institution for information security management systems) (1) The validity period of the designation of a certification body for information security management systems or an examination institution for information security management systems under Article 53-2 shall be 3 years. <Amended on Aug. 17, 2012; May 31, 2016>

(2) A certification body may file an application for redesignation during the period from 6 months before the expiry of the validity period under paragraph (1) to the expiry date. In such cases, the designation shall be deemed to continue to be valid until the applicant for

redesignation is notified of a decision on the application.

(3) Articles 53 and 53-2, and paragraph (1) shall apply mutatis mutandis to the redesignation under paragraph (2). <Amended on Aug. 17, 2012>

[Title Amended on May 31, 2016]

[Moved from Article 49 <Aug. 17, 2012>]

Article 53-4 (Follow-up management of certification body for information security management systems and examination institution for information security management systems) (1) Each certification body for information security management systems and examination institution for information security management systems shall submit a report according to the following classification for the previous year to the Minister of Science and ICT by January 31 each year: <Amended on May 31, 2016; Jul. 26, 2017>

1. Certification body for information security management systems: Report on the certification performance records for the previous year;
2. Examination institution for information security management systems: Report on the certification examination performance records for the previous year.

(2) If the Minister of Science and ICT deems it necessary to ascertain whether a certification body for information security management systems or an examination institution for information security management systems falls under any subparagraph of Article 47-2 (1) of the Act, he or she may require the certification institution or the examination institution to submit data or may conduct an on-site inspection. <Amended on Mar. 23, 2013; May 31, 2016; Jul. 26, 2017>

[This Article Added on Aug. 17, 2012]

[Title Amended on May 31, 2016]

Article 54 (Guidelines for revocation of designation) Guidelines for administrative dispositions rendered for the revocation of designation or the suspension of business under Article 47-2 of the Act are as prescribed in Appendix 4.

Article 54-2 Deleted. <Dec. 9, 2022>

Article 54-3 (Entrustment of affairs regarding measures to prevent cyber security incidents and preclude spread thereof) (1) The head of a central administrative agency may entrust

affairs regarding measures to be taken under Article 47-4 (1) of the Act to the Korea Internet and Security Agency or an organization that specializes in protecting users' information, which the head of the central administrative agency determines in consultation with the Minister of Science and ICT. <Amended on Dec. 9, 2022>

(2) Where the head of the central administrative agency designates an entrusted agency pursuant to paragraph (1), he or she shall publicly notify the entrusted agency and the details of the affairs to be entrusted.

[This Article Added on Dec. 8, 2020]

Article 55 (Terms and conditions for requests to users for protective measures) Matters that shall be stipulated in the terms and conditions of use with respect to a request to users for protective measures under Article 47-4 (3) of the Act shall be as follows: <Amended on Aug. 17, 2012; Dec. 8, 2020>

1. Grounds for requesting users to take protective measures and a method of making such request;
2. Details of protective measures that users shall take;
3. The period during which access to an information and communications network is restricted, if a user fails to take protective measures;
4. Procedures for filing a user's objection and for compensation therefor, if a user' access is unreasonably restricted on the grounds of the user's failure to take protective measures.

Article 55-2 (Criteria for examination for assignment of information security management grade) (1) The criteria for examination for the assignment of an information security management grade under Article 47-5 (1) of the Act shall be as follows:

1. The scope and period of operation of the information security management system;
2. An organization exclusively dedicated to information security and the budget therefor;
3. Information security management activities and security measure level.

(2) Matters necessary for the detailed evaluation criteria, evaluation methods, etc. for each examination criterion listed under paragraph (1) shall be determined and publicly notified by the Minister of Science and ICT. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Added on Aug. 17, 2012]

Article 55-3 (Methods and procedures for assignment of information security management grade) (1) A person who intends to obtain an information security management grade under Article 47-5 (1) of the Act shall file an application (including in electronic form) for an information security management grade with the Korea Internet and Security Agency, along with a copy of the certificate of information security management system.

(2) The examination for assignment of an information security management grade shall be conducted by means of reviewing documents or through an on-site examination.

(3) The examination under paragraph (2) may be conducted only by certification examiners.

(4) If the results of an examination administered under paragraph (2) meet the criteria for examination under Article 55-2, the Korea Internet and Security Agency shall issue a certificate of information security management grade to the applicant for the grade qualified for management.

(5) Except as provided in paragraphs (1) through (4), detail matters necessary for applying for and examining the assignment of an information security management grade, issuing a certificate of information security management grade, and performing relevant affairs shall be determined and publicly notified by the Minister of Science and ICT. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Added on Aug. 17, 2012]

Article 55-4 (Fees for information security management grades) Articles 48 and 52 shall apply mutatis mutandis to fees for information security management grades and indication and publicity thereof.

[This Article Added on Aug. 17, 2012]

Article 55-5 (Validity period of information security management grades) The validity period of an information security management grade under Article 55-3 shall be one year.

[This Article Added on Aug. 17, 2012]

Article 55-6 (Awards to disclosers of information security vulnerabilities) (1) Persons entitled to monetary awards and the criteria and procedures for the payment thereof under Article 47-6 (1) of the Act shall be as specified in Appendix 4-2.

(2) Where the Minister of Science and ICT entrusts duties related to the payment of monetary awards to the Korea Internet and Security Agency pursuant to Article 47-6 (3) of

the Act, he or she shall publicly notify the details of the entrusted duties.
[This Article Added on Dec. 9, 2022]

Article 56 (Countermeasures against cyber security incidents) "Other countermeasures against cyber security incidents prescribed by Presidential Decree" in Article 48-2 (1) 4 of the Act means the following measures: <Amended on Jan. 28, 2009; Dec. 8, 2020>

1. Requesting a major provider of information and communications services or a business operator who operates and manages integrated information and telecommunications facilities for the provision of information and communications services of other persons under Article 46 (1) of the Act to cut off access channels (limited to access channels that have been used, or are likely to be used, for spreading cyber security incidents);
2. Requesting a software business operator, defined under subparagraph 4 of Article 2 of the Software Promotion Act, who produced or distributed the software involved in a cyber security incident, to produce and distribute a program by which the vulnerability in security of the software is cured and corrected (hereinafter referred to as "program for curing the vulnerability in security") and requesting the provider of information and communications services to release the program for curing the vulnerability in security through information and communications networks;
3. Spreading forecasts and warnings of cyber security incidents under Article 48-2 (1) 2 of the Act to mass media and providers of information and communications services;
4. Providing information about cyber security incidents to the heads of related agencies, if necessary for the security of national information and communications networks.

Article 57 (Persons providing information about cyber security incidents) "Persons prescribed by Presidential Decree from among those who operate an information and communications network" in Article 48-2 (2) 3 of the Act means any of the following persons among those who operate an information and communications network: <Amended on Mar. 28, 2008; Jan. 28, 2009; Oct. 1, 2010; Aug. 29, 2011; Mar. 23, 2013; Jul. 26, 2017>

1. An institution subject to a protection plan and protection guidelines on critical information and communications infrastructure, formulated and established by the Minister of Science and ICT pursuant to Articles 6 and 10 of the Act on the Protection of

Information and Communications Infrastructure;

2. A person who periodically observes the current status of operation of information and communications networks by providers of information and communications services and provides information on cyber security incidents;
3. A person specified and publicly notified by the Minister of Science and ICT among private business operators who operate information and communications networks independently with Internet protocol addresses allocated by the Korea Internet and Security Agency under subparagraph 1 (a) of Article 2 of the Internet Address Resources Act;
4. A producer of antivirus software against computer viruses among persons who engage in the information protection industry.

Article 58 (Provision of information on cyber security incidents) A person who provides information on cyber security incidents under Article 48-2 (2) of the Act shall comply with the following subparagraphs in providing information on cyber security incidents: <Amended on Mar. 23, 2013; Jul. 26, 2017>

1. A method which a person applies to providing such information shall conform to a method determined by the Minister of Science and ICT, taking into consideration characteristics of information and communications networks, trends in cyber security incidents, etc.;
2. The person shall take measures to prevent the destruction, obliteration, and alteration of information on cyber security incidents;
3. The person shall adopt encryption techniques determined by the Minister of Science and ICT;
4. The person shall comply with other methods and procedures determined and publicly notified by the Minister of Science and ICT.

Article 58-2 (Time, methods, and procedures for reporting of cyber security incidents) (1) Where a provider of information and communications services intends to report a cyber security incident pursuant to the former part of Article 48-3 (1) of the Act, he or she shall report the following matters to the Minister of Science and ICT or the Korea Internet and Security Agency within 24 hours from the time he or she becomes aware of the occurrence

of the cyber security incident:

1. The date, time, cause, and details of damage caused by the cyber security incident;
2. Current status of responses, such as measures to be taken against the cyber security incident;
3. The department and contact information in charge of responding to the cyber security incident.

(2) The provider of information and communications service shall, if there is any additionally verified fact regarding the cyber security incident after filing a report pursuant to paragraph (1), report it within 24 hours from the time it is verified.

(3) A report under paragraphs (1) and (2) may be made in writing, by e-mail, by telephone, by inputting it into the website of the Ministry or the Agency, or through other means.

[This Article Added on Aug. 13, 2024]

Article 58-3 (Procedures for inspection of implementation of measures on cyber security incidents) Where the Minister of Science and ICT intends to inspect the implementation of measures under Article 48-4 (2) of the Act in accordance with Article 48-4 (3) of the Act, he or she shall notify the relevant provider of information and communications services of an inspection plan including the purpose, date and time, method, details, etc. of the inspection by no later than 7 days prior to the inspection; provided, he or she need not notify the provider of information and communications services in advance if it is deemed urgent, such as the expected occurrence of additional cyber security incidents or if it is deemed impractical to achieve the purpose of inspection due to destruction of evidence, etc. by prior notification.

[This Article Added on Aug. 13, 2024]

Article 59 (Organization and operation of private-public joint investigation team) (1) A private-public joint investigation team referred to in Article 48-4 (4) of the Act (hereinafter referred to as the "Investigation Team") shall be comprised of approximately 20 investigation members, including the head and the deputy head, and the number of such members may be adjusted based on the scale and type of a cyber security incident. <Amended on Aug. 13, 2024>

(2) Members of the Investigation Team shall be appointed or commissioned by the Minister of Science and ICT from among the following persons; and the head shall be designated by the Minister of Science and ICT from among public officials of at least Grade IV specified in subparagraph 1 and the deputy head shall be nominated by the Minister of Science and ICT from among persons specified in subparagraph 3:

1. Public officials of the Ministry of Science and ICT in charge of investigation of cyber security incidents;
2. Persons who have expertise and experience in relation to cyber security incidents;
3. Executive officers and employees of the Korea Internet and Security Agency;
4. Other persons deemed necessary for analyzing the causes of cyber security incidents.

(3) The Investigation Team shall be comprised of an investigation task force that analyzes the causes of cyber security incidents and a verification task force that verifies the analysis results; provided, the head of the Investigation Team may operate a task force by integrating such investigation and verification task forces or organize another task force if it is deemed necessary.

(4) The head of the Investigation Team may seek advice from relevant experts or companies specializing in information security, if necessary for analyzing the causes of a cyber security incident.

(5) Allowances, travel expenses, and other necessary expenses may be paid within the budget to the members of the Investigation Team who are not public officials and relevant experts, etc. referred to in paragraph (4).

(6) Upon completing the analysis of the causes of a cyber security incident, the head of the Investigation Team shall prepare a report on the results thereof without delay and report it to the Minister of Science and ICT.

(7) Where the purpose of organizing the Investigation Team is deemed accomplished, the Minister of Science and ICT may dissolve the Investigation Team.

(8) Except as provided in paragraphs (1) through (7), matters necessary for the composition and operation of the Investigation Team shall be determined by the Minister of Science and ICT.

[This Article Wholly Amended on Dec. 9, 2022]

Article 60 (Protection of data related to cyber security incidents and methods and procedures for investigation) (1) The Minister of Science and ICT and the Investigation Team shall keep the data submitted or information learned through investigation under Article 48-4 (6) of the Act in a safe manner to prevent such data or information from being stolen, divulged, damaged, or altered. <Amended on Aug. 13, 2024>

(2) When a public official under the Minister's jurisdiction or a member of the Investigation Team enters the place of business of a relevant person pursuant to the main clause of Article 48-4 (6) of the Act, he or she shall present identification in the form specified in Appendix 5 verifying his or her authority to the relevant person. <Amended on Aug. 13, 2024>

[This Article Wholly Amended on Dec. 9, 2022]

Article 60-2 (Specialized organizations for responding to cyber security incidents related to devices and the like connected to information and communications networks) "Specialized organizations prescribed by Presidential Decree" in the provisions, with the exception of the subparagraphs, of Article 48-5 (4) of the Act means the following institutions:

1. The Korea Internet and Security Agency;
2. An institution determined through consultation between the Minister of Science and ICT and the heads of relevant central administrative agencies, which has expertise in dealing with cyber security incidents related to devices and the like connected to information and communications networks.

[This Article Added on Dec. 8, 2020]

Article 60-3 (Procedures for information security certification) (1) A person who intends to obtain information security certification under Article 48-6 (1) of the Act (hereinafter referred to as "information security certification") shall submit an application for information security certification prescribed by Decree of the Ministry of Science and ICT to the Minister of Science and ICT along with the following documents and shall produce devices and the like connected to information and communications networks, subject to information security certification:

1. Documents proving that the certification standards under Article 48-6 (2) of the Act (hereinafter referred to as "information security certification standard") have been

satisfied;

2. A user manual of devices and the like connected to information and communications networks subject to information security certification;
3. Other documents prescribed by Decree of the Ministry of Science and ICT as necessary for information security certification.

(2) Upon receipt of an application for information security certification pursuant to paragraph (1), the Minister of Science and ICT shall request a testing agency for certification designated pursuant to Article 48-6 (4) of the Act (hereinafter referred to as "testing agency for certification") to conduct a test to confirm compliance with the certification standards under paragraph (2) of that Article (hereinafter referred to as "information security certification test").

(3) Where necessary for conducting an information security certification test, a testing agency for certification may conduct a test on the site where the relevant devices and the like connected to information and communications networks are installed.

(4) A testing agency for certification shall submit a report on the results of information security certification tests to the Minister of Science and ICT.

(5) The Minister of Science and ICT shall examine a report on the results of information security certification tests submitted pursuant to paragraph (4); and where the devices and the like connected to information and communications networks meet the information security certification standards, he or she shall issue an information security certification prescribed by Decree of the Ministry of Science and ICT to a person who applies for information security certification pursuant to paragraph (1), and shall publicly announce such fact on the Ministry's website.

(6) The Minister of Science and ICT who has revoked information security certification pursuant to Article 48-6 (3) of the Act shall notify the relevant person of such fact and publicly announce it on the Ministry's website.

[This Article Added on Dec. 8, 2020]

Article 60-4 (Validity period of information security certification) (1) The validity period of information security certification shall be 3 years and may be extended only once by up to 2 years.

(2) A person who intends to extend the validity period of information security certification pursuant to paragraph (1) shall file an application for an extension of the validity period of information security certification with the Minister of Science and ICT by no later than 6 months before the expiration of the validity period, as prescribed by Decree of the Ministry of Science and ICT.

(3) Upon receipt of an application for extension of the validity period under paragraph (2), the Minister of Science and ICT may extend the validity period only where the sameness of the characteristics and configuration is recognized for the devices and the like connected to the information and communications network for which the information security certification has been granted.

(4) The Minister of Science and ICT who extends the validity period under paragraph (3) shall issue information security certification reflecting the extended validity period as prescribed by Decree of the Ministry of Science and ICT to the applicant for extension of the validity period and shall publicly announce such fact on the Ministry's website.

[This Article Added on Dec. 8, 2020]

Article 60-5 (Fees for information security certification) (1) A person who intends to apply for information security certification shall pay a fee.

(2) The criteria for calculating fees under paragraph (1) shall be determined and publicly notified by the Minister of Science and ICT.

[This Article Added on Dec. 8, 2020]

Article 60-6 (Follow-Up management of information security certification) (1) Where devices and the like connected to information and communications networks for which information security certification has been granted fail to meet the standards for information security certification due to discovery of vulnerabilities, the Minister of Science and ICT may request a person who has obtained the relevant information security certification to fix such vulnerabilities for a specified period.

(2) Details necessary for a request to fix vulnerabilities under paragraph (1) shall be determined and publicly notified by the Minister of Science and ICT.

[This Article Added on Dec. 8, 2020]

Article 60-7 (Standards for designation of testing agencies for certification) (1) "Institution satisfying the designation standards prescribed by Presidential Decree" in Article 48-6 (4) of the Act means an institution meeting all of the following standards:

1. It shall be a corporation engaged in the affairs related to information security certification tests;
2. It shall have human resources (including two full-time workers) with technical capabilities, who are in charge of the affairs related to information security certification tests, and an organization dedicated to such affairs;
3. It shall have a test environment, such as facilities and laboratory spaces, to perform the affairs related to information security certification tests;
4. It shall have the operational ability to perform the affairs related to information security certification tests.

(2) A person seeking to be designated as a testing agency for certification shall file an application for designation as a testing agency for certification with the Minister of Science and ICT, along with documents proving that he or she meets the designation standards provided in paragraph (1).

(3) Upon receipt of an application under paragraph (2), the Minister of Science and ICT may designate a testing agency for certification after examining whether it satisfies the designation standards under paragraph (1).

(4) The Minister of Science and ICT who designates a testing agency for certification pursuant to paragraph (3) shall issue a certificate of designation in the form prescribed by Decree of the Ministry of Science and ICT to the applicant and shall publicly announce such fact in the Official Gazette and on the Ministry's website.

(5) The validity period of the designation under paragraph (3) shall be determined by the Minister of Science and ICT for up to 3 years; and where it is intended to continue to conduct the affairs of a testing agency for certification after the validity period expires, an application for redesignation shall be filed from 6 months before the expiry of the validity period until the expiration date of the validity period.

(6) The designation shall be deemed valid until the applicant is notified of the results of the examination of the application for redesignation under paragraph (5).

(7) Detailed matters related to the designation standards and procedures for testing agencies for certification, redesignation, etc. under paragraphs (1) through (6) shall be determined and publicly notified by the Minister of Science and ICT.
[This Article Added on Dec. 8, 2020]

Article 60-8 (Follow-up management of testing agencies for certification and revocation of designation of such agencies) (1) A testing agency for certification shall submit the results of certification tests for the previous year to the Minister of Science and ICT by January 31 of each year in a report in the form prescribed by Decree of the Ministry of Science and ICT.
(2) The Minister of Science and ICT may request a testing agency for certification to submit data or visit the site to verify whether it meets the designation standards under Article 48-6 (4) of the Act or whether it gives rise to the grounds for revocation of designation under the subparagraphs of paragraph (5) of that Article.
(3) Upon revoking a designation as a testing agency for certification under Article 48-6 (5) of the Act, the Minister of Science and ICT shall notify the relevant institution of the revocation and publicly announce such revocation in the Official Gazette and on the Ministry's website.
[This Article Added on Dec. 8, 2020]

Article 60-9 (Entrustment of information security certification affairs) Pursuant to Article 48-6 (6) of the Act, the Minister of Science and ICT shall entrust the following affairs to the Korea Internet and Security Agency:

1. Receiving applications for information security certification, requesting the implementation of information security certification tests, receiving reports on the results of information security certification tests, issuing information security certificates, and publicly announcing information security certification and revocation thereof, under Articles 60-3 (1), (2), and (4) through (6);
2. Receiving applications for extension of the validity period of information security certification, issuing an information security certificate, and publicly announcing information security certification pursuant to Article 60-4 (2) and (4);

3. Reviewing the fix of vulnerabilities of information security certification and supporting the delivery of requests to fix vulnerabilities under Article 60-6.

[This Article Added on Dec. 8, 2020]

Article 60-10 (Terms and conditions on measures for prevention of damage) Matters that shall be stipulated in the terms and conditions of use under Article 49-2 (5) of the Act with respect to measures to prevent damage and the spread thereof shall be as follows:

1. The grounds for and details of the measures prescribed in the items of Article 49-2 (3) 3 of the Act;
2. The period of taking the measure to discontinue the provision of services pursuant to Article 49-2 (3) 3 (b) of the Act;
3. The procedures for filing a user's objection to any of the measures taken under the items of Article 49-2 (3) 3 of the Act;
4. Where any of the measures prescribed in the items of Article 49-2 (3) 3 of the Act is taken, the methods and procedures for notifying users of the grounds for and details of such relevant measure, the procedure for filing an objection, and other relevant matters.

[This Article Added on Dec. 9, 2022]

Article 60-11 (Discontinuance of telecommunications services for phone numbers used as means of deception) (1) "Person prescribed by Presidential Decree, including the Commissioner General of the Korean National Police Agency, the Prosecutor General, and the Governor of the Financial Supervisory Service" in Article 49-3 (1) of the Act means the Commissioner General of the Korean National Police Agency, the Prosecutor General, and the Governor of the Financial Supervisory Service.

(2) Where a user intends to file an objection pursuant to Article 49-3 (2) of the Act, the user shall submit a written statement of the following matters to the authority that requested the discontinuance of the relevant telecommunications service pursuant to paragraph (1) of that Article (hereafter in this Article referred to as "authority that requested the discontinuance of the service") within 30 days from the date the telecommunications service was discontinued:

1. The name or business name, address, and contact information of the petitioner;

2. The grounds for the objection;

3. The date the telecommunications service was discontinued.

(3) Upon receipt of an objection filed under paragraph (2), the authority that requested the discontinuance of the service shall make a decision on the objection within 15 days from the date of receipt and shall notify the results of the decision, in writing, to the petitioner; provided, if it is impracticable to make a decision within the period due to an unavoidable reason, the authority may extend the period by up to 15 days and shall notify the petitioner of the reason for the extension and the extended period.

(4) If there is any deficiency in a written statement submitted under paragraph (2) or further facts need to be verified, the authority that requested the discontinuance of the service may request that such statement or facts be supplemented. In such cases, the period taken for supplementation shall not be included in the period specified in paragraph (3).

(5) Where the authority that requested the discontinuance of the service deems that an objection filed under Article 49-3 (2) of the Act is reasonable, it shall request the Minister of Science and ICT to terminate the discontinuance of the relevant telecommunications service without delay.

[This Article Added on Dec. 9, 2022]

Article 61 (Guidelines for transmission of advertising information for profit) (1) "Period prescribed by Presidential Decree" in Article 50 (1) 1 of the Act means 6 months from the date the trade of the relevant goods, etc. is concluded. <Amended on Nov. 28, 2014>

(2) "Media prescribed by Presidential Decree" in the proviso of Article 50 (3) of the Act means electronic mail.<Added on Nov. 28, 2014>

(3) Matters that a person who transmits advertising information for profit, using an electronic transmission medium pursuant to Article 50 (4) of the Act shall clearly state in the relevant information, and methods therefor shall be as specified in Appendix 6. <Amended on Nov. 28, 2014>

Article 62 (Provision of free telephone services for refusal of reception or withdrawal of consent to reception) A person who transmits advertising information for profit, using an electronic transmission medium shall clearly state information about free telephone

services, etc. for the refusal of reception or for the withdrawal of consent to reception, as prescribed in Appendix 6, and shall provide such services to addressees in accordance with Article 50 (6) of the Act. <Amended on Mar. 29, 2011; Nov. 28, 2014>

Article 62-2 (Notification of results of handling of consent to receive messages) A person who intends to transmit advertising information for profit, using an electronic transmission medium pursuant to Article 50 (7) of the Act shall notify an addressee of the following matters within 14 days from the date the relevant addressee expresses his or her consent to receipt of messages, refusal to receive messages or withdrawal of his or her consent to receive messages:

1. The name of a sender;
2. The fact that the addressee has consented to receive messages, refused to receive messages, or withdrawn his or her consent to receive messages, and the date he or she expresses the relevant intent;
3. The results of the handling thereof.

[This Article Added on Nov. 28, 2014]

Article 62-3 (Verification of addressees' consents to receive messages) (1) A person who has obtained prior consent from an addressee pursuant to Article 50 (1) or (3) of the Act shall verify whether the relevant addressee gives consent to receive messages every two years from the date he or she obtains consent to receive messages from the addressee (referring to the day before every second year from the date he or she obtains consent to receive messages) pursuant to paragraph (8) of the aforesaid Article.

(2) A person who intends to verify whether an addressee gives his or her consent to receive messages pursuant to paragraph (1) shall advise the addressee of the following matters:

1. The name of a sender;
2. The fact that the addressee gives consent to receive messages, and the date he or she gives consent to receive messages;
3. The methods for expressing his or her intent to maintain or withdraw his or her consent to receive messages.

[This Article Added on Nov. 28, 2014]

Article 63 (Devices for restricting installation of advertising programs for profits) "Information processing device prescribed by Presidential Decree" in the former part of Article 50-5 of the Act means an information processing device with which information can be transmitted and received by connecting it to an information and communications network, such as mobile Internet and mobile telephones. <Amended on Aug. 29, 2011>

Article 64 (Subsidization for development of software designed to cut off transmission of advertising information for profits) (1) Pursuant to Article 50-6 of the Act, the Korea Communications Commission may fully or partially subsidize a project of a public institution, corporation, or organization that develops and distributes a piece of software or a computer program for conveniently blocking or reporting advertising information transmitted for profits in violation of Article 50 of the Act (hereinafter referred to as "software for blocking or reporting advertisements"), within the budget.

(2) The Korea Communications Commission may recommend providers of information and communications services and users to use the software for blocking or reporting advertisements developed in accordance with paragraph (1). <Amended on Jan. 28, 2009; Aug. 4, 2020>

Article 65 (Operation of the Korea Internet and Security Agency) (1) The Minister of Science and ICT, the Minister of the Interior and Safety, the Korea Communications Commission, or the Personal Information Protection Commission may request the head of a related agency to dispatch public officials related to the affairs of the Korea Internet and Security Agency under the subparagraphs of Article 52 (3) of the Act. <Amended on Oct. 1, 2010; Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017; Aug. 4, 2020>

(2) When the head of a related agency who dispatched a public official under paragraph (1) needs to have the public official returned during the period of dispatch service, he or she shall consult with the head of the agency that requested for such dispatch.

(3) The head of the Korea Internet and Security Agency may authorize a research institute related to information and communications to conduct part of the business affairs specified in Article 52 (3) 4 of the Act, with approval therefor from the Minister of Science and ICT, the Minister of the Interior and Safety or the Korea Communications Commission.

<Amended on Oct. 1, 2010; Mar. 23, 2013; Nov. 28, 2014; Jul. 26, 2017>

(4) If a business affair that the head of the Korea Internet and Security Agency conducts in accordance with Article 52 (3) of the Act is related to the protection of a public institution's information, he or she shall obtain approval therefor from the head of the related institution. <Amended on Oct. 1, 2010>

(5) The Korea Internet and Security Agency shall perform the following affairs in order to promote programs for transmitting advertising information under Article 52 (3) 10 and 22 of the Act. <Add on Aug. 4, 2020; Jul. 23, 2024>

1. Settlement of grievances relating to the transmission of advertising information and counseling thereon;
2. Provision of technical advice under Article 64 (10) of the Act related to the transmission of advertising information and other necessary assistance;
3. Research on measures to prevent illegal transmission of advertising information;
4. Education and publicity for the prevention of illegal transmission of advertising information;
5. Affairs related to the duties under subparagraphs 1 through 4.

(6) If deemed necessary for requiring providers of information and communications services to submit relevant articles, documents, etc. or for efficiently conducting inspections under Article 64 (1) or (3) of the Act related to the transmission of advertising information, the Korea Communications Commission may dispatch its public officials to the Korea Internet and Security Agency pursuant to Article 32-4 of the State Public Officials Act. <Added on Aug. 4, 2020>

[Title Amended on Oct. 1, 2010]

Article 66 Deleted. <Aug. 4, 2020>

CHAPTER VI-2 TELECOMMUNICATIONS BILLING SERVICES

Article 66-2 (Requirements for registration) (1) A person who intends to be registered as a provider of telecommunications billing services under Article 53 of the Act shall meet all the following requirements: <Amended on Mar. 23, 2013; Jul. 26, 2017; Dec. 28, 2021; Dec. 31, 2024>

1. The ratio of the total liabilities to the equity capital, total contributions, or endowment shall not exceed a ratio determined and publicly notified by the Minister of Science and ICT, which shall not exceed 200/100. If the majority stockholder is a company that belongs to a conglomerate, defined under subparagraph 11 of Article 2 of the Monopoly Regulation and Fair Trade Act, (excluding conglomerates defined under Article 38 (1) 1 and 2 of the Enforcement Decree of the aforesaid Act) in such cases, the calculation of such ratio shall be based on the conglomerate, but companies that engage in financial business or insurance business, from among companies that belong to the conglomerate, shall be excluded from the calculation;
2. The person shall be fully equipped with the following human resources and physical facilities with which the person can conduct the business:
   (a) At least 5 executive officers and employees who have work experience of at least two years in operating electronic computer systems;
   (b) Electronic computer systems and various computer programs necessary for smoothly providing telecommunications billing services;
   (c) An information protection system under Article 57 (2) of the Act;
3. The paid-in capital, total contributions, or endowment shall be at least an amount specified in paragraph (2).

(2) "Amount prescribed by Presidential Decree" in Article 53 (2) of the Act means 1 billion won.

[This Article Added on Mar. 28, 2008]

Article 66-3 (Procedures for registration) (1) A person who intends to register as a provider of telecommunications billing services pursuant to Article 53 of the Act shall submit an application for registration in the form prescribed and publicly notified by the Minister of Science and ICT to the Minister of Science and ICT. <Amended on Feb. 27, 2024>

(2) An application for registration under paragraph (1) shall be accompanied by the following documents: <Amended on Feb. 27, 2024>

1. Articles of incorporation;
2. Documents proving that the applicant meets the requirements for registration under Article 66-2;

3. A business plan for three years after the commencement of business (including estimated financial statements and a statement of estimated revenues and expenditures);
4. A plan for the protection of users of telecommunications billing services (including matters under Articles 66-7 through 66-9).
5. A document proving that the applicant does not fall under any of the disqualifications under Article 54 of the Act.

(3) Upon receipt of an application for registration under paragraph (1), the Minister of Science and ICT shall verify the relevant corporate registration by sharing administrative information under Article 36 (1) of the Electronic Government Act.<Amended on May 4, 2010; Nov. 2, 2010; Mar. 23, 2013; Jul. 26, 2017>

(4) The Minister of Science and ICT may request the applicant to supplement the documents submitted pursuant to paragraphs (1) and (2) if there is a defect in the documents submitted, and may extend the supplementation period if the applicant requests it within 10 days from the date of submission. <Amended on Mar. 23, 2013; Jul. 26, 2017; Feb. 27, 2024>

(5) Upon receipt of an application for registration pursuant to paragraph (1), the Minister of Science and ICT shall register the applicant as a provider of communication billing services if the applicant meets the requirements for registration under Article 66-2 and issue a certificate of registration as a provider of communication billing services in the form prescribed and publicly notified by the Minister of Science and ICT to the applicant. <Added on Feb. 27, 2024>

(6) Where the Minister of Science and ICT registers a provider of telecommunications billing services, he or she shall publish the details of the registration in the Official Gazette and shall inform the general public thereof through the Internet, etc. <Amended on Mar. 23, 2013; Jul. 26, 2017; Feb. 27, 2024>

[This Article Added on Mar. 28, 2008]

Article 66-4 (Grounds for disqualification from registration) "Investor prescribed by Presidential Decree" in subparagraph 1 of Article 54 of the Act means any of the following persons: <Amended on Jul. 29, 2008; Sep. 5, 2017>

1. The principal who holds the largest number of outstanding voting stocks of, or shares in contributions to, the relevant corporation (hereafter referred to as "stocks or the like" in

this Article), when the stocks held by the principal and those held by persons related to the principal, as defined under any subparagraph of Article 3 (1) of the Enforcement Decree of the Act on Corporate Governance of Financial Companies, on their own accounts respectively in whosever name are aggregated;

2. A person who holds at least 10/100 of stocks or the like of the relevant corporation on his or her account in whosever name or a stockholder who exercises the de facto control over important matters relating to the management of the corporation through appointment and dismissal of executive officers or by other means, who is a related person defined under any subparagraph of Article 3 (1) of the Enforcement Decree of the Act on Corporate Governance of Financial Companies.

[This Article Added on Mar. 28, 2008]

Article 66-5 (Administrative dispositions) (1) Deleted. <Dec. 22, 2015>

(2) When the Minister of Science and ICT intends to revoke the registration of a provider of telecommunications billing services under Article 55 of the Act, he or she shall hold a hearing. <Amended on Mar. 23, 2013; Jul. 26, 2017>

(3) When the Minister of Science and ICT revokes the registration of a provider of telecommunications billing services under Article 55 of the Act, he or she shall publish the details thereof in the Official Gazette and shall notify the general public thereof through the Internet or by other means. <Amended on Mar. 23, 2013; Jul. 26, 2017>

[This Article Added on Mar. 28, 2008]

Article 66-6 (Measures necessary for securing stability and reliability of telecommunications billing services) Administrative and technical measures that a provider of telecommunications billing services shall take in accordance with Article 57 (2) of the Act in order to secure the stability and reliability of transactions through telecommunications billing services are as shown in Appendix 7.

[This Article Added on Mar. 28, 2008]

Article 66-7 (Retention period of transaction records and methods of changing terms and conditions) (1) Pursuant to Article 58 (4) and (7) of the Act, a provider of telecommunications billing services shall preserve records of the following matters for 1 year from the date on which each transaction is conducted; provided, the records of a

transaction, the amount of which exceeds 10,000 won, shall be preserved for 5 years: <Amended on Aug. 29, 2011; Mar. 23, 2013; Nov. 28, 2014; Jul. 26, 2017; Dec. 11, 2018>

1. The type of a transaction conducted through telecommunications billing services;
2. The amount of a transaction;
3. The other party to a transaction of purchase or use through telecommunications billing services (referring to a person who sells goods or provides services in return for a price therefor through telecommunications billing services; hereinafter referred to as the "other party to a transaction");
4. The date and time of a transaction;
5. The subscriber number of telecommunications services for which charges are billed and collected;
6. Matters regarding access to telecommunications services in connection with the relevant transaction;
7. Matters regarding an application for a transaction and amendment to terms and conditions;
8. Matters regarding approval for a transaction;
9. Other matters determined and publicly notified by the Minister of Science and ICT.

(2) Transaction records under paragraph (1) shall be preserved in paper, microfilms, discs, magnetic tapes, or other electronic information processing systems; provided, where such records are preserved in discs, magnetic tapes, or other electronic information processing systems, the requirements under Article 5 (1) of the Framework Act on Electronic Documents and Transactions shall be fully met. <Amended on Aug. 31, 2012>

(3) When a provider of telecommunications billing services (limited to those who provide the services described in Article (2) (1) 10 (a)) changes terms and conditions pursuant to Article 58 (6) of the Act, he or she shall notify users of telecommunications billing services by any means of e-mail, writing, facsimile, telephone or other means similar thereto.<Added on Nov. 28, 2014; Jan. 5, 2021>

(4) A user of telecommunications billing services may raise an objection to the changed terms and conditions from the date he or she receives notification under paragraph (3) until the business day before the effective date of the changed terms and conditions. <Added on Nov. 28, 2014>

[This Article Added on Mar. 28, 2008]

[Title Amended on Nov. 28, 2014]

[Moved from Article 66-8 <Dec. 11, 2018>]

Article 66-8 (Content of and procedures for requesting information on purchasers) (1) Where a user of telecommunications billing services requests the other party to a transaction pursuant to the former part of Article 58-2 (1) of the Act for information about the name and date of birth of a person who purchased or used goods or service (hereinafter referred to as "purchaser information"), he or she shall submit a written request (including an electronic document) for purchaser information, stating the following information:

1. Personal data of the user of telecommunications billing services: Name, date of birth, and contact information (referring to a telephone number, electronic mail address, etc.);
2. Requested details of payment: The telephone number used for payment and the date, time, and amount of payment;
3. The statement that purchaser information needs to be written separately for each type of goods or services.

(2) Where any institution or organization authorized to mediate in and resolve disputes under Article 59 (2) of the Act requests for purchaser information on behalf of a user of telecommunications billing services, it shall submit a document (including an electronic document) confirming that the user of telecommunications billing services has given consent to requesting purchaser information on behalf of the user, along with the written request under paragraph (1).

[This Article Added on Dec. 11, 2018]

[Previous Article 66-8 moved to Article 66-7 <Dec. 11, 2018>]

Article 66-9 (Procedures for filing objections and redressing violations of rights) (1) A provider of telecommunications billing services shall designate a manager and an officer in charge of the protection of users of telecommunications billing services for filing objections and redressing violations of rights under Article 59 (3) of the Act and shall notify the contact information of such manager and officer (referring to telephone numbers, facsimile numbers, e-mail addresses, etc.) to users of telecommunications billing services through the Internet and by other means. <Amended on Dec. 11, 2018; Jan. 5,

2021>

(2) A user of telecommunications billing services may file an objection with regard to telecommunications billing services to the relevant provider of telecommunications billing services in writing (or by an electronic document), telephone, facsimile, or other similar means. <Amended on Jan. 5, 2021>

(3) Upon receipt of an objection under paragraph (2), the provider of telecommunications billing services shall notify the user of the results of the relevant investigation or decision within 2 weeks from the date when such objection is filed.

[This Article Added on Mar. 28, 2008]

CHAPTER VI-3 INTERNATIONAL COOPERATION

Article 67 Deleted. <Aug. 4, 2020>

CHAPTER VII SUPPLEMENTARY PROVISIONS

Article 68 (Submission of data) "Ground prescribed by Presidential Decree to believe that it is necessary for the protection of users" in Article 64 (1) 3 of the Act means either of the following cases: <Amended on Mar. 28, 2008; Aug. 29, 2011>

1. Where it is necessary to prepare policy measures for the protection of youths under Article 41 (1) of the Act;
2. Where it is necessary to ascertain whether a person responsible for the protection of youths under Article 42-3 (3) of the Act performs the duty of protecting youths;
3. Deleted. <Aug. 17, 2012>

Article 68-2 (Methods for publication of order of corrective measures) (1) When the Minister of Science and ICT or the Korea Communications Commission orders a provider of information and communications services under Article 64 (4) of the Act to make a public publication of the fact that the service provider is ordered to take corrective measures, the Minister of Science and ICT or the Korea Communications Commission shall prescribe the details, number of times, and media of publication, the size of pages, etc. in issuing such order, taking the following factors into consideration: <Amended on Sep. 29, 2011; Mar.

23, 2013; Jul. 26, 2017; Aug. 4, 2020>

1. Details and severity of relevant violations;

2. The duration and number of times of relevant violations.

(2) When the Minister of Science and ICT or the Korea Communications Commission orders a provider of information and communications services under paragraph (1) to make a publication of the fact that the service provider is ordered to take corrective measures, the Minister of Science and ICT or the Korea Communications Commission may consult on the text of the publication with the provider of information and communications services. <Amended on Sep. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Aug. 4, 2020>

[This Article Added on Jan. 28, 2009]

Article 69 (Disclosure of order to take corrective measures) (1) In either of the following cases, the fact that a provider of information and communications services is ordered to take corrective measures under Article 64 of the Act may be disclosed. In such cases, the Minister of Science and ICT or the Korea Communications Commission shall notify the relevant provider of information and communications services of the disclosure in advance: <Amended on Mar. 28, 2008; Jan. 28, 2009; Sep. 29, 2011; Mar. 23, 2013; Jul. 26, 2017; Aug. 4, 2020>

1. Where a provider of information and communications services is ordered to take corrective measures for an act specified in any provision of Articles 71 through 74 of the Act;

2. Where a provider of information and communications services has been ordered to take corrective measures at least twice a year.

(2) The disclosure of an order to take corrective measures under paragraph (1) shall be made by publishing it on Internet websites or general daily newspapers circulated nationwide under the Act on the Promotion of Newspapers. <Amended on Jan. 27, 2010>

Article 69-2 (Scope of persons required to submit transparency reports) "Person who meets the standards prescribed by Presidential Decree" in the provisions, with the exception of the subparagraphs, of Article 64-5 (1) of the Act means a person obligated to designate a person responsible for preventing the circulation of illegally filmed materials or the like.

[This Article Added on Dec. 8, 2020]

Article 69-3 Deleted. <Aug. 4, 2020>

Article 69-4 Deleted. <Aug. 4, 2020>

Article 70 (Delegation of authority and entrustment of affairs) (1) Pursuant to Article 65 (1) of the Act, Minister of Science and ICT shall delegate the authority to impose administrative fines under Article 76 of the Act upon the following persons and to collect administrative fines from them to the Director General of the Central Radio Management Service: <Amended on Mar. 28, 2008; Jul. 3, 2008; Oct. 1, 2010; Mar. 23, 2013; Nov. 28, 2014; Jul. 26, 2017; Sep. 28, 2018; Jun. 11, 2019; Jun. 25, 2019; Dec. 7, 2021; Jul. 3, 2023>

1. A business operator not possessing line equipment under Article 22 (2) 2 of the Enforcement Decree of the Telecommunications Business Act;
2. A person required to designate and a chief information security officer, and report thereon pursuant to the proviso of Article 45-3 (1) of the Act;

2-2. A person required to ensure that the chief information security officer may not concurrently hold another office, other than the one performing duties prescribed in Article 45-3 (4) of the Act pursuant to Article 45-3 (3) of the Act;

2-3. A person who fails to comply with a corrective order issued under Article 46 (3) of the Act;

2-4. A person who fails to comply without good cause with a request to submit data under Article 46 (4) of the Act; provided, the foregoing shall not apply to the heads of relevant central administrative agencies (including their affiliated agencies);

3. A person who has registered as a provider of telecommunications billing services pursuant to Article 53 (1) of the Act.

(2) The Minister of Science and ICT shall delegate the following authority to the President of the Central Radio Management Service pursuant to Article 65 (1) of the Act: <Added on Aug. 4, 2020; Dec. 7, 2021; Jul. 3, 2023>

1. Reporting on the designation of a chief information security officer under Article 45-3 (1) of the Act;

1-2. Conducting inspections and issuing corrective orders under Article 46 (3) of the Act;

1-3. Requesting for submission of data under Article 46 (4) of the Act (limited to cases where submission of data is requested for inspection under Article 46 (3) of the Act);
2. Registration of providers of telecommunications billing services under Article 53 (1) of the Act;
3. Reporting on the modification of registered matters of a provider of telecommunications billing services, the transfer of business or acquisition by transfer of business, or the merger or inheritance of business, the succession to business, and temporary discontinuation, permanent discontinuation, dissolution of business of a provider of telecommunications billing services under Article 53 (4) of the Act;
4. Revocation of the registration of a provider of telecommunications billing services under Article 55 (1) of the Act;
5. Reporting on terms and conditions (including reporting on changes in terms and conditions) on telecommunications billing services under Article 56 (1) of the Act;
6. Recommending a provider of telecommunications billing services to change terms and conditions pursuant to Article 56 (2) of the Act;
7. Issuing orders to refuse, suspend, or restrict the provision of telecommunications billing services under Article 61 of the Act;
8. Requesting the submission of data and conducting inspections under Article 64 (1) and (3) of the Act to verify facts of violations of Articles 45-3 and 53 through 61 of the Act;
9. Issuing an order to a person who has obtained registration as a provider of telecommunications billing services pursuant to Article 53 (1) of the Act to take corrective measures under Article 64 (4) of the Act.

(3) The Korea Communications Commission shall delegate the following authority to the President of the Broadcasting and Communications Office under Article 65 (1) of the Act: <Added on Aug. 4, 2020>

1. Issuance of orders to take corrective measures and orders for making a public announcement under Article 64 (4) of the Act for a person who has violated Articles 50, 50-3 (1), 50-4, 50-5, 50-7 and 50-8 of the Act;
2. Imposition and collection of administrative fines under Article 76 of the Act on and from persons who violate Articles 50, 50-4 (4), 50-5, and 50-7 (1) and (2) of the Act.

(4) Pursuant to Article 65 (3) of the Act, the Korea Communications Commission shall entrust the following affairs to the head of the Korea Internet and Security Agency: <Amended on Mar. 28, 2008; Oct. 1, 2010; Sep. 29, 2011; Nov. 28, 2014; Aug. 4, 2020>

1. Affairs relating to a request for the submission of data and inspections under Article 64 (1) and (3) of the Act (limited to grievances and counseling items filed with the Korea Internet and Security Agency for the protection of users) to verify whether a person violates Article 22-2, 23-2, or 23-3 of the Act or falls under any subparagraph of Article 23-4 (1);
2. Duties relating to a request for the submission of data and inspections under Article 64 (1) through (3) of the Act for ascertaining a violation of any provision of Articles 50, 50-3 through 50-5, 50-7, and 50-8 of the Act (limited to grievances filed with the Korea Internet and Security Agency for settlement or counseling in connection with the transmission of advertising information).

(5) Deleted. <Aug. 4, 2020>

[Title Amended on Dec. 7, 2021]

Article 70-2 (Processing of personally identifiable information) The Minister of Science and ICT or the Korea Communications Commission (including persons delegated with the authority or entrusted with the affairs of the Minister of Science and ICT or the Korea Communications Commission under Article 70) may process data containing resident registration numbers or alien registration numbers under Article 19 (1) or (4) of the Enforcement Decree of the Personal Information Protection Act if it is essential for conducting the following business affairs:

1. Registration, etc. of providers of telecommunications billing services under Article 53 of the Act;
2. Requests for submission, perusal, inspection, etc. of materials, etc. under Article 64 (1) through (3) of the Act.

[This Article Wholly Amended on Feb. 27, 2024]

Article 71 (Re-examination of regulation) (1) Deleted. <Mar. 3, 2020>

(2) The Minister of Science and ICT shall examine the appropriateness of the following matters every 3 years (referring to the period ending on the date preceding every third

anniversary from the base date), counting from each base date specified in the following, and take measures, such as making improvements: <Amended on Dec. 30, 2016; Jul. 26, 2017; Dec. 11, 2018; Jun. 11, 2019; Dec. 8, 2020; Dec. 7, 2021; Jul. 3, 2023>

1. Qualifications of chief information security officers under Article 36-7 (4) and (6) and the scope of providers of information and communications services under paragraph (5) of that Article: January 1, 2020;
2. Protective measures by integrated information and communication facility operators, etc. under Article 37: January 1, 2017;
3. Obligations to purchase an insurance policy and the minimum amount of insurance coverage under Article 38: January 1, 2017;

3-2. Inspection of implementation under Article 39: January 1, 2024;

3-3. Reports by integrated information and communication facility operators, etc. on service interruption under Article 40: January 1, 2024;

3-4. Obligations of lessees of integrated information and communications facilities to take measures under Article 41: January 1, 2024;

4. Scope of persons subject to the certification of information protection and management systems under Article 49: January 1, 2014;
5. Follow-up management and notification on the certification of information protection and management systems under Article 51: January 1, 2017;
6. Standards for designation of certification bodies for information security management systems and examination institutions for information security management systems under Article 53: January 1, 2017;
7. Procedures for designation of certification bodies for information security management systems and examination institutions for information security management systems under Article 53-2: January 1, 2017;
8. Requirements for the registration of a provider of telecommunications billing services under Article 66-2: January 1, 2014;
9. Period and methods for preservation of transaction records under Article 66-7: January 1, 2014.

(3) Deleted. <Dec. 30, 2016>

(4) The Korea Communications Commission shall examine the appropriateness of the following matters every 3 years counting from January 1, 2024 (referring to the period that ends on the day before the base date of every third year) and shall take measures, such as making improvements. <Amended on Feb. 27, 2024; May 20, 2025>

1. Physical, technical, and administrative measures taken by identity service agencies and security measures taken by entities using connecting information under Article 13 (1) and (2);
2. Entities subject to inspection of the current status under Article 14;
3. Scope of persons obliged to designate persons responsible for the protection of youths under Article 25;
4. Criteria for persons subject to technical and administrative measures, record retention period, and types of measures under Article 35-2.

[This Article Added on Dec. 30, 2013]

Article 72 Deleted. <Dec. 27, 2010>

Article 73 Deleted. <Aug. 18, 2009>

Article 74 (Criteria for imposition of administrative fines) Criteria for the imposition of administrative fines under the provisions of Article 76 (1) through (3) of the Act are as prescribed in Appendix 9.

[This Article Wholly Amended on Oct. 1, 2010]