Note: This document is a tentative translation of "Common Model of Information Security Measures for Government 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 Information Security Measures for Government Agencies

31st August, 2016
Cybersecurity Strategic HQ Decision

Chapter 1. Purpose and Application Target

(Purpose)

Article 1. The purpose of this model is to provide a common framework of measures that government agencies shall take as policy standards on the cybersecurity of national administrative organs stipulated by item (2) of paragraph 1 of article 25 of the Basic Act on Cybersecurity (Act No. 104 in 2014. hereinafter referred to as the "Act") and to strengthen and enhance information security measures including cybersecurity measures of the whole government agencies by making each government agency work for measures with its own responsibility.

(Application Target)

Article 2. Government agencies that are the application target of this model are agencies of Cabinet based on rule of law or relevant agencies of the Cabinet, the Imperial Household Agency, agencies regulated by paragraph 1 or 2 of article 49 of the Cabinet Office Establishment Act (Act No. 89 in 1999), agencies regulated by paragraph 2 of article 3 of National Government Organization Act (Act No. 120 in 1948) or agencies placed under them

(hereinafter referred to as “government agencies” or “government agency” when it means a single organization).

2. Persons who are the application target of this model are national public servants engaged in administrative affairs in government agency and other persons serving in the instruction of government agency, both 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 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

(Risk Evaluation and Measures)

Article 3. Government 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 10, result of information security audit defined by article 11 and result of audit implemented by the cybersecurity strategic HQ based on Law in light of purpose of its own agency.

2. Government agency shall review information security measures when there is any change in the evaluation of the previous paragraph.

(Information Security Document of Government agencies)

Article 4. Government agency shall stipulate government agency’s basic policy (it is the basic policy of its own information security measures. The same shall apply hereinafter) and government agency’s own standards (it is the standards of information security measures to ensure information security of information system and information of government agency’s own. The same shall apply hereinafter) in light of characteristics of its own agency. Government agency can decide the name of government agency’s basic policy and government agency’s own standards (hereinafter referred to as “government agency’s policy”) by themselves.

2. Government 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. Government agency's own standards shall be stipulated to enable information security measures that are same as or higher than the Common Standards for Information Security Measures for Government Agencies that are separately defined (it is hereinafter referred to as "Common Standards").
4. Government agency shall evaluate and review government agency's policy by considering the evaluation result of the paragraph 1 of the previous article.

Chapter 3. Basic Measures of Information Security Measures for Government Agencies

(Management System)

Article 5. Government agency shall establish organization and system to implement information security measures.
2. Government agency shall designate chief information security officer.
3. The chief information security officer shall organize information security committee with function of discussing government agency's own standards 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 government agency provided by this model.
5. The chief information security officer can delegate their own responsible tasks defined by the Common Standards to a responsible person defined by the Common Standards.

(Promotion Plan of Measures)

Article 6. The chief information security officer shall establish the plan (hereinafter referred to as "promotion plan of measures") to comprehensively promote information security measures in aligning with evaluation results of paragraph 1 of article 3.
2. Government agency shall implement information security measures based on promotion plan of measure.
3. The chief information security officer shall evaluate implementation status of the previous paragraph and review the promotion plan of measures by considering any critical changes on information security.

(Exceptional Actions)

Article 7. Government 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 government agency's policy.

(Education)

Article 8. Government agency shall be in charge of education for information security so that employees can implement information security measures defined by the government agency's policy with awareness.

(Handling Information Security Incident)

Article 9. Government agency shall establish an appropriate system, decide necessary actions and implement them to address information security incidents (information security incident in JIS Q 27000:2014. The same shall apply hereinafter).

2. Employees who recognize any possibility of information security incident shall report to the points of contact that is provided by government agency's policy.

3. Responsible person who are defined by government agency's policy shall take necessary actions when an information security incident is reported or recognized.

(Self-check)

Article 10. Government agency shall conduct self-check for information security measures.

(Audit)

Article 11. Government agency shall conduct information security audits to confirm whether government agency's own standards comply with this model and Common Standards and whether the actual operations comply with government agency's own standards.

(Classification of Information)

Article 12. Government agency shall determine the classification of information to handle with confidentiality, integrity and availability points of view.

2. Government 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 government agencies.

(Handling Restriction on Information)

Article 13. Government agency shall stipulate handling restrictions according to classifications of information.

2. Government agency shall provide the handling restriction that is defined by the previous paragraph on the information to be handled.

3. Government agency shall indicate the handling restriction of information when information is provided, carried and sent across the government agencies.

(Information Lifecycle Management)

Article 14. Government 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 15. Government 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 16. Government agency shall specify necessary actions and implement them when information processing task is outsourced.

2. When outsourcing task (excluding using external service on general terms and conditions), 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 government agencies shall include it in the specification content.
3. Government agency shall not handle confidential information by using the external service on general terms and conditions.
4. In order to procure safe devices, government agency shall establish the selection criteria including appropriate handling to supply chain risks that countermeasures are not provided against known vulnerability, insecure technology is used, malware is embedded and so forth.

(Preparation of Document and Ledger on Information System)

Article 17. Government agency shall prepare document and inventory of competent information systems.

(Ensuring Information Security for Overall Information System Lifecycle)

Article 18. Government 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 19. Government agency shall consider information security measures in emergency cases when preparing the plan for continuously operating of competent information system (it is hereinafter referred to as "operational continuity plan").

2. When training is provided for operational continuity plan, government agency shall confirm whether it is possible to operate information security measures in emergency cases or not.

(Encryption and Digital Signature)

Article 20. Government agency shall stipulate necessary actions for use of encryption and digital signature in their own organizations and implement them.

(Provision of Administrative Service Using the Internet)

Article 21. When an administrative service is provided by using the internet, government agency shall stipulate necessary actions to prevent any conduct that leads lowering information security level of user devices and implement them.

(Use of Information System)

Article 22. When an information system is used, government 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 a necessary detailed rules including procedures of implementing this model and its execution other than the provisions defined by this model.

Supplementary provisions

Common Model of Information Security Measures for Government Agencies (Information Security Policy Council decision on 21st April 2011) is abolished.