Guidelines for Formulation and Implementation of Standards for Information Security Measures for the Central Government Computer Systems

15 September, 2005
Decision by the Information Security Policy Council

Contents

1. Position of the Guidelines and Others

1-1. Position of the Guidelines

The purposes of these guidelines are to provide necessary factors to formulate uniform standards of information security measures to be implemented by government agencies and to implement these measures, based on Policy for Enhancement of Information Security Measures for the Central Government Computer Systems (decision made on 15 September, 2005 by the Information Security Policy Council), in order to reinforce and improve information security measures in government agencies.

1-2. Definitions of Major Terms Used in the Guidelines

The terms used in these guidelines are defined as follows:

(1) **Government agencies** – refer to Cabinet Secretariat, Cabinet Legislation Bureau, National Personnel Authority, Cabinet Office, Imperial Household Agency, Fair Trade Commission, National Public Safety Commission (National Police Agency), Defense Agency, Financial Service

Agency, Ministry of Internal Affairs and Communication, Ministry of Justice, Ministry of Foreign Affairs, Ministry of Finance, Ministry of Education, Culture, Sports, Science and Technology, Ministry of Health, Labor and Welfare, Ministry of Agriculture, Forestry and Fishery, Ministry of Economy, Trade and Industry, Ministry of Land, Infrastructure and Transport and Ministry of Environment.

(2) **Information security policies** – refer to the document that comprehensively describes policies, measures and systems adopted by an organization to ensure its information security.

(3) **Standards for Measures** – refer to the uniform standards of the whole government that define the minimum information security measures to be carried out as part of cross-sectoral efforts to promote consistency and integrity of information security measures in government agencies.

(4) **Basic policies of government agency** – refer to basic policies of information security measures in a government agency.

(5) **Standards for measures implemented by government agency** – refer to the information security standards that are applicable to all information assets in a government agency complying with the Standards for Measures.

(6) **Standards of government agency** – refer to the information security policies formulated by each government agency that comprise of the basic policies of government agency and standards for measures implemented by government agency.

(7) **Operation procedures** – refer to the document explaining what procedures government agency is to follow in implementing measures stipulated in the standards in operating specific information systems.

(8) **Set of individual manuals of the Standards for Measures** – is a collective term of the manuals used as reference by each government agency for forming operation procedures based on standards for government agency, and is in principle formulated by the National Information Security Center (hereinafter referred to as the “NISC”).

2. Nature of Information Security Measures in Government Agencies

2-1 Promotion of Information Security Measures in Each Government Agency

Each government agency in principle shall be responsible for information assets that are under its control to ensure information security and shall take information security measures suitable for its operations and information systems features.

Based on this principle, in order to appropriately promote information security, each government agency shall form a unified concept and shall compile standards and operation procedures for the agency in a written form so that the decision for handling information assets of the agency will not be guided by personal discretion, and shall be consigned proper application of concerned provisions.

Furthermore, when formulating the standards of measures implemented by government agency, each government agency must make sure that the document does not contain deficiencies in the contents, taking into account the Standards for Measures.

The NISC shall formulate a set of individual manuals of the Standards for Measures in cooperation with concerned agencies to contribute to preventing deficiencies in the contents and efficient formulation of operation procedures in each government agency.

2-2. Inspection and Evaluation of Implementation of Measures conducted by the NISC

Evaluations of the information security measures shall in principle be carried out under the responsibility of each government agency; however, evaluations should be based on judgment criteria that would enable objective comparisons, so that the government can effectively and efficiently perform evaluations, thus upgrading the level of information security of the whole government.

At the same time, it is important that information security measures are not transitory, but something that allow efforts to be continuously carried out without delay.

From above, in line with the Standards for Measures, the NISC shall conduct inspections and evaluations on the process of formulating the standards of each government agency, operation procedures, process of developing other information related rules and implementation of measures, from a comprehensive, objective and integrated perspective and on a periodic and as-needed basis, and shall promote improvement of measures whenever the need arises.

Meanwhile, each government agency shall cooperate with the NISC's inspections and evaluations.

3. Information Security Measures Based on the Standards of Government Agency

3-1. Points to Remember about the Standards of Government Agency

(1) Clarification of what basic policies of the information security in an agency shall ensure.

Together with the need to identify and protect information assets that are threatened (for example, wiretapping, intrusion, falsification, destruction, theft, leakage, denial of service attack, etc.), threats of each information asset will be analyzed while giving due consideration to the importance of assets and usage environment, etc. In doing so, information assets to be protected and the level of information security required by the relevant information system are the basis for considering information security measures.

Furthermore, it is first necessary to establish a system for implementing information security measures. With sufficient awareness of the fact that one information system involves various people, such as those who operate and manage information systems, users, and those who are responsible for the information security measures of the system, it is then necessary to clarify the scope of power and responsibility of the people to facilitate appropriate implementation of security measures as an organization.

(2) Continuous efforts in line with the implementation cycle of information security measures based on the standards of government agency

For each government agency, information security measures should not be transitory when standards are formulated and completed; instead, they become meaningful only when continuous efforts are made after formulating the standards. Therefore, what is necessary is continuous effort in line with the implementation cycle of information security measures, as shown in Figure 1. Thus, in order to appropriately maintain the level of information security, it is important to introduce and appropriately adopt the standards of government agency, accurately evaluate its effectiveness and review the standards when necessary.

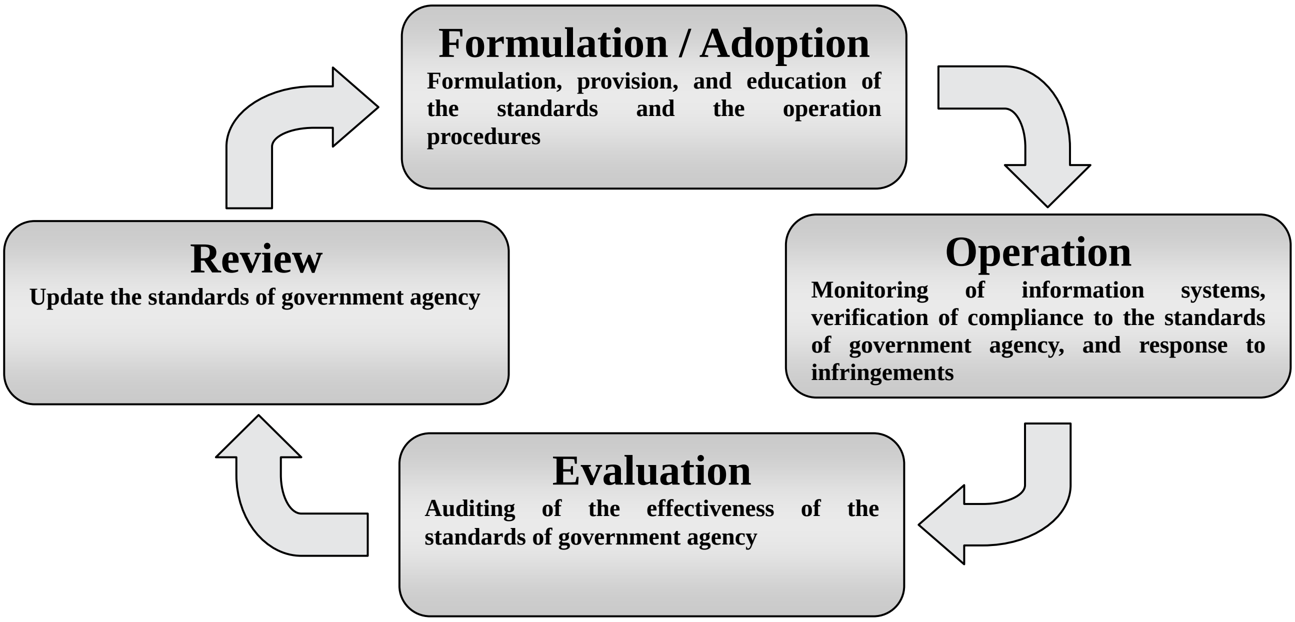
Formulation / Adoption
Formulation, provision, and education of the standards and the operation procedures
Operation
Monitoring of information systems, verification of compliance to the standards of government agency, and response to infringements
Evaluation
Auditing of the effectiveness of the standards of government agency
Review
Update the standards of government agency

Figure 1: Implementation Cycle of Information Security Measures based on the Standards of Government

3-2. Formulation

Principles of items to be stipulated in the Standards of Government Agency

(1) Outline of formulation procedures

The formulation of the standards of government agency follows procedures shown in Figure 2: specifically, (a) establish a framework and system for the formulation; (b) formulate the basic policies of government agency under the established framework and system; (c) conduct risk analysis; (d) formulate standards for measures implemented by government agency based on risk analysis; and (e) unify and document the concept within each government agency.

Furthermore, (f) each government agency shall formulate operation procedures in accordance with the standards of government agency.

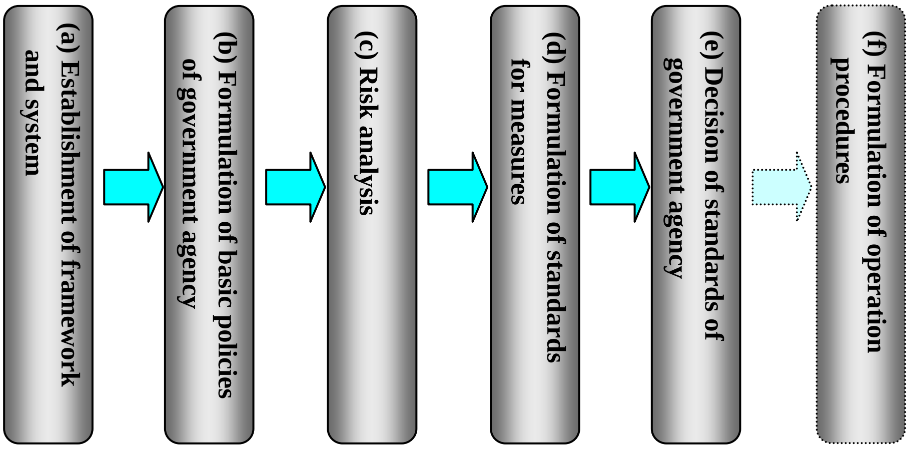
(a) Establishment of framework and system
(b) Formulation of basic policies of government agency
(c) Risk analysis
(d) Formulation of standards for measures
(e) Decision of standards of government agency
(f) Formulation of operation procedures

Figure 2: Outline of Policies Formulation Procedures

Much care is required to handle relevant documents, such as standards for measures implemented by government agency, operation procedures, and results of risk analysis, since they contain considerable information that can provide clues for attacks.

(2) Framework and system for formulation

The information security of each government agency must be ensured on its own responsibility, and cross-sectoral efforts within the agency are required. Therefore, the formulation of the standards of government agency requires involvement of executive officers. In order to clarify the locus of responsibility for the formulation and implementation of the standards of government agency and overall information security in each government agency, a chief information security officer shall be appointed, who shall then designate officers in charge of implementation on an as-needed basis. In order to formulate effective and practical standards of government agency, it is necessary to secure not only the division in charge of operating information systems, but also the cross-sectoral discussion framework, involving personnel and accounting divisions. It is also necessary to establish a framework, such as a committee, comprising not only concerned staffs but also executive officers (hereinafter referred to as “information security committee”). To that end, each government agency shall identify objectives, power, name, operations, and members of the information security committee in the standards of government agency.

(3) Formulation of the basic policies of government agency

Each government agency shall formulate its own basic policies on information security to specify basic principles for information security, including objectives and the scope of information security measures, in order to ensure information security required by information assets.

Since basic policies determine the basic direction of information security, it is necessary to bear in mind that they are not subject to frequent changes.

(4) Risk analysis

Risk analysis is to identify information assets to be protected and assess the risks associated with them. As Figure 3 shows, it involves (a) examination of information assets, (b) classification of information assets in order of priority, (c) examination of threats on information assets, and (d) analysis of the likelihood of the threat occurring and the magnitude of damage. From these, (e) the level of information security required by the relevant information asset is determined. In order to implement adequate information security measures, risk analysis must be carried out in a reliable manner so that it would lead to effective information security measures, since it is important to set up appropriate information security levels for protecting each information asset.

When there are changes in information assets or changes in threats on information assets, a risk analysis on relevant information assets shall be conducted. Based on the results, the standards of government agency shall be reviewed if necessary. At the time of periodical evaluation and review of the standards, risks may be reanalyzed when the needs arise. A prompt response is required if urgency is indicated in the risk analysis for issues of information security measures.

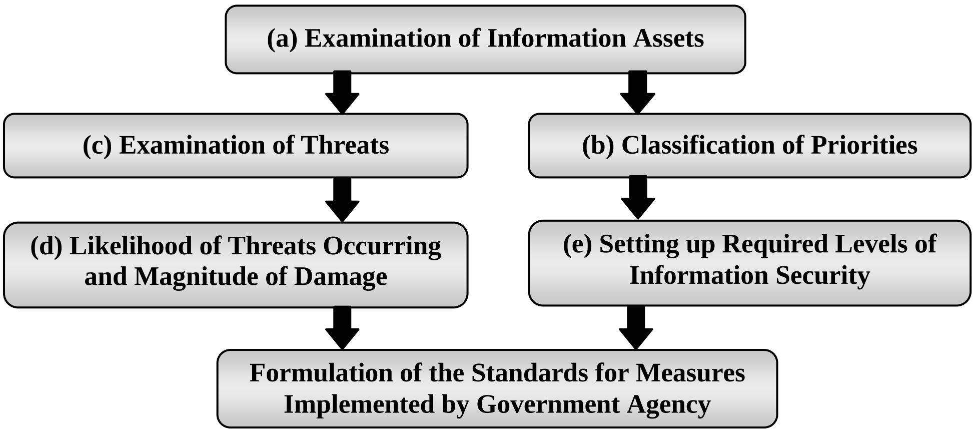
(a) Examination of Information Assets
(c) Examination of Threats
(b) Classification of Priorities
(d) Likelihood of Threats Occurring and Magnitude of Damage
(e) Setting up Required Levels of Information Security
Formulation of the Standards for Measures Implemented by Government Agency

Figure 3: Procedures of Risk Analysis

(5) Formulation of standards for measures implemented by government agency

Standards for measures implemented by government agency shall be formulated on each information security measure for individual information assets based on results of risk analysis.

In principle, the Standards for Measures shall be formulated in such a way as to encompass information security measures required for each government agency. This is effective in simplifying the process of risk analysis and selection measures requiring specialized knowledge by complying them with the Standards for Measures.

Thus, when formulating the standards for measures implemented by government agency, each government agency shall comply with the Standards for Measures in accordance with the characteristics of each information asset.

(6) Decision of standards of government agency

The prepared draft of standards of government agency is subject to validity assessment based on the evaluations of specialists in information security and the opinions of related divisions, etc.

The standards of government agencies describe the procedures required to reflect the opinions of related divisions, and also stipulate that each government agency should obtain consensus as a whole body before the standards are decided.

3-3. Adoption

(1) Formulation of operation procedures

Operation procedures describe what procedures are to be followed in specific information systems and operations to perform what is specified in the standards of government agency. The operation procedures are deemed to be a manual for every person to adhere to the standards as to what and how to do or what not to do, in order to ensure information security depending on handled information, the implemented operations and the information systems in use, etc. Thus, each government agency shall formulate appropriate operation procedures by individual information systems and operations in accordance with the operational environment, while referring to the set of individual manuals of the Standards for Measures and revise them as needed.

Since it is effective to formulate operation procedures for specific purposes based on standards for measures implemented by government agency and to flexibly perform an implementation cycle, such as evaluation and review, etc., it is necessary to allow information system managers to formulate, update and abolish them without the information security commissions' permission.

(2) Dissemination of standards of government agency and operation procedures

In order to achieve information security measures, it is necessary to inform all concerned personnel about standards of government agency and operation procedures.

It is also necessary to inform contractors in advance and make them agree to comply strictly with the standards.

3-4. Operation

In order to fully adhere to the standards of government agency, it is necessary to establish a framework and system for that purpose and confirm whether the measures are appropriately aligned with the standards.

It is also essential to formulate emergency response plans, conduct drills based on the plans, and appropriately evaluate and review the plans in preparation for possible incidents of information security infringements.

3-5. Evaluation (Auditing)

Each government agency needs to implement information security measures in such a way as to be in line with the standards from an objective point of view. Thus, it is necessary to conduct auditing and evaluations. In doing so, it is essential to perform comprehensive auditing and evaluations, not being confined to the security of technical, physical and personal information pertaining to information systems, but also encompassing security of the related information itself.

When conducting auditing using outside expertise, it is necessary to cautiously verify credibility and select auditors while considering the risk of disclosing information systems’ weaknesses to concerned parties.

3-6. Review

With respect to updating the standards of government agency, since sufficient consideration of the difference between the standards of government agency and reality is necessary for updating the standards, it is desirable to hold hearings from concerned departments and understand the current situation. Furthermore, when updating the standards of government agency, it is important to bring them in line with actual state, by reviewing risk analysis whenever it is deemed necessary. It is also important to make daily efforts to collect information on new attacks and use it to update the standards.

Once new clauses are stipulated in the standards of government agency are set, thorough dissemination is necessary.

When the Standards for Measures has been revised based on results of inspection and evaluations on information security in government agencies, each government agency is required to review its own standards accordingly.

4. Efforts for Standards for Measures

4-1. Formulation and Implementation of the Standards for Measures

A draft of the Standards for Measures shall be formulated by the NISC. The Standards for Measures shall in principle be reviewed annually and revised on an as-needed basis, based on the occurrence of new threats and results of implementation by each government agency.

Due consideration should be given to the following points when formulating the Standards for Measures.

(1) The Standards for Measures shall in principle contain all information security measures required by each government agency.

(2) The responsibility and implementation systems, measures shall be designed in an applicable manner based on the situation of each government agency, so that each government can comply with the Standards for Measures without much difficulty.

(3) When formulating the Standards for Measures, necessary consideration shall be given to consistency with international standards and others.

4-2. Formulation and Provision of a Set of Individual Manuals for the Application of the Standards for Measures

The NISC shall formulate a set of individual manuals for the Standards for Measures in cooperation with government agencies as reference for such documents as operation procedures, regulations, manuals, etc., which are formulated when adopting the standards of government agency.

The set of manuals shall be formulated or revised based on the occurrence of new threats and results of implementation in each agency in the order of importance and urgency and be promulgated to all government agencies.

Supplementary Provision: Guidelines for the Formulation of Information Security Policies (decision made on 18 July, 2000 by the Information Security Promotion Council) shall be abolished.