

*Note: This document is a tentative translation of “Common Model of Cybersecurity Measures for Government Agencies and Related Agencies” for purpose of reference and its accuracy is not guaranteed. Any entity does not accept responsibility for any disadvantage derived from the information described in the document.*

## **Common Model of Cybersecurity Measures for Government Agencies and Related Agencies**

31<sup>st</sup> August, 2016

Revised 25<sup>th</sup> July, 2018

Revised 1<sup>st</sup> April, 2019

Revised 7<sup>th</sup> July, 2021

Revised 4<sup>th</sup> July, 2023

Cybersecurity Strategic HQ Decision

Chapter 1. Purpose and Application Target (Articles 1 to 2)

Chapter 2. Basic Policy of Information Security Measures for Government Agencies and Related Agencies (Articles 3 to 14)

Chapter 3. Basic Measures of Information Security Measures for Government Agencies and Related Agencies (Articles 15 to 24)

Supplementary provisions

Chapter 1. Purpose and Application Target

(Purpose)

Article 1. The purpose of this model is to provide a common framework of measures that Agencies shall take as policy standards on the cybersecurity of national administrative organs, Incorporated Administrative Agencies, and Designated Corporations (hereinafter referred to as the “Agencies”) stipulated by Item (2), Paragraph 1, Article 26 of the Basic Act on Cybersecurity (Act No. 104 of 2014; hereinafter referred to as the “Act”) and to strengthen and enhance information security measures including cybersecurity measures of Agencies as a whole by making each Agency work for measures under its own responsibility.

(Application Target)

Article 2. The organizations that are the application target of this model shall include those listed in the following items.

(a) National administrative organs: Agencies of the Cabinet based on rule of law or relevant agencies of the Cabinet, the Imperial Household Agency, agencies regulated by Paragraph 1 or 2, Article 49 of the Cabinet Office Establishment Act (Act No. 89 of 1999), agencies regulated by Paragraph 2, Article 3 of the National Government Organization Act (Act No. 120 of 1948) or agencies placed under them.

(b) Incorporated Administrative Agencies: Corporations regulated by Paragraph 1, Article 2 of the General Rules for Incorporated Administrative Agencies (Act No. 103 of 2009)

(c) Designated Corporations: Designated Corporations regulated in Article 13 of the Act

2. Persons who are the application target of this model are national public servants engaged in administrative affairs in national administrative organs, executives of Incorporated Administrative Agencies and Designated Corporations engaged in the work of said organizations, and other people serving under the supervision of Agencies, all of whom handle the information that is defined by the next paragraph (hereinafter referred to as “employees”).

3. Information that is the application target of this model is the information recorded in the system provided for information process or communication purpose (hereinafter referred to as “information system”) or in external electronic or magnetic recording medium (including information described on a paper outputted from the said system or information described on a paper inputted into information system) and the information relating to design or operation management of information system, both of which are officially handled by employees.

## Chapter 2. Basic Policy of Information Security Measures for Government Agencies and Related Agencies

(Management System)

Article 3. Agency shall establish organization and system to implement information security measures.

2. Agency shall designate chief information security officer.

3. The chief information security officer shall organize information security committee with function of discussing Agency’s own standards (it is the standards of information security measures to ensure information security of information system and information of Agency’s own. The same shall apply hereinafter) and assign a chairperson and members of the committee.

4. The chief information security officer directs and is responsible for tasks associated with

information security measures at Agency stipulated by this model.

5. The chief information security officer can delegate their own responsible tasks defined by the Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies; (hereinafter referred to as “the Common Standards”) that is separately stipulated to a responsible person defined by the Common Standards.

(Asset Management)

Article 4. Agency shall prepare document and inventory of competent information systems to understand the status of assets of Agencies.

(Risk Evaluation and Measures)

Article 5. Agency shall analyze a possibility of threat occurrence relating to retained information and used information system and loss at the time of threat existence, evaluate risk and take necessary information security measures by taking into consideration result of self-assessment defined by Article 11, result of information security audit defined by Article 12 and result of audit implemented by the cybersecurity strategic HQ based on Law in light of purpose of its own agency.

(Information Security Documents)

Article 6. Agency shall stipulate Agency’s basic policy (it is the basic policy of its own information security measures. The same shall apply hereinafter) and Agency’s own standards in light of characteristics of its own agency. Agency can decide the name of Agency’s basic policy and Agency’s own standards (hereinafter referred to as “Agency’s policy”) by themselves.

2. Agency’s basic policy shall provide a basic idea on information security including purpose of information security measures and target scopes to ensure information security.
3. The standards shall be stipulated to comply with the Common Standards and to enable information security measures that are the same as or higher than them.

(Promotion Plan of Measures)

Article 7. The chief information security officer shall establish the plan (hereinafter referred to as “promotion plan of measures”) to systematically and continuously implement and comprehensively promote information security measures in aligning with evaluation results of Article 5.

2. Agency shall implement information security measures based on promotion plan of measure.

(Exceptional Actions)

Article 8. Agency shall decide the procedure and employees in charge for request, examination and approval required for applying exceptional actions for implementation of information security measures provided by Agency's policy.

(Education)

Article 9. Agency shall be in charge of education for information security so that employees can implement information security measures defined by the Agency's policy with awareness.

(Handling Information Security Incident)

Article 10. Agency shall establish an appropriate system, decide necessary actions and implement them to address information security incidents.

2. Employees who recognize any possibility of information security incident shall report to the points of contact that is provided by Agency's policy.
3. Responsible person who are defined by Agency's policy shall take necessary actions when an information security incident is reported or recognized.

(Self-check)

Article 11. Agency shall conduct self-check for information security measures.

(Information Security Audit)

Article 12. Agency shall conduct information security audits to confirm whether Agency's own standards comply with this model and Common Standards and whether the actual operations comply with Agency's own standards.

(Review of Measures)

Article 13. Agency shall review information security measures when there is any change in the evaluation of the Article 5.

2. Agency shall evaluate and review Agency's policy by considering the evaluation result of the Article 5.
3. The chief information security officer shall evaluate the operation of information security measures, self-check, information security audit and the audit implemented by the cybersecurity strategic HQ based on Law and review the promotion plan of measures by considering any critical changes on information security.

(Incorporated Administrative Agencies and Designated Corporations)

Article 14. National administrative organs shall require that the Incorporated Administrative Agencies and Designated Corporations under their control refer to the organ's own policies when said agencies and corporations establish policies.

2. Incorporated Administrative Agencies and Designated Corporations shall comply with the requirements from the previous paragraph and it shall be reflected in its own policies as needed.
3. The competent minister in charge of Incorporated Administrative Agencies includes an aim of taking information security measures in mid-term objective of the item indicated by the rule of Paragraph 1, Article 29 of the Act on General Rules for Incorporated Administrative Agencies (Act No. 103 of 1999), mid and long-term objectives of the item indicated by the rule of item (1), Paragraph 4 of Article 35, or in annual objective of the item indicated by the item (1), Paragraph 9 of Article 35, according to policies established based on the Common Standards Group. The national administrative organ overseeing Designated Corporations makes the necessary recommendations on information security measures for the designated corporations in question based on the individual governing laws.
4. The competent minister in charge of Incorporated Administrative Agencies also evaluates the implementation status of information security measures and publishes the evaluation result when operations' actual performance is assessed based on the Act on General Rule of Incorporated Administrative Agencies. The national administrative organ in charge of Designated Corporations evaluates the implementation status of information security measures for the designated corporations in question based on the individual governing laws.

### Chapter 3. Basic Measures of Information Security Measures for Government Agencies and Related Agencies

(Classification of Information)

Article 15. Agency shall determine the classification of information to handle with confidentiality, integrity and availability points of view.

2. Agency shall indicate the applied classification of information that is defined by the previous paragraph by labeling etc. when information is provided, carried and sent across the Agencies.

(Handling Restriction on Information)

Article 16. Agency shall stipulate handling restrictions according to classifications of information.

2. Agency shall provide the handling restriction that is defined by the previous paragraph on the

information to be handled.

3. Agency shall indicate the handling restriction of information when information is provided, carried and sent across the Agencies.

(Information Lifecycle Management)

Article 17. Agency shall provide necessary actions and implement them in order not to impair necessary handling in accordance with classifications of information and handling restrictions in each stage of creating, obtaining, using, saving, providing, carrying, sending and deleting information.

(Information Handling Area)

Article 18. Agency shall appropriately define the area scope in which measures need to be implemented for the facility and environment, which is under management of its own organization such as government offices managed by them, facilities borrowed by the organization other than own organizations and so forth, decide the measures specific to the characteristics and implement them.

(Outsourcing)

Article 19. Agency shall specify necessary actions and implement them when the task to handle Agency's information is outsourced.

2. When outsourcing task involving disclosure of confidential information, implementation of necessary information security measures shall be the criteria to select outsourcing parties including countermeasures against information leakage and management so that unintended change can't be made to the information systems and Agencies shall include it in the specification content.
3. Agency shall define and implement the measures to ensure information security when it uses cloud services.
4. Agency shall establish the selection criteria including appropriate handling to supply chain risks such as management is in place to prevent unauthorized changes during the development of devices.

(Ensuring Information Security for Overall Information System Lifecycle)

Article 20. Agency shall stipulate actions to ensure information security in each stage to plan, procure/construct, operate/maintain, renew/dispose and review competent information systems and implement them.

(Operational Continuity Plan of Information System)

Article 21. When preparing the plan for continuously operating of competent information system, Agency shall ensure consistency with business continuity plans, policies, and maintain and operate it.

(Use of Information System)

Article 22. When an information system is used, Agency shall stipulate necessary actions that need to be implemented by employees and implement them to ensure information security.

(Entrustment to the Common Standards)

Article 23. Common Standards stipulate the requirements needed for the implementation of this model other than the provisions defined by this model.

(Formulation)

Article 24. This code is drafted by the Cabinet Secretariat's National center of Incident readiness and Strategy for Cybersecurity and decided by the Cyber Security Strategic Headquarters after the Cybersecurity Measures Promotion Committee (decided by the Chair of Cyber Security Strategic Headquarters on February 10, 2015).

Supplementary provisions

Common Model of Information Security Measures for Government Agencies (Information Security Policy Council decision on 21<sup>st</sup> April 2011) and the Guidance on Operations of Cybersecurity Measures of Government Agencies and Related Agencies (Cyber Security Strategic Headquarters decision on 31<sup>st</sup> August 2016) are abolished.