The Basic Act on Cybersecurity

(Act No. 104 of November 12, 2014)

Table of Contents

Chapter I General Provisions

(Purpose)

Article 1 In consideration of the fact that ensuring cybersecurity while securing the free flow of information is an urgent issue, due to the increasing severity of threats to cybersecurity and other changes in internal and external circumstances that are arising on a global scale, as the internet and other advanced information and telecommunications networks develop, and the use of information and communications technologies (referred to below as "information and telecommunications technologies") prescribed in Article 2 of the Basic Act on the Formation of a Digital Society (Act No. 35 of 2021) expands, the purpose of this Act is to set basic principles for Japan's cybersecurity policies, clarify the responsibilities and other aspects of the national and local governments, and provide for the formulation of a cybersecurity strategy and other particulars that will become the foundation of cybersecurity policies, and also in conjunction with the same Act, to comprehensively and effectively advance cybersecurity policies in ways such as establishing a Cybersecurity Strategic Headquarters, and by doing so, to enhance economic and social vitality and achieve sustainable development and bring about a society which enables its people to live safely and free of anxiety, and also to contribute to ensuring peace and safety in the international community and contribute to Japan's national security.

(Definitions)

Article 2 The term "cybersecurity" as used in this Act means that the necessary measures have been taken to prevent the leakage, loss, or damage of information that is recorded, sent, transmitted, or received in electronic form, magnetic form, or any other form that cannot be perceived by the human

senses (referred to below as "electronic or magnetic form" in this Article) and to securely manage that information in other ways; that the necessary measures have been taken to ensure the security and reliability of information systems and of information and communications networks (including the necessary measures to prevent damage from unauthorized activities directed at a computer through an information and communications network or through a storage medium associated with a record that has been created in electronic or magnetic form (referred to below as "electronic or magnetic recording medium")); and that these systems and networks are being properly maintained and managed.

(Basic Principles)

Article 3 (1) In consideration of the fact that ensuring the free flow of information through the development of the internet and other advanced information and telecommunications networks, and through the use of information and communications technologies is important for such aspects as people's enjoyment of freedom of expression, the creation of innovations, and the enhancement of economic and social vitality through the use of these networks and technologies; cybersecurity policy must be advanced with the principle to proactively respond to cybersecurity threats, through coordination among a variety of entities, such as national and local governments and critical social infrastructure providers (meaning those engaged in business that provides infrastructure which is the foundation of the lives of the people and economic activities, and whose functional failure or deterioration would cause an enormous impact to them; the same applies below).

(2) The cybersecurity policy must be advanced with the principle to raise awareness for each individual member of the public about cybersecurity and encourage each individual member of the public to take voluntary actions, and positively promote actions to establish resilient systems which can prevent any damage caused by threats against cybersecurity and quickly recover from damage or failure.

(3) The cybersecurity policy must be advanced with the principle of developing the internet and other such advanced information and telecommunications networks, and positively promote actions to establish a vital economy and society through the utilization of information and communications technologies.

(4) The cybersecurity policy must be advanced through international cooperation with the principle for Japan to assume a leading role in formulating and developing an international cybersecurity framework, in consideration of the fact that responding to cybersecurity threats is a common issue throughout the international community, and that Japan's economy and society operate within the context of internationally close and interdependent relationships.

(5) The cybersecurity policy must be advanced in consideration of the basic principles of the Basic Act on the Formation of a Digital Society.
(6) The cybersecurity policy must be advanced with due consideration not to unjustly infringe on the rights of the people.

(Responsibilities of the National Government)
Article 4 The national government is responsible for formulating and implementing comprehensive cybersecurity policies in line with the basic principles prescribed in the preceding Article (referred to below as "basic principles").

(Responsibilities of Local Governments)
Article 5 Local governments are responsible for formulating and implementing independent cybersecurity policies in line with the basic principles, and in consideration of the appropriate division of roles with the national government.

(Responsibilities of Critical Social Infrastructure Providers)
Article 6 In line with the basic principles, a critical social infrastructure provider is to deepen their interest in and understanding of the importance of cybersecurity and to endeavor independently and actively to ensure cybersecurity, as well as endeavoring to cooperate in the implementation of the cybersecurity policy that the national or local government implements, to provide their services in a stable and appropriate manner.

(Responsibilities of Cyberspace-Related Business Entities and Other Business Entities)
Article 7 In line with the basic principles, cyberspace-related business entities (meaning those engaged in business regarding the maintenance of the internet and other advanced information and telecommunications networks, the utilization of information and communications technologies, or business relating to cybersecurity; the same applies below) and other business entities are to endeavor independently and actively to ensure cybersecurity, as well as endeavoring to cooperate in the implementation of the cybersecurity policy that the national or local government implements, in the course of their business activities.

(Responsibilities of Educational and Research Organizations)
Article 8 In line with the basic principles, universities and other educational and research organizations are to independently and actively endeavor to ensure cybersecurity, foster human resources related to cybersecurity, carry out research on cybersecurity, and disseminate the results, while endeavoring to

cooperate with the cybersecurity policy that the national or local government implements.

(Efforts of the People)

Article 9 In line with the basic principles, the people are to endeavor to deepen their interest in and understanding of the importance of cybersecurity and pay necessary attention to ensuring cybersecurity.

(Legislative Measures)

Article 10 The national government must take legislative, financial, or tax measures or any other measures that are necessary to implement the cybersecurity policy.

(Development of Administrative Organizations)

Article 11 In implementing the cybersecurity policy, the national government is to endeavor to develop administrative organizations and to improve administrative management.

Chapter II Cybersecurity Strategy

Article 12 (1) The national government must establish a basic plan for cybersecurity (referred to below as the "cybersecurity strategy") to comprehensively and effectively promote the cybersecurity policy.

(2) The cybersecurity strategy is to provide for the following particulars:

(i) basic guidelines for the cybersecurity policy;

(ii) information concerning the ensuring of cybersecurity within national administrative organs and other related organs;

(iii) information concerning the promotion of ensuring cybersecurity in critical social infrastructure providers, the associations that they form, and local governments (referred to below as "critical social infrastructure providers and other related entities"); and

(iv) beyond what is stated in the preceding three items, information necessary to comprehensively and effectively promote cybersecurity policies.

(3) The Prime Minister must request a cabinet decision on the proposed cybersecurity strategy.

(4) When the cybersecurity strategy is established, the national government must report it to the Diet without delay and make it public through the use of the internet and other appropriate means.

(5) The provisions of the preceding two paragraphs apply mutatis mutandis in the case of amendments to the cybersecurity strategy.

(6) The national government must endeavor to take necessary measures for

implementing the cybersecurity strategy smoothly, such as appropriating the necessary funding in the budget each fiscal year, to the extent that national finances allow, to ensure necessary funding for the costs needed to implement the cybersecurity strategy.

Chapter III Basic Policies

(Ensuring Cybersecurity at National Administrative Organs and Related Organs)

Article 13 Regarding cybersecurity at national administrative organs, incorporated administrative agencies (referring to incorporated administrative agencies prescribed in Article 2, paragraph (1) of the Act on General Rules for Incorporated Administrative Agencies (Act No. 103 of 1999); the same applies below), special corporations (referring to a corporation directly incorporated by law or incorporated by a special law through a special incorporation procedure which is subject to Article 4, paragraph (1), item (viii) of the Act for Establishment of the Ministry of Internal Affairs and Communications (Act No. 91 of 1999); the same applies below), and so forth, the national government is to provide necessary measures including: formulating common standards of cybersecurity measures for national administrative organs, incorporated administrative agencies and designated corporations (special corporations and authorized corporations (referring to a corporation incorporated by a special law which needs the approval of a governmental entity for their incorporation and associated matters; the same applies in Article 33, paragraph (1)) which are designated by the Cybersecurity Strategic Headquarters as ones for which the national government needs to further enhance measures which it is providing to ensure cybersecurity, in consideration of the impact on the people's living conditions and economic activities accrued in the case in which cybersecurity in the corporations is not ensured; the same applies below); the collaborative use of interoperable information systems among national administrative organs; monitoring and analysis of malicious activities against information systems of national administrative organs, incorporated administrative agencies or designated corporations through information and communications networks or electronic or magnetic recording media; cybersecurity exercises and training at national administrative organs, incorporated administrative agencies and designated corporations; responses to cybersecurity threats in cooperation, communication and coordination with relevant domestic and foreign parties; the sharing of information regarding cybersecurity among national administrative organs, incorporated administrative agencies, special corporations, and so forth.

(Ensuring Cybersecurity at Critical Social Infrastructure Providers and Other Related Entities)

Article 14 The national government is to provide measures such as formulating standards, exercises and training, information sharing, and promoting other voluntary activities, and other necessary measures regarding cybersecurity in critical social infrastructure providers and other related entities.

(Facilitation of Voluntary Activities of Private Enterprises, Educational, Research, and Other Organizations)

Article 15 (1) The national government is to provide necessary measures, including increasing interest in and understanding of the importance of cybersecurity, offering consultation on cybersecurity, and providing necessary information and advice, to promote the voluntary activities for cybersecurity of private enterprises such as small and medium-sized enterprises, or of educational and research organizations such as universities, considering that information related to their intellectual property is critical for enhancing Japan's international competitiveness.

(2) Considering that it is important for each member of the public to make an effort to voluntarily endeavor to ensure cybersecurity, the national government is to provide necessary measures, including offering consultation on cybersecurity and providing necessary information and advice on actions such as, appropriate choices about products and services in the daily use of computers, the internet or other advanced information and telecommunications networks.

(Coordination with Diverse Entities)

Article 16 The national government is to enhance coordination among relevant administrative organs, and is to take necessary measures to enable diverse entities, such as the national government, local governments, critical social infrastructure providers, and cyberspace-related business entities, to work on cybersecurity policies in mutual coordination.

(Cybersecurity Council)

Article 17 (1) The Chief of the Cybersecurity Strategic Headquarters prescribed in Article 28, paragraph (1) and the commissioned Minister of State (referred to as "Chief, etc." in the following paragraph) is to establish the Cybersecurity Council (referred to below as the "Council" in this Article) to hold the necessary consultations on the advancement of cybersecurity policies.

(2) When the Chief, etc. finds it necessary to do so, upon going through deliberations, the Chief, etc. may have the following persons join the Council as members:

(i) heads of national administrative organs (excluding the Chief, etc.);
(ii) local governments or associations that they form;
(iii) critical social infrastructure providers or associations that they form;
(iv) cyberspace-related business entities or associations that they form;
(v) universities and other educational and research organizations, or associations that they form;
(vi) other persons considered to be necessary by the Chief, etc.

(3) The Council may request its members concerned for submission of materials, expression of opinions, explanations, or any other cooperation regarding the advancement of cybersecurity policies when the Council finds it necessary for consultations referred to in paragraph (1). In this case, the members of the Council must respond to the request, unless there is a justifiable reason for not doing so.

(4) Any person who engages or previously engaged in the affairs of the Council must not divulge or misappropriate any secrets learned in connection with those affairs without justifiable grounds.

(5) The general affairs of the Council are performed by the Cabinet Secretariat and managed by an Assistant Chief Cabinet Secretary as ordered.

(6) Beyond what is prescribed in the preceding paragraphs, necessary matters concerning the organization and operation of the Council are prescribed by the Council.

(Cybercrime Control and Prevention of Spread of Damage)

Article 18 The national government is to take necessary measures to control cybersecurity-related crimes and prevent the spread of damage caused by them.

(Response to Incidents Which May Critically Impact the Country's Safety)

Article 19 The national government is to take necessary measures to improve and strengthen systems at the relevant bodies, and to strengthen mutual coordination and clarify the division of roles among the relevant bodies for responding to cybersecurity-related incidents that might critically affect the country's safety.

(Enhancement of Industrial Development and International Competitiveness)

Article 20 In consideration of the fact that it is critical for Japan to have self-reliant capabilities to ensure cybersecurity, the national government is to take necessary measures related to cybersecurity, including the promotion of advanced research and development, technological advancements, the development and recruitment of human resources, the strengthening of the market environment and the development of new businesses through the improvement of competitive conditions, the internationalization of

technological safety and reliability standards and the participation in frameworks for mutual recognition of those standards, to create new business opportunities, develop sound businesses, and enhance international competitiveness, so that the cybersecurity sector can become a "growth industry" which creates employment opportunities.

(Promotion of Research and Development)

Article 21 In consideration of the fact that it is critical for Japan to maintain self-reliant technological cybersecurity capabilities, the national government is to take necessary measures related to cybersecurity, including the improvement of the cybersecurity research environment, the promotion of basic research on technological safety and reliability, the promotion of research and development for core technologies, the development of skilled researchers and engineers, the strengthening of coordination among national research institutes, universities, the private sector, and other relevant parties, and international coordination for research and development, to promote research and development for cybersecurity and its technological and other relevant demonstrations, and to have the relevant cybersecurity results publicized.

(Development of Human Resources)

Article 22 (1) In close coordination and cooperation with universities, colleges of technology, specialized training colleges, private enterprises, and other relevant entities, the national government is to take necessary measures to ensure appropriate employment conditions and treatment of the workforce in the field of cybersecurity, and by doing so, enabling their duties and work environments to become attractive enough to meet their professional values.

(2) In close coordination and cooperation with universities, colleges of technology, specialized training colleges, private enterprises, and other relevant entities, for the purposes of recruitment, development, and quality improvement of cybersecurity-related human resources, the national government is to take necessary measures, including the utilization of a qualification scheme and training of young technical experts.

(Promotion of Education and Learning, Public Awareness Raising)

Article 23 (1) The national government is to take necessary measures, including the promotion of education and learning, public awareness activities, and the dissemination of knowledge in the field of cybersecurity, to deepen interest and understanding about cybersecurity among the people on a broad scale.

(2) The national government is to take necessary measures, including the implementation of events for public awareness and the dissemination of information on cybersecurity, and the designation of the period to promote

cybersecurity activities in a focused and effective manner, to contribute to the promotion of the measures prescribed under the preceding paragraph.

(Promotion of International Cooperation)

Article 24 In order for Japan to play an active role in the international community in the field of cybersecurity and promote Japan's international interests, the national government is to advance international cooperation relating to cybersecurity, including through independent participation in the formulation of international rules, by building relationships of trust and promoting information-sharing on an international level, by providing active support for capacity building in developing regions' cybersecurity response and other such international technological cooperation, and through crime control; and is also to take the necessary measures for deepening other countries' understanding of cybersecurity in Japan.

Chapter IV Cybersecurity Strategic Headquarters

(Establishment)

Article 25 The Cybersecurity Strategic Headquarters (referred to below as the "Headquarters") is established under the Cabinet to effectively and comprehensively advance cybersecurity policies.

(Affairs under Jurisdiction of the Headquarters)

Article 26 (1) The Headquarters is responsible for the following affairs:

(i) preparing a draft of the cybersecurity strategy and promoting its implementation;

(ii) establishing the standards of cybersecurity measures for national administrative organs, incorporated administrative agencies and designated corporations, and promoting the implementation of the evaluation (including audit) of measures based on the standards and other measures taken based on the standards;

(iii) evaluating the countermeasures against critical cybersecurity-related incidents involving national administrative organs, incorporated administrative agencies or designated corporations (including investigation into finding the cause or causes of an incident);

(iv) facilitating communication and coordination with domestic and foreign parties concerned when a cybersecurity-related incident occurs; and

(v) beyond the affairs stated in the preceding items, engaging in research and deliberation on proposals for major cybersecurity policies; establishing cross-departmental plans; making guidelines for estimates of relevant administrative organs' expenditures and establishing the basic principles for

implementing their policies; promoting the implementation of those policies, such as evaluating them; and carrying out overall coordination.

(2) In preparing a draft of the cybersecurity strategy, the Headquarters must hear the opinions of the National Security Council in advance.

(3) The Headquarters is to work in close coordination with the National Security Council on critical issues concerning cybersecurity in the context of national security.

(Organization)

Article 27 The Headquarters consists of the Chief of the Cybersecurity Strategic Headquarters, the Deputy Chief of the Cybersecurity Strategic Headquarters, and the members of the Cybersecurity Strategic Headquarters.

(Chief of the Cybersecurity Strategic Headquarters)

Article 28 (1) The person in charge of the Headquarters is referred to as the Chief of the Cybersecurity Strategic Headquarters (referred to below as the "Chief"), and the Chief Cabinet Secretary serves in that capacity.

(2) The Chief engages in the overall management of the Headquarters' affairs and directs and supervises personnel at the Headquarters.

(3) The Chief may make recommendations to the heads of relevant administrative organs when it is found necessary, based on the evaluations prescribed in Article 26, paragraph (1), items (ii), (iii), and (v), or the documents, information or other materials provided pursuant to the provisions of the Articles 32 or 33.

(4) After making the recommendations pursuant to the provisions of the preceding paragraph, the Chief may request a report from the heads of the relevant administrative organs regarding the measures taken based on the recommendations.

(5) In relation to the recommendations made pursuant to the provisions of paragraph (3) of this Article, when the Chief finds it particularly necessary to do so, the Chief may present opinions to the Prime Minister to take action under Article 6 of the Cabinet Law (Act No. 5 of 1947) in regards to the relevant matter.

(Deputy Chief of the Cybersecurity Strategic Headquarters)

Article 29 (1) The Deputy Chief of the Cybersecurity Strategic Headquarters (referred to below as the "Deputy Chief") is assigned to the Headquarters, and a Minister of State serves in that capacity.

(2) The Deputy Chief assists the Chief's duties.

(Members of the Cybersecurity Strategic Headquarters)

Article 30 (1) The members of the Cybersecurity Strategic Headquarters are assigned to the Headquarters (referred to as "members" in the following paragraph).

(2) Those listed below are designated as members (except in a case in which someone listed in items (i) through (vi) is designated as the Deputy Chief):

(i) the Chairperson of the National Public Safety Commission;

(ii) the Minister for Digital Transformation;

(iii) the Minister for Internal Affairs and Communications;

(iv) the Minister for Foreign Affairs;

(v) the Minister of Economy, Trade and Industry;

(vi) the Minister of Defense;

(vii) beyond the persons stated in the preceding items, the person whom the Prime Minister designates from among any Ministers of State other than the Chief and Deputy Chief, as those considered indispensable in carrying out the affairs under the jurisdiction of the Headquarters; and

(viii) among experts with exceptional knowledge and experiences with cybersecurity, those designated by the Prime Minister.

(Entrustment of Affairs)

Article 31 (1) The Headquarters, according to the category of affairs stated in the following items, may entrust a part of its affairs to the persons specified in each of the items:

(i) affairs stated in Article 26, paragraph (1), item (ii) (limited to one relating to audit based on the standards of cybersecurity measures for incorporated administrative agencies and designated corporations) or affairs stated in item (iii) of that paragraph (limited to one relating to investigation into finding the cause of critical cybersecurity-related incidents involving incorporated administrative agencies or designated corporations): the Information-technology Promotion Agency, Incorporated Administrative Agency or a corporation specified by Cabinet Order as one that has sufficient technical competence and expert knowledge and experience concerning the cybersecurity measures and that is capable of carrying out those affairs reliably; and

(ii) affairs stated in Article 26, paragraph (1), item (iv): a corporation specified by Cabinet Order as having sufficient technical competence and specialized knowledge and experience in communication and coordination with domestic and foreign parties in the event of a cybersecurity-related incident, and that is capable of carrying out those affairs reliably.

(2) An officer or employee of a corporation that has been entrusted with affairs pursuant to the provisions of preceding paragraph or a person who had been in that position, must not divulge or misappropriate any secrets learned in

connection with those affairs under that entrustment, without justifiable grounds.

(3) An officer or employee of a corporation entrusted with affairs pursuant to the provisions of paragraph (1) who engages in the affairs under the entrustment, is deemed to be an official engaged in public services pursuant to laws and regulations, regarding the application of the Penal Code (Act No. 45 of 1907) or other penal provisions.

(Submission of Materials)

Article 32 (1) The heads of relevant administrative organs must provide the Headquarters with materials or information related to cybersecurity that is beneficial to the performance of the affairs under its jurisdiction in a timely manner, as set by Headquarters.

(2) Beyond what is provided for in the preceding paragraph, as requested by the Chief, the heads of the relevant administrative organs must cooperate with the Headquarters, such as by providing materials or information related to cybersecurity that is necessary for the performance of the affairs under its jurisdiction, or by explaining those materials or information.

(Submission of Materials and Other Cooperation)

Article 33 (1) If the Headquarters finds it necessary to do so for performing the affairs under its jurisdiction, in relation to the measures which the Headquarters takes in coordination with the national government, or other cybersecurity measures for preventing the spread of damage caused by threats against cybersecurity and promoting a quick recovery from any damage, it may request to submit the necessary materials, present the necessary opinions, give the necessary explanation, or provide any other cooperation from the following persons: the heads of local governments or incorporated administrative agencies; the deans or the presidents of national university corporations (meaning national university corporations prescribed in Article 2, paragraph (1) of the National University Corporation Act (Act No.112 of 2003)); the heads of inter-university research institute corporations (meaning inter-university research institute corporations provided for in Article 2, paragraph (3) of the same Act); the president of the Japan Legal Support Center (meaning the Japan Legal Support Center provided for in Article 13 of the Comprehensive Legal Support Act (Act No. 74 of 2004)); the representatives of special corporations or authorized corporations designated by the Headquarters; and the representatives of the relevant entity facilitating cybersecurity-related communication and coordination with domestic and foreign parties concerned. In that case, the relevant person must respond to the request, unless there is a justifiable reason for not doing so.

(2) If the Headquarters finds it particularly necessary to do so for performing the affairs under jurisdiction of the Headquarters, it may request the cooperation referred to in the preceding paragraph from a party other than the parties prescribed in the same paragraph.

(Cooperation for Local Governments)

Article 34 (1) If a local government finds it necessary to do so for formulating or implementing the policy prescribed in Article 5, it may request the Headquarters to provide information and other cooperation.

(2) If the Headquarters is requested cooperation under the preceding paragraph, it is to endeavor to meet the request.

(Affairs)

Article 35 The affairs of the Headquarters are performed by the Cabinet Secretariat and managed by an Assistant Chief Cabinet Secretary as ordered.

(Competent Minister)

Article 36 For matters related to the Headquarters, the Prime Minister serves as the competent minister referred to in the Cabinet Act.

(Delegation to Cabinet Orders)

Article 37 Beyond what is provided for in this Act, Cabinet Order prescribes the necessary matters relating to the Headquarters.

Chapter V Penal Provisions

Article 38 A person who violates the provisions of Article 17, paragraph (4) or Article 31, paragraph (2) is subject to imprisonment for not more than one year or a fine of not more than 500,000 yen.

Supplementary Provisions

(Effective Date)

Article 1 This Act comes into effect as of the date of promulgation; provided, however, that the provisions of Chapters II and IV as well as Article 4 of the Supplementary Provisions come into effect as of the day specified by Cabinet Order within a period not exceeding one year from the date of promulgation.

(Review)

Article 2 For cybersecurity incidents classed as emergencies specified in Article 21, paragraph (1) of the Act on the Peace and Independence of Japan and

Maintenance of the Nation and its People's Security in an Armed Attack Situations (Act No.79 of 2003), and other malicious activities against computers through information and communications networks or electronic or magnetic recording media, the national government is to review, from a broad point of view, measures aimed at further strengthening the capability of the defense of infrastructure which is the foundation of the peoples' living conditions and economic activities, and the functional failure or deterioration of which would risk enormous impacts on them.

Supplementary Provisions [Act No.66 of September 11, 2015] [Extract]

(Effective Date)

Article 1 This Act comes into effect as of April 1, 2016.

Supplementary Provisions [Act No.76 of September 30, 2015] [Extract]

(Effective Date)

Article 1 This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding six months from the date of promulgation.

Supplementary Provisions [Act No.31 of April 22, 2016] [Extract]

(Effective Date)

Article 1 This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding six months from the date of promulgation; provided, however, that the provisions of the following Article and Article 3, Article 5 and Article 6 of the Supplementary Provisions come into effect as of the date of promulgation.

(Delegation to Cabinet Order)

Article 6 Beyond what is provided for in Articles 2 through the preceding Article of the Supplementary Provisions, Cabinet Order prescribes the necessary transitional measures for the enforcement of this Act (including transitional measures for penal provisions).

Supplementary Provisions [Act No.91 of December 12, 2018] [Extract]

(Effective Date)

(1) This Act comes into effect as of the day specified by Cabinet Order within a period not exceeding one year from the date of promulgation.

Supplementary Provisions [Act No.11 of May 24, 2019] [Extract]

(Effective Date)

Article 1 This Act comes into effect as of April 1, 2020; provided, however, that the amending provisions in Article 2 that add one Article to the Supplementary Provisions of the National University Corporation Act; in Article 4, the provisions amending Article 3 of the National Institution for Academic Degrees and Quality Enhancement of Higher Education Act, and amending Article 16, paragraph (1) of the same Act; and the provisions of the following Article, and the provisions of Article 4, paragraph (3) and paragraph (4), Article 9, Article 11 and Article 12 of the Supplementary Provisions come into effect as of the date of promulgation.

Supplementary Provisions [Act No.35 of May19, 2021] [Extract]

(Effective Date)

Article 1 This Act comes into effect as of September 1, 2021.

Supplementary Provisions [Act No.36 of May19, 2021] [Extract]

(Effective Date)

Article 1 This Act comes into effect as of September 1, 2021; provided, however, that the provisions of Article 60 of the Supplementary Provisions come into effect as of the date of promulgation.

(Transitional Measures Concerning Dispositions)

Article 57 (1) After this Act comes into effect, beyond what is otherwise provided for in laws and regulations, any dispositions such as authorizations or other acts which a former national government organ granted or made before this Act comes into effect pursuant to the provisions of one of the relevant laws before amendment by this Act (including orders based on them; referred to below as "former laws and regulations " in this Article and the following Article) are deemed to be dispositions such as authorizations or other acts which a corresponding national government organ granted or made pursuant to the corresponding provisions of the relevant Act after its amendment by this Act (including orders based on them; referred to below as "new laws and regulations" in this Article and the following Article).

(2) Beyond what is otherwise provided for in laws and regulations, an application, notification or any other act that has been filed with or made to the former national government organs pursuant to the provisions of the former laws and regulations at the time of the enforcement of this Act is deemed to be an

application, notification or any other act that has been filed with or made to the corresponding national government organs pursuant to the corresponding provisions of new laws and regulations after this Act comes into effect.

(3) Beyond what is otherwise provided for in laws and regulations, if procedures such as applications or notifications are required to be made with the former national government organs pursuant to the provisions of the former laws and regulations before this Act comes into effect, but those procedures have not been made with the former national government organs before the date of enforcement of this Act, the provisions of the new laws and regulations apply after this Act comes into effect, deeming that the procedures have not been made to the corresponding national government organs pursuant to the corresponding provisions of new laws and regulations.

(Transitional Measures Concerning Effect of Order)

Article 58 After this Act comes into effect, the Cabinet Office Order stated in Article 7, paragraph (3) of the Act for Establishment of the Cabinet Office, or the Ministerial Order stated in Article 12, paragraph (1) of the National Government Organization Act that has been issued pursuant to the provisions of the former laws and regulations is to remain in force as the corresponding Order of the Digital Agency stated in Article 7, paragraph (3), or the Ministerial Order stated in Article 12, paragraph (1) of the National Government Organization Act that has been issued based on the corresponding provisions of the new laws and regulations, unless otherwise provided for in laws and regulations.

(Transitional Measures for Application of Penal Provisions)

Article 59 Prior laws continue to govern the applicability of penal provisions to conduct that a person engages in before this Act comes into effect.

(Delegation to Cabinet Order)

Article 60 Beyond what is provided for in Article 15, Article 16, Article 51 and the preceding three Articles of the Supplementary Provisions, transitional measures necessary for the enforcement of this Act (including transitional measures concerning penal provisions) are to be provided for by Cabinet Order.

Supplementary Provisions [Act No.68 of June17, 2022] [Extract]

(Effective Date)

(1) This Act comes into effect as of the date on which the Act Partially Amending the Penal Code and Related Acts comes into effect; provided, however, that the provisions stated in the following items come into effect as of the date

prescribed in the items:
(i) the provisions of Article 509: the date of promulgation