ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

[Enforcement Date 24. Jan, 2025.] [Act No.20068, 23. Jan, 2024., Partial Amendment]

과학기술정보통신부 (사이버침해대응과)044-202-6465 ,6466

ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

[Enforcement Date 24. Jan, 2025.] [Act No.20068, 23. Jan, 2024., Partial Amendment]
과학기술정보통신부 (사이버침해대응과) 044-202-6465 ,6466

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose) The purpose of this Act is to operate critical information and communications infrastructure in a stable manner by formulating and implementing measures concerning the protection of such infrastructure, in case of an electronic intrusion, thereby contributing to the safety of the State and the stability in people's lives.

Article 2 (Definitions) The terms used in this Act are defined as follows: <Amended on Dec. 21, 2007; Jun. 9, 2020>

1. The term "information and communications infrastructure" means electronic control and management system related to the operations for the national security, administration, national defense, public security, finance, communications, transportation, energy, etc. and information and communications network under Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection;
2. The term "electronic intrusion" means any act of attacking information and communications infrastructure by any of the following:
   (a) Means of hacking, computer virus, logic or email bombs, denial of service, high-power electromagnetic waves, etc.;
   (b) Means of installing a program, technical device, etc. that enables to circumvent normal protection and authentication processes for access to the information and communications infrastructure in the information and communications infrastructure;
3. The term "cyber security incident" means a situation took place by any act of electronic intrusions.

CHAPTER II SYSTEM FOR PROTECTING CRITICAL INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

Article 3 (Committee for protection of information and communications infrastructure) (1) The Committee for Protection of Information and Communications Infrastructure (hereinafter referred to as the "Committee") shall be established under the control of the Prime Minister, so as to deliberate on matters concerning the protection of critical information and communications infrastructure (hereinafter referred to as "critical information and communications infrastructure") designated under Article 8. <Amended on Jun. 9, 2020>

(2) The Committee shall be comprised of up to 25 members, including 1 chairperson.

(3) The Chairperson of the Committee shall be the Minister of the Office for Government Policy Coordination, and members shall be public officials holding a rank equivalent to that of a Vice Minister of a central administrative agency prescribed by Presidential Decree, and persons commissioned by the Chairperson. <Amended on Dec. 21, 2007; Feb. 29, 2008; Mar. 23, 2013; Jun. 9, 2020>

(4) Working committees, each respectively in charge of the public and private sectors, shall be established under the control of the Committee for the efficient operation of the Committee. <Amended on Dec. 21, 2007>

(5) Matters necessary for, among other things, establishing and operating the Committee and working committees shall be prescribed by Presidential Decree.

Article 4 (Functions of committee) The Committee shall deliberate on the following matters: <Amended on Dec. 21, 2007; Feb. 21, 2018; Jun. 9, 2020>

1. Matters concerning the coordination of policies for protecting critical information and communications infrastructure;
2. Matters concerning the integration and coordination of protection plans on critical information and communications infrastructure under Article 6 (1);
3. Matters concerning the outcomes of implementing protection plans on critical information and communications infrastructure under Article 6 (1);
4. Matters concerning the improvement of systems related to the protection of critical information and communications infrastructure;

4-2. Matters concerning the designation of critical information and communications infrastructure or revocation thereof under Article 8 (5);

4-3. Matters concerning whether to designate critical information and communications infrastructure under the latter part of Article 8-2 (1);

5. Other major policies concerning the protection of critical information and communications infrastructure that are submitted by the chairperson for consideration.

Article 5 (Establishment of measures to protect critical information and communications infrastructure) (1) The head of an organization which manages critical information and communications infrastructure (hereinafter referred to as "management organization") shall formulate and implement management measures, including physical and technological measures such as those for incident prevention, backup, and recovery to securely protect critical information and communications infrastructure and management information under his or her jurisdiction (hereinafter referred to as "measures to protect critical information and communications infrastructure"), based on the outcomes of the analysis and evaluation of vulnerabilities under Article 9 (1) or (2). <Amended on Jan. 20, 2015; Dec. 10, 2019>

(2) When establishing measures to protect critical information and communications infrastructure under paragraph (1), the head of a management organization shall submit details of such measures to the head of a central administrative agency in charge of critical information and communications infrastructure (hereinafter referred to as "relevant central administrative agency"); provided, this shall not apply where the head of a management organization is the head of the relevant central administrative agency. <Amended on Jun. 9, 2020>

(3) Details of measures to protect critical information and communications infrastructure of a management organization controlled and supervised by the head of a local government, shall be submitted to the Minister of the Interior and Safety by the head of the local government.<Amended on Feb. 29, 2008; Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017>

(4) The head of a management organization shall designate a person in general charge of affairs concerning the protection of critical information and communications infrastructure under his or her jurisdiction (hereinafter referred to as "chief information security officer"); provided, this shall not apply where the head of a management organization is the head of the relevant central administrative agency.

(5) Matters necessary for the designation, affairs, etc. of a chief information security officer shall be prescribed by Presidential Decree.

Article 5-2 (Verifying implementation of measures to protect critical information and communications infrastructure) (1) The Minister of Science and ICT and the heads of national agencies prescribed by Presidential Decree, such as the Director of the National Intelligence Service (hereinafter referred to as the "Director of the National Intelligence Service and head of an equivalent agency") may verify whether a management organization implements measures to protect critical information and communications infrastructure. <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

(2) The Minister of Science and ICT, Director of the National Intelligence Service, and head of an equivalent agency may request the head of the relevant central administrative agency to submit data, including the measures to protect critical information and communications infrastructure submitted to him or her under Article 5 (2), when necessary for verification under paragraph (1). <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

(3) The Minister of Science and ICT, Director of the National Intelligence Service, and head of an equivalent agency may notify the head of the relevant central administrative agency of whether measures to protect critical information and communications infrastructure verified under paragraph (1) have been implemented. <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

(4) Matters necessary for procedures for verifying the implementation of measures to protect critical information and communications infrastructure under paragraph (1) shall be prescribed by Presidential Decree.

[This Article Added on Dec. 21, 2007]

Article 6 (Establishment of plans for protecting critical information and communications infrastructure) (1) The heads of relevant central administrative agencies shall establish and implement plans for protecting critical information and communications infrastructure in areas under their jurisdiction (hereinafter referred to as "plans for protecting critical information and communications infrastructure"), by integrating and coordinating measures to protect critical information and communications infrastructure submitted under Article 5 (2). <Amended on Jun. 9, 2020>

(2) The heads of relevant central administrative agencies shall submit details on outcomes of implementing plans for protecting critical information and communications infrastructure of the previous year and plans for protecting critical information and

communications infrastructure for the following year to the Committee for deliberation; provided, this shall not apply to matters deemed confidential by the chairperson of the Committee.

(3) Plans for protecting critical information and communications infrastructure shall include the following: <Amended on Jan. 20, 2015>

1. Matters concerning the analysis and evaluation of vulnerabilities of critical information and communications infrastructure;
2. Matters concerning measures for prevention of cyber security incidents on critical information and communications infrastructure and management information, backup, and recovery;
3. Other matters necessary for the protection of critical information and communications infrastructure.

(4) The Minister of Science and ICT and the Director of the National Intelligence Service may establish guidelines for formulating measures to protect critical information and communications infrastructure and plans for protecting critical information and communications infrastructure, following consultation with each other, and may notify the heads of relevant central administrative agencies of such guidelines. <Amended on Dec. 21, 2007; Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

(5) The heads of relevant central administrative agencies shall designate a person in general charge of affairs related to the protection of critical information and communications infrastructure in areas under their jurisdiction (hereinafter referred to as an "officer in charge of information protection").

(6) Matters necessary for the establishment and implementation of plans for protecting critical information and communications infrastructure and the designation, affairs, etc. of officers in charge of information protection shall be prescribed by Presidential Decree.

Article 7 (Support for protection of critical information and communications infrastructure) (1) The heads of management organizations may request the Minister of Science and ICT, the Director of the National Intelligence Service, and head of an equivalent agency or, if deemed necessary, the heads of specialized institutions prescribed by Presidential Decree to provide technological support to the following duties, where the heads of the relevant management organizations deem it necessary to do so, or where the Chairperson of the Committee believes that inadequate measures to protect critical information and

communications infrastructure of a specific management organization are likely to cause harm to national security and the economy and society as a whole and therefore issues an order to supplement such measures: <Amended on Dec. 21, 2007; Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017; Jun. 9, 2020; Jan. 23, 2024>

1. Establishment of measures to protect critical information and communications infrastructure;
2. Prevention of cyber security incidents on critical information and communications infrastructure and the recovery thereof;
3. Compliance with an order to take protection measures under Article 11.

(2) When the head of a management organization, in charge of the following critical information and communications infrastructure which has significant influence on national security, requests for technological support under paragraph (1), he or she shall preferentially make such request to the Director of the National Intelligence Service; provided, the Director of the National Intelligence Service may provide such support, in consultation with the heads of the relevant central administrative agencies, where a substantial and imminent threat to national security exists and it is likely to cause irrecoverable damage if he or she waits for the head of a management organization to make such request: <Amended on Dec. 21, 2007>

1. Critical transportation facilities, such as roads, railroads, subways, airports and harbors;
2. Facilities for water resources and energy, including electricity, gas and oil;
3. Relay broadcast facilities and the national command control communication network;
4. Research facilities of government-funded research institutes related to nuclear energy, national defense and science, or advanced defense industry.

(3) The Director of the National Intelligent Service shall not provide technological support to any information and communications infrastructure which stores personal information, such as financial information and communications infrastructure, notwithstanding paragraphs (1) and (2). <Amended on Dec. 21, 2007; Jun. 9, 2020>

CHAPTER III DESIGNATION AND ANALYSIS OF VULNERABILITIES OF CRITICAL INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

Article 8 (Designation of critical information and communications infrastructure) (1) The heads of central administrative agencies may designate information and communications

infrastructure under their jurisdiction which is deemed to require protection from electronic intrusions, as critical information and communications infrastructure, by taking into account the following: <Amended on Dec. 10, 2019; Jun. 9, 2020>

1. The national and social importance of duties performed by an organization which manages the relevant information and communications infrastructure;
2. The degree of dependence of affairs conducted by an organization under subparagraph 1 on information and communications infrastructure;
3. The inter-connection with other information and communications infrastructure;
4. The areas and extent of damage caused by cyber security incidents to the national security, economy and society, if any;
5. The likelihood of occurrence of cyber security incidents and the easiness of recovering them.

(2) The heads of central administrative agencies may request the relevant management organization to submit data necessary for making a decision on designation under paragraph (1). <Amended on Jun. 9, 2020>

(3) The head of the relevant central administrative agency may revoke the designation of critical information and communications infrastructure either ex officio or upon request of the relevant management organization when a management organization abolishes, suspends or changes the relevant affairs.

(4) The Minister of the Interior and Safety may designate information and communications infrastructure of an organization managed and supervised by the head of a local government as critical information and communications infrastructure, in consultation with the head of the local government, or may revoke such designation.<Amended on Feb. 29, 2008; Mar. 23, 2013; Nov. 19, 2014; Jul. 26, 2017>

(5) When the head of a central administrative agency intends to grant a designation or revoke such designation under paragraphs (1) and (3), he or she shall submit it for deliberation by the Committee. In such cases, the Committee may order the head of a management organization subject to designation or the revocation thereof under paragraphs (1) and (3) to appear before the Committee and voice his or her opinions. <Amended on Jun. 9, 2020>

(6) When the head of a central administrative agency designates critical information and communications infrastructure or revokes such designation under paragraphs (1) and (3), he or she shall publicly notify such fact; provided, he or she need not publicly notify such

fact subject to deliberation by the Committee, when necessary for guaranteeing national security. <Amended on Jun. 9, 2020>

(7) Matters necessary for the designation of critical information and communications infrastructure and the revocation of such designation shall be prescribed by Presidential Decree.

Article 8-2 (Recommendation for Designation of Critical Information and Communications Infrastructure) (1) The Minister of Science and ICT, Director of the National Intelligence Service, and head of an equivalent agency may recommend the head of a central administrative agency to designate specific information and communications infrastructure as critical information and communications infrastructure, when they deem it necessary to designate such information and communications infrastructure as critical information and communications infrastructure. In such cases, the head of a central administrative agency in receipt of such recommendation shall determine whether to grant the designation subject to deliberation by the Committee. <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017; Feb. 21, 2018>

(2) The Minister of Science and ICT, Director of the National Intelligence Service, and head of an equivalent agency may request the head of a central administrative agency to submit data on the relevant information and communications infrastructure, when necessary for making a recommendation under paragraph (1). <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017>

(3) Procedures for recommending the designation of critical information and communications infrastructure under paragraph (1) and other necessary matters shall be prescribed by Presidential Decree.

[This Article Added on Dec. 21, 2007]

Article 9 (Analysis and evaluation of vulnerabilities) (1) The head of a management organization shall analyze and evaluate the vulnerabilities of critical information and communications infrastructure under his or her jurisdiction on a regular basis as prescribed by Presidential Decree. <Amended on Jun. 9, 2020>

(2) The head of a central administrative agency may order the head of a relevant management organization to analyze and evaluate the vulnerabilities of critical information and communications infrastructure in any of the following cases: <Added on Dec. 10, 2019>

1. Where necessary to protect critical information and communications infrastructure from new forms of electronic intrusion;
2. Where a separate analysis and evaluation of vulnerabilities is necessary as a result of a material change in critical information and communications infrastructure.

(3) When intending to analyze and evaluate vulnerabilities under paragraph (1) or (2), the head of a management organization shall form a task force team dedicated to analyzing and evaluating the vulnerabilities as prescribed by Presidential Decree. <Amended on Dec. 10, 2019>

(4) Where the head of a management organization intends to analyze and evaluate vulnerabilities under paragraph (1) or (2), he or she may require any of the following institutions to analyze and evaluate the vulnerabilities of critical information and communications infrastructure under his or her jurisdiction; provided, in such cases, he or she need not form a task force team under paragraph (3): <Amended on Dec. 18, 2002; Dec. 21, 2007; May 22, 2009; Mar. 23, 2013; Jun. 22, 2015; Dec. 10, 2019>

1. The Korea Internet and Security Agency (hereinafter referred to as "KISA") under Article 52 of the Act on Promotion of Information and Communications Network Utilization and Information Protection;
2. Information sharing and analysis centers under Article 16 (limited to information sharing and analysis centers which meet the standards prescribed by Presidential Decree);
3. Enterprises specializing in information security services, designated under Article 23 of the Act on the Promotion of Information Security Industry;
4. The Electronics and Telecommunications Research Institute under Article 8 of the Act on the Establishment, Operation, and Fostering of Government-Funded Research Institutes.

(5) The Minister of Science and ICT shall determine standards for the analysis and evaluation of vulnerabilities under paragraphs (1) and (2), in consultation with the heads of relevant central administrative agencies and the Director of the National Intelligence Service, and shall notify the heads of the relevant central administrative agencies of such standards. <Amended on Feb. 29, 2008; Mar. 23, 2013; Jul. 26, 2017; Dec. 10, 2019>

(6) Matters necessary for the methods, procedures, etc. for analyzing and evaluating the vulnerabilities of critical information and communications infrastructure shall be prescribed by Presidential Decree. <Amended on Dec. 10, 2019>

CHAPTER IV PROTECTION OF CRITICAL INFORMATION AND COMMUNICATIONS INFRASTRUCTURE AND RESPONSE TO CYBER SECURITY INCIDENTS

Article 10 (Protection guidelines) (1) The heads of the relevant central administrative agencies may establish protection guidelines on critical information and communications infrastructure under their jurisdiction and order the head of a management organization in the relevant area to comply with such guidelines. <Amended on Jan. 23, 2024>

(2) The head of the management organization in receipt of an order under paragraph (1) shall comply with the order. <Add on Jan. 23, 2024>

(3) The heads of the relevant central administrative agencies shall revise and supplement protection guidelines under paragraph (1) on a regular basis, taking into account technological advancements, etc. <Amended on Jun. 9, 2020; Jan. 23, 2024>

Article 11 (Orders for protection measures) (1) The heads of the relevant central administrative agencies may order the head of the relevant management organization to take measures necessary to protect critical information and communications infrastructure, in any of the following cases: <Amended on Jan. 23, 2024>

1. Where it is deemed necessary to take separate protection measures after analyzing the measures to protect critical information and communications infrastructure submitted under Article 5 (2);
2. Where it is deemed necessary to take separate protection measures after analyzing whether the measures to protect critical information and communications infrastructure notified under Article 5-2 (3) have been implemented.

(2) Notwithstanding paragraph (1), where the head of a relevant central administrative agency does not issue an order for protection measures, the Minister of Science and ICT and the Director of the National Intelligence Service, etc. may order the head of the relevant management agency to take measures necessary for the protection of critical information and communications infrastructure on behalf of the head of the relevant central administrative agency. <Added on Jan. 23, 2024>

[This Article Wholly Amended on Dec. 21, 2007]

[Title Amended on Jan. 23, 2024]

Article 12 (Prohibition against intrusion on critical information and communications infrastructure) No one shall commit any of the following acts: <Amended on Jun. 9, 2020>

1. Accessing critical information and communications infrastructure by any person who has no access authority, or manipulating, destroying, concealing or leaking stored data by any person who exceeds his/her access authority;
2. Destroying the data of critical information and communications infrastructure, or using programs, such as computer viruses and logic bombs, with the intention of obstructing the operation of critical information and communications infrastructure;
3. Abruptly sending large amounts of signals with the intention of obstructing the operation of critical information and communications infrastructure, or causing errors in information processing by such means as inducing the processing of improper orders.

Article 13 (Notification of cyber security incident) (1) When the head of a management organization recognizes that the occurrence of cyber security incidents has led to the disturbance, paralysis, or destruction of critical information and communications infrastructure under his or her jurisdiction, he or she shall notify a relevant administrative agency, an investigation agency, or KISA (hereinafter referred to as "relevant organization, etc.") of such fact. In such cases, the relevant organizations, etc. shall take measures necessary for preventing the spread of damage caused by cyber security incidents and swiftly respond to such incidents. <Amended on Mar. 23, 2013>

(2) The Government may provide financial support for expenses incurred in recovering from damage and the like to a management organization that has contributed to preventing the spread of damage by notifying cyber security incidents under paragraph (1), within the budget. <Amended on Jun. 9, 2020>

Article 14 (Recovery measures) (1) The head of a management organization shall take measures necessary to recover and protect relevant information and communications infrastructure in a swift manner upon occurrence of a cyber security incident on critical information and communications infrastructure under his or her jurisdiction.

(2) The head of the relevant central administrative agency may, when a cyber security incident on critical information and communications infrastructure occurs, order the head of the relevant management organization to take measures to recover and protect critical information and communications infrastructure. <Amended on Jan. 23, 2024>

(3) Notwithstanding paragraph (2), where the head of a relevant central administrative agency does not issue an order to take measures for recovery and protection, the Minister of Science and ICT and the Director of the National Intelligence Service, etc. may order the head of the relevant management agency to take measures necessary for the recovery and protection of critical information and communications infrastructure on behalf of the head of the relevant central administrative agency. <Amended on Jan. 23, 2024>

(4) The head of a management organization may request the head of a relevant central administrative agency or the head of KISA to provide support when necessary for taking measures for recovery and protection under paragraphs (1) through (3); provided, this shall not apply in cases falling under Article 7 (2). <Added on Jan. 23, 2024>

(5) When the head of the relevant central administrative agency or the head of KISA receives requests for support under paragraph (4), he or she shall provide support necessary for the fast recovery from damage, such as technological support, and shall take appropriate measures to prevent the spread of damage, in cooperation with the head of a management organization. <Added on Jan. 23, 2024>

Article 15 (Organization of headquarters for countermeasures) (1) When cyber security incidents on critical information and communications infrastructure occur in a wide range, the chairperson of the Committee may establish the Headquarters for Countermeasures against Cyber Security Incidents on Information and Communications Infrastructure (hereinafter referred to as the "Countermeasure Headquarters") under the control of the Committee, fixing a period for taking emergency measures, providing technological support, and recovering from damage, etc.

(2) The chairperson of the Committee may request the dispatch of public officials related to the affairs of the Countermeasure Headquarters to the head of a relevant administrative agency.

(3) The chairperson of the Committee shall appoint the head of the Countermeasure Headquarters, in consultation with the head of a central administrative agency in charge of information and communications infrastructure on which cyber security incidents occurred.

(4) The head of the Headquarters for Countermeasures may request the head of the relevant administrative agency, the head of a management organization and the head of KISA, to provide cooperation and support to respond to cyber security incidents on critical information and communications infrastructure. <Amended on Mar. 23, 2013>

(5) Upon a request for cooperation and support under paragraph (4), the head of the relevant administrative agency, etc. shall comply with such request, unless there is a special reason not to do so. <Newly Inserted on Jun. 9, 2020>

(6) Matters necessary for the organization and operation of the Countermeasure Headquarters shall be prescribed by Presidential Decree.

Article 16 (Information sharing and analysis center) (1) Any person who intends to perform the following affairs to protect information and communications infrastructure by area, such as finance and communications, may establish and operate an information sharing and analysis center:

1. Provision of information concerning vulnerabilities, intrusion factors, and countermeasures;
2. Operation of the real-time alarm and analysis system if cyber security incidents occur.

(2) Deleted. <Dec. 22, 2015>

(3) Deleted. <Dec. 22, 2015>

(4) The Government may encourage the establishment of an information sharing and analysis center which performs duties falling under each subparagraph of paragraph (1) and may provide financial and technological support thereto. <Amended on Dec. 22, 2015>

(5) Deleted. <Dec. 22, 2015>

CHAPTER V Deleted.

Article 17 Deleted. <May 22, 2009>

Article 18 Deleted. <May 22, 2009>

Article 19 Deleted. <May 22, 2009>

Article 20 Deleted. <May 22, 2009>

Article 21 Deleted. <May 22, 2009>

Article 22 Deleted. <May 22, 2009>

Article 23 Deleted. <May 22, 2009>

CHAPTER VI TECHNOLOGICAL SUPPORT AND COOPERATION WITH THE PRIVATE SECTOR

Article 24 (Technological development) (1) The Government may formulate implementation policies for the development of technology necessary for protecting information and communications infrastructure and the fostering of specialized human resources.

(2) The Government may require research institutes and private organizations related to the development of information protection technology to develop technology on its behalf, when necessary for efficiently advancing development of technology necessary for the protection of information and communications infrastructure. In such cases, the Government may fully or partially subsidize expenses incurred in such development.

Article 25 (Support for management organization) With respect to a management organization, the Government may transfer technology necessary for protecting critical information and communications infrastructure and may provide equipment and other necessary support.

Article 26 (International cooperation) (1) The Government shall identify international trends concerning the protection of information and communications infrastructure and promote international cooperation.

(2) The Government may provide support for international exchanges of related technologies and human resources and projects for international standardization, international joint research and development, etc. so as to promote international cooperation for the protection of information and communications infrastructure.

Article 27 (Obligation of confidentiality) No one who is or has been employed in any of the following organizations shall divulge any confidential information obtained in the course of performing his or her duties; provided, this shall not apply where any other statute provides otherwise: <Amended on Dec. 21, 2007; Dec. 10, 2019; Jun. 9, 2020>

1. The Committee and the working committees under Article 3;
2. Any organization in charge of the analysis and evaluation of the vulnerabilities of critical information and communications infrastructure under Article 9 (4);

3. Any relevant organization which performs duties related to the acceptance of notification of cyber security incidents and recovery measures under Article 13;
4. Any information sharing and analysis center which performs duties referred to in the subparagraphs of Article 16 (1).

CHAPTER VII PENALTY PROVISIONS

Article 28 (Penalty provisions) (1) Any person who disturbs, paralyzes or destroys critical information and communications infrastructure, in violation of Article 12, shall be punished by imprisonment with labor for not more than 10 years or by a fine not exceeding 100 million won.

(2) Any person who has attempted a crime referred to in paragraph (1) shall be subject to punishment.

Article 29 (Penalty provisions) Any person who divulges any confidential information, in violation of Article 27, shall be punished by imprisonment with labor for not more than five years, by suspension of qualifications for not more than 10 years, or by a fine not exceeding 50 million won.

Article 30 (Administrative fines) (1) Any of the following persons shall be subject to a fine not exceeding 50 million won; provided, the foregoing shall not apply if the head of a management organization is the head of the relevant central administrative agency (including the head of its affiliated agency): <Added on Jan. 23, 2024>

1. A person who fails to comply with an order issued under Article 10 (1);
2. A person who fails to comply with an order for recovery and protection measures under Article 14 (2) or (3).

(2) Any of the following persons shall be subject to a fine not exceeding 30 million won; provided, the foregoing shall not apply if the head of a management organization is the head of the relevant central administrative agency (including the head of its affiliated agency): <Amended on Dec. 21, 2007; Jun. 9, 2020. 6. 9; Jun. 10, 2022; Jan. 23, 2024>

1. A person who violates an order for protection measures under Article 11 (1) or (2);
2. Deleted; <Dec. 22, 2015>

3. Deleted; <May 22, 2009>
4. Deleted; <May 22, 2009>
5. Deleted. <May 22, 2009>

(3) Any of the following persons shall be subject to a fine not exceeding 5 million won: Provided That, the foregoing shall not apply if the head of a management organization is the head of the relevant central administrative agency (including the head of its affiliated agency). <Added on Jun. 10, 2022; Jan. 23, 2024>

1. A person who fails to analyze and evaluate vulnerabilities on a regular basis, in violation of Article 9 (1);
2. A person who fails to comply with an order to analyze and evaluate vulnerabilities, in violation of Article 9 (2).

(4) Deleted. <Mar. 14, 2017>

(5) Deleted. <Mar. 14, 2017>

(6) Deleted. <Mar. 14, 2017>

(7) An administrative fine under paragraphs (1) and (3) shall be imposed and collected by the head of the relevant central administrative agency or the Minister of Science and ICT as prescribed by Presidential Decree. <Amended on Feb. 29, 2008; May 22, 2009; Mar. 23, 2013; Jul. 26, 2017; Jun. 9, 2020; Jun. 10, 2022; Jan. 23, 2024>