Standards for Information Security Measures for the Central Government Computer Systems

(Fourth Edition)

February 3, 2009

Established by the Information Security Policy Council

Table of Contents

Volume 1 Basics

Chapter 1.1 General

1.1.1.1 Positioning of Standards for Measures

⑴ Positioning of these Standards for Measures on enhancement of Information Security Measures for the Central Government Computer Systems

In principle, each government agency must take its own responsibility for measures to ensure information security. However, it is necessary to formulate a unified framework to provide guidance on such measures and raise the level of information security in unison based on the “Policy for Enhancement of Information Security Measures for the Central Government Computer Systems (decision by the Information Security Council on Sep 15, 2005)” in order to enhance the information security measures across the board for government agencies. These Standards for Measures will provide the standards for the measures that each government agency should take to achieve information security and the measures to further raise the level of information security in the unified framework.

⑵ Revising the Standards for Measures

It is important to grasp the changes in circumstances appropriately and review the information security measures in order to maintain an appropriate level of information security. It is possible that what and how to add to or revise these Standards for Measures will be known after each government agency uses these to formulate its own standards of government agency and operation procedures in view of its characteristics and to evaluate its information security measures. Also, it is possible that revising information security measures in these Standards for Measures is required to be made in accordance with development of information technologies.

With this in mind, these Standards for Measures shall be reviewed periodically and added to or expanded in order to maintain their applicability in the future. Each government agency must update its standards of government agency appropriately when these Standards for Measures are revised.

⑶ Complying with laws and regulations

How information and information systems should be handled is also formulated in laws and regulations (hereinafter referred to as “relevant laws and regulations”). So, besides these Standards for Measures, such relevant laws and regulations must be conformed to when information security measures are taken. Because these relevant laws and regulations should be conformed to regardless of the information security measures formulated, these Standards for Measures do not specifically mention them. Also, the existing government decisions on information security measures must be conformed to as well.

1.1.1.2 How to use Standards for Measures

⑴ Relationship of these Standards for Measures and Standards of Government Agency

These Standards for Measures provide the standards for the measures that each government agency should take to achieve information security and the measures to further raise the level of information security. Each government agency shall review the current information security rules as needed in order to achieve higher information security than provided for in these Standards for Measures. Therefore, each government agency must not leave its standards of government agency unchanged based on these Standards for Measures without rational reasons. Each government agency must determine what to define in its standards of government agency in view of its characteristics and update it appropriately by referring to these Standards for Measures directly, and incorporating the relevant contents of these Standards for Measures with or without modifications (structure, expressions.)

⑵ Scope

These Standards for Measures shall be applied as follows:

(a) These Standards for Measures are formulated for the purpose of protecting "information." "Information" in these Standards for Measures means information that is stored in the information systems, stored in the electronic storage media outside the information systems, and written or printed on the documents for information systems. Unfinished documents are also included within this scope. Information written or printed on the documents can be electronically recorded information that is described in the documents (containing information input into the information systems or information output from the information systems) and specifications of information systems.

(b) The Standards for Measures shall be applied to the employees. "Employees" means government officials and those who are under supervision of the municipal governments who handle information and information systems which managed by each municipal governments.

(c) In the Standards for Measures, "government agency" means Cabinet Secretariat, Cabinet Legislation Bureau, National Personnel Authority, Cabinet Office, Imperial Household Agency, Japan Fair Trade Commission, National Public Safety Commission (National Police Agency), Financial Services Agency, Ministry of Internal Affairs and Communications, 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 Fisheries, Ministry of Economy, Trade and Industry, Ministry of Land, Infrastructure, Transport, and Ministry of the Environment and Ministry of Defense.

(3) Structure

The Standards for Measures is comprised of four levels – volume, chapter, section and item.

The Standards for Measures categorizes information security measures into the chapters of "Basics" and "Information System". Basics defines compliances such as maintenance of organization and system to promote information security measures as the entire organization, information security measures at each phase of the information life cycle and regulations related to the information system. "Information System" specifies technical matters including items for compliance including security requirements for the information systems, which would be revised frequently.

"Basics" includes "General", "Building the Organization and System," "Measures for Information," "Measures for information processing" and "Basic Measures for Information systems". "Information Systems" includes sections "Measures based on the Clarified Information Security Requirements". "Measures for Components of Information Systems," and "Measures for Individual Considerations," and arranges the contents into sections, then itemizes standards for the measures.

Each section further itemizes measures, which is followed by the standards for measures as below.

(a) “Building the Organization and System” describes organizational issues such as operation systems, assessment procedure, violation, and exceptional measures and also clarifies operational authority and responsibilities of employees for the whole organization can take information security measures.

(b) “Measures for Information” defines requirements for daily tasks, focusing on the information lifecycle – creation, use, storage, transfer, provision, and deletion of information. It also specifies the measures that employees **must** always take at each stage in terms when they execute their tasks to protect information.

(c) Measures for information processing” defines limited requirements for information processing on outside the government facility as well as information processing using information systems provided by non-government organizations.

(d) “Basic measures for information systems” defines requirements to be taken at each stage of the information system life cycle such as planning, building, operation, transfer, abolishment and review of information systems in order to properly implement requirements specified in the chapter “Information System”, as well as items to take as a rule for information securities concerning the information systems.

(e) “Measures based on Clarified Information Security Requirements” explains security functions such as access control to introduce intothe information systems, and also defines compliance requirements to prevent threats such as security holes, malware, and denial of service attacks in order to describe measures to take for the information systems.

(f) “Measures for Components of Information Systems” defines compliance requirements of the information systems from a terms of the individual characteristics and lifecycle of computers and communication lines.

(g) “Measures for Individual Consideration” defines compliance requirements for individual consideration that need specific attention in terms of information security such as new technologies to be implemented.

(4) Itemized Measures

These Standards for Measures set compliance requirements for measures each government agency should take by individual item.

(5) Setting Security Levels

The information security measures that should be taken depend on the importance of the information assets to protect or threats that exist. Also, the measures must be strong enough for the characteristics of information systems and tasks. With this in mind, these Standards for Measures set the strength level for each measure to meet compliance requirements. This level is called “the level of a measure” and is formulated as follows:

(a) “BASIC Requirements”: measures that must be taken for the information to protect and the information systems that handle such information

(b) "ENHANCED Requirements": measures that should be taken for especially important information and the information systems that handle such information if the respective government agency considers them required.

By following the above compliance requirements, each government agency shall take measures that satisfy or exceed the BASIC Requirements. Each government agency must evaluate the risks in view of the characteristics of information systems and tasks in order to select an appropriate level for each compliance requirement.

⑹ Evaluation Procedure

It is essential that information security measures are continuously feasible without delay but not transient. Therefore, each government agency must confirm that the following requirements are met based on these Standards for Measures by conducting information security auditing periodically or as need arises.

(a) The standards of government agency conform to these Standards for Measures (confirming compliance in design)

(b) Actual operations conform to the standards of government agency (confirming compliance in operation)

(c) The standards of government agency are appropriate and efficient for the risks, or not unfeasible (confirming the adequacy in design)

(d) Actual operations are appropriate and efficient for the risks (confirming the adequacy of operations).

Particularly, the most important purpose of information security auditing at each government agency is to confirm compliance in design and operation. In the case that any improvements that it believes necessary in terms of validity of design and operation are found in the course of the auditing, it is desirable to put it on a list of concerns. In these Standards for Measures, compliance requirements are formulated along with the person who should execute the tasks. So, each employee shall conduct a self-assessment of how well the measures are taken based on his or her role. It is essential for each employee to fulfill his or her role to implement information security measures and conducting self-assessment helps to operate with valid measures. To achieve this goal, each government agency shall grasp how well the measures are implemented by conducting an auditing as to whether the self-assessment is adequate and how well compliance in operation is achieved.

In principle, each government agency must take responsibility for implementing its own information security measures. However, in order to promote information security measures for government agencies across the board, it must report to the National Information Security Center about how well the measures are implemented and the results of auditing. Then, National Information Security Center will inspect and evaluate how well the information security rules for each government agency are formulated and measures are implemented based on the evaluation metrics related to these Standards for Measures periodically or as needed. The scope of applicable information systems shall be discussed and determined by the National Information Security Center and each government agency.

1.1.1.3 Classification of Information and Type of Limitation

(1) Classification and limitation

Security levels of information for administrative tasks vary depending on the purpose or use. The classification of information and type of marking are defined in order to take appropriate measures for such security levels of information security. Defined the classification of the information and type of limitation this follows.

Classification and limitation of information should be properly defined so the person who created or obtained the information would make others to recognize the security level of information and take appropriate security measures.

Classification and limitation of information enables the users of the information to further recognize the necessity of daily tasks information security measures for their regular use of it. In specific, users may recognize that information and information security measures are closely linked whenever they create or obtain information, moreover they take measures according to the classification and limitation of information.

Therefore, the employees must understand the importance to implement on a basis.

(2) Classification

The following are the definition of classifications for the three aspects: confidentiality, integrity and availability for information.

The following classifications are used as the basic requirement of the Standards for measures to comply, though each government agencies may change or add definitions as necessary. However, the employee must confirm that the classification and the compliance requirements are consistent in meaning to the Standards of Measures under the standards of measures of each government agency for change or additions of definitions. It is also required to define measures to transfer the information of change or add classification how it correlates to the classification under the Standards for Measures. For instance, the employee may add-in the description of the classification used for the Standards for Measures when they provide information to other government agencies.

(a) Classification is defined as confidentiality, integrity and availability below.

Definition of Confidentiality Classification

Classification	description of classification
Confidentiality	Confidentiality information, regarded as confidential

class-3 information	information for administrative uses.
Confidentiality class-2 information	Information for administrative uses, which would not require confidentiality but could threaten citizens’ rights or disturb operations of administrative uses.
Confidentiality class-1 information	Information other than Confidentiality class-2 information or Confidentiality class-3 information.

Note that Confidentiality class-2 and Confidentiality class-3 information’s are regarded as “CONFIDENTIAL INFORMATION”.

Definition of integrity classification

Classification	description of classification
Integrity class-2 information	Information for administrative uses (except in writing), which would not require integrity but could threaten citizens' rights or disturb properly operations of administrative uses (except minor disturbances) due to falsification, mistakes and damages**.**
Integrity class-1 information	Information other than Integrity class-2 information (except in writing)

Note that Integrity class-2 is regarded as "INTEGRITY INFORMATION".

Definition of availability classification

Classification	description of classification
Availability class-2 information	Information for administrative uses (except in writing), which would not require availability but could threaten citizens' rights or disturb properly operations of administrative uses (except minor disturbances) due to its damage, loss or unavailability to use the information.
Availability class-1 information	Information other than Integrity class-2 information (except in writing)

Note that Availability class-2 information is regarded as "AVAILABILITY INFORMATION".

Confidentiality, integrity and availability information are regarded as "INFORMATION to be PROTECTED".

(3) Type of limitation

Information is categorized into three aspects: confidentiality, integrity and availability for a basic definition of each limitation to use. "Limitation" means a restriction in handling information such as to prohibit copying, taking out, distribution, to secure encryption or other measures for proper handling of information such as disposal after reading.

(a) The types of limitation shall be specified for confidentiality, integrity, and availability. Note that some other types of limitation may be used.

1.1.1.4 Definition of Terms

- “Access control” means to restrict objects to which a subject is allowed to have access.
- “Secure area” means the inside of an office or a server room in which computers and communication equipment are located, where the measures against information security violations caused by outside hackers and disasters are implemented physically and environmentally.
- “Contractor” means companies or individuals who handle projects for part or all of information processing matters such as designing, contracting and operation of information systems.
- “Delivery personnel” means a person whose purpose is to receive or pass items to employees working in a secure area and who does not need to enter the secure area. Such exchanges of items can occur in courier services and delivery of office equipment, etc.

- “Outsourcing” means having companies or individuals outside the government agencies to handle projects for part or all of information processing matters such as designing, contracting and operation of information systems.
- “Availability” means to have a status in which a person who is allowed to access information can access the information and the related assets without being interrupted when he or she needs to do so.
- “Integrity” means to have a state in which information is not damaged, altered, or deleted.
- “Equipment, etc.” means information equipment and software.
- “Confidentiality” means a state in which only a person who is allowed access can access the information.
- “Shared identification code” means an identification code that is shared by multiple subjects. In principle, a single identification code is granted to a single subject; however, it can be shared by multiple subjects if there are any restrictions on the information system or in consideration of how they are used. Such an identification code is called a shared identification code.
- “Storage media” means media on which information is recorded or described. Storage media include paper or other tangible objects which contain information perceptible by the human senses through writing, documents and other letters and figures (hereinafter referred to as “written documents”) and records created through methods imperceptible by the human senses, such as through electronic methods, magnetic methods or others, that are

provided for information processing by computers (hereinafter referred to as “electronic storage media”). Electronic storage media include embedded electronic storage media that are built in computers and communication equipment and external electronic storage media such as an external hard drive CD-R, DVD, MO, USB memory, and flash memory.

- “Administration” means to manage the information for authentication (including identification code and authentication information) and the granting of information for permission of access control.
- “Announced security hole” means a security hole that can be known to everyone and includes announced by software or hardware manufacturers and vendors or announced by security-related organizations such as the JPCERT Coordination Center.

- “Service” means a set of functions that is composed of a single or multiple functions provided to the connected computer by an application running on a server.
- 「“Least privilege” means a function to limit the spectrum where administrative rights can be exercised to the minimum extent necessary for the administrative task.
- “Identification” means to identify the subject that accesses an information system.
- “Identification code” means a code that an information system recognizes to identify the subject. A User ID is a typical identification code.
- “Important specifications” means specifications related to an information system that are necessary for the appropriate management of the relevant information system and the missing or leakage thereof may hinder the operation of tasks of the government agency.
- “Subject” means a person who accesses the information systems or other information systems and a device. A subject is supposed to be human in principle; however, other information systems and devices can be subjects when multiple information systems and devices work in coordination.
- “Authentication” means to verify whether the subject that presents an identification code is legitimate or the one that is granted the identification code. The information system recognizes the subject as legitimate if the identification code and authentication information are presented in a correct way and authentication is successful. Though being “authenticated” means to be proved officially or by a third party, ”authentication” in these Standards for Measures does not always mean such proof.
- “Authentication information” means information that a subject presents to an information system in order to become authenticated. A password is typical authentication information.
- “Authentication information storage device” means a device that stores authentication information so that a legitimate subject can own or hold it. In the case that an authentication method based on ownership is used, the information system recognizes the subject as legitimate if it has this.

  A magnetic strip card and IC card are typical authentication information storage devices.
- “Standards of government agency” means information security standards that are

applicable to all information assets of the respective government agencies.

- “Information system” means a computer system that provides information processing and communications.
- “Information security rules” means the standards of government agency and the operation procedures that provide step-by-step instructions on how to execute the measures formulated in the standards of government agency in specific information systems and tasks.
- “Information transfer” means to transmit electronically recorded information and to transport electronic storage media and written documents that contain information outside the government agency.
- “Legal employee” means an employee who is designated to execute administrative tasks by appointment.
- “Software” means procedures and orders to operate a computer that are written in a form that computers can understand. An operating system and applications running on the operating system can be viewed as software in a broad sense.

- “Terminal” means a computer that an employee directly operates (including an operating system and connected peripheral devices) such as a PC and a PDA.
- “Communication line” means a mechanism by which multiple computers are connected to send or receive information in a prescribed communication protocol. A communication line which is established by connecting a line and communication equipment is called a physical communication line, and a communication line which is formulated over the physical communication line and can exchange information in a prescribed communication protocol is called a logical communication line.
- “Communication equipment” means a device that is located to connect the lines and used to control the information exchanged by computers via a line. Repeater hubs, switching hubs, routers, and firewalls are included.
- “Computers” means computers in general and includes operating systems, servers including connected peripheral devices, and terminals.
- “Marking” is information to indicate restrictions on how to handle the information (meaning measures to secure appropriate handling of information such as “do not copy,” “internal use only,” “do not re-distribute,” “encryption required,” and “destroy after reading,” etc.)

- “Multiple factors authentication / composite authentication” is an authentication method in which multiple factors of knowledge, ownership, and biological information are used to authenticate.
- “Outside the government agency” means outside the organization or building managed by

the government agency that legal employees belong to.

- “Communication line outside the government agency” means a logical communication line which computers that are not managed by the government agency are connected with and is used for communications between such computers regardless of what physical communication lines (wired/wireless, real/virtual, managed by the government agency/other organizations) or communication equipment are used.
- “Information processing outside the government agency” means doing information processing required to execute the administrative tasks outside the organization or building managed by the government agency. This includes offline processing as well as online processing by connecting from outside the government agency to the information systems of the government agency that legal employees belong to.
- “Information systems not supplied by the government (unsupplied information system)” means the information systems that are not the ones supplied by the government agency which legal employees belong to. These include private PCs and the information systems provided to loan employees working in the relevant government agency by the original organization.
- “Information processing using information systems not supplied by the government” means doing information processing required to execute the administrative tasks using unsupplied information systems. This includes not only using the devices directly but also using the services provided by the devices. A service here means one such as an e-mail service for private use. Transferring business e-mail messages required to execute the administrative tasks to a privately used e-mail service and vice versa are the examples.
- “Inside the government agency” means inside the organization or building managed by the government agency which legal employees belong to.
- “Communication line inside the government agency” means a logical communication line which computers that are managed by the government agency are connected with and is used for communications between such computers regardless of what physical communication lines (wired/wireless, real/virtual, managed by the government agency/other organizations) or communication equipment are used.
- “Malware” means software in general which brings a result unwanted for computer users, such as computer viruses and spyware.
- “Malware definition file” means the data which antivirus software, etc. uses to determine malware.

- “Labeling, etc.” means to put information into a state in which all persons who handle it can have a common understanding of its classification. The classification must be shown for each item of information in principle. However, this includes any measures to make a common understanding of classification of the information. For specific information systems, it is also deemed as labeling, if the rule, etc. clearly states classification of information stored in the information system and the rule is notified to all persons who use the information system.

- “Mobile PC” means a terminal that is movable as needed for business purposes regardless of terminal shape. A laptop PC that is used at a specific place is not a mobile PC.

- “Vital information” means availability class-2 information.
- “Confidential information” means confidentiality class-2 information and confidentiality class-3 information.
- “Classified information” means confidential information, critical information, and vital information.
- “Critical information” means integrity class-2 information.

- “Exceptional measures” means that an employee takes alternative measures required in order to continue executing his or her administrative tasks appropriately, or, if there is a rational reason for doing so, reports and obtains permission not to meet compliance requirements in the case that complying with the relevant information security rules is difficult.
- “Login” means an action in which a subject requests authentication. Because login is followed by authentication, validity of the subject is unknown at the login stage.
- “Logon” means the status in which the subject that has requested authentication by login is validated by the information system.

Chapter 1.2 Building the Organization and System

1.2.1 Introduction

1.2.1.1 Establishing the Organization and System

Compliance Requirements

⑴ Designating the chief information security officer

[BASIC Requirements]

(a) A chief information security officer must be designated.

(b) The chief information security officer must direct the tasks for information security measures in the respective government agency.

⑵ Designating the Information Security Council

[BASIC Requirements]

(a) The chief information security officer must establish the Information Security Council and designate a chairperson and members of the committee.

(b) The Information Security Council must compile the standards of government agencies concerning information security for approval of the chief information security officer. Note that some technical matters may be assigned to designated personnel if the chief information security officer approves in advance.

⑶ Designating the chief information security auditors

[BASIC Requirements]

(a) The chief information security officer must designate the chief information security auditors.

(b) The chief information security auditors must direct the tasks for the audit under the direction of the chief information security officer.

⑷ Designating the information security officers

[BASIC Requirements]

(a) The chief information security officer must determine the management unit to be used to implement the information security measures and designate an information security officer for each unit. The head of information security officers must be designated to give directions to the information security officers.

(b) The information security officer must give directions for the administrative tasks for information security measures in the unit he or she governs.

(c) The head of the information security officers must develop administrative procedures for employment, job termination, and job transfer that occur in implementing information security measures.

(d) The information security officer must periodically ensure that administrative procedures for employment, job termination, and job transfer that occur in implementing information security measures are followed.

(e) The chief information security officer must report the designating and changing of any information security officers to the head of information security officers.

(f) The head of information security officers must formulate a network for all information security officers.

⑸ Designating the information system security officers

[BASIC Requirements]

(a) The information system security officer must designate information system security officers for the information systems in the unit he or she manages until the planning phase of this information system project.

(b) The information system security officer must direct the administrative tasks for information security measures for the information systems he or she manages.

(c) The information security officer must report the designating and changing of any information system security officers to the head of information security officers.

(d) The head of information security officers must formulate a network for all information system security officers.

⑹ Designating the information system security administrators

[BASIC Requirements]

(a) The information system security officer must designate an information system security administrator for each unit required for the administrative tasks for the information system he or she manages.

(b) The information system security administrator must implement information security measures for the administrative tasks he or she manages.

(c) The information system security officer must report the designating and changing of any information system security administrators to the head of information security officers.

(d) The head of information security officers must formulate a network for all information system security administrators.

(7) Designating the division/office information security officers

[BASIC Requirements]

(a) The information security officer must designate a division/office information security officer for each division/office.

(b) The division/office information security officer must direct the administrative tasks for information security measures in the division/office he or she manages.

(c) The information security officer must report the designating and changing of any division/office information security officers to the head of information security officers.

(d) The head of information security officers must formulate a network for all division/office information security officers.

(8) Chief information security advisor

[BASIC Requirements]

(a) The chief information security officer must designate chief information security advisor with expertise and experiences concerning information security expert.

(b) The chief information security officer must specify the job descriptions of the chief information security advisor such as operation of information security measures.

1.2.1.2 Assignment of Roles

Compliance Requirements

(1) Defining the roles that must not be undertaken by the same person

[BASIC Requirements]

(a) In the context of the implementation of information security measures, the following roles must not be undertaken by the same employee.

(i) The applicant for approval or permission and the authority to issue the approval or permission (hereinafter referred to as “approval authority, etc.”)

(ii) The audile and the auditor

(2) Approval or permission by supervisors

[BASIC Requirements]

(a) The employee must apply for approval with the supervisor of the approval authority, etc. when it is found inappropriate for the relevant approval authority, etc. to make a decision of approval or permission (hereinafter referred to as “approval, etc.”) in the light of their official authority. In this case, when approval is obtained from the supervisor of the approval authority, etc., it is not required to obtain approval from the approval authority, etc.

(b) In the case that the employee is granted approval, etc. in the preceding case, he or she must take necessary measures in accordance with requirements for approval authority, etc.

1.2.1.3 Violation and Exceptional Measures

Compliance Requirements

(1) Handling the violations

[BASIC Requirements]

(a) The employee must report to the information security officer who is responsible for the information security rules in the case of finding any serious breach of them.

(b) The information security officer must instruct the violator or the pertinent persons to take necessary measures to maintain information security in the case of being informed of or finding any serious breach of the information security rules.

(c) The information security officer must report to the chief information security officer in the case of being informed of or finding any serious breach of the information security rules.

⑵ Exceptional measures

[BASIC Requirements]

(a) The Information Security Council must designate the person who judges whether the request for applying any exceptional measures should be allowed or denied (hereinafter referred to as "the judge") and define the judgment procedure.

(b) The employee must request for the approval for exceptional measures to the judge by following the formulated procedures. However, the employee can make this request after the fact promptly in the case that the exceptional measure is immediately needed for executing his or her tasks and the immediate taking of alternative measures that are not provided for in the information security rules or the violation of the rules are unavoidable. The employee must clarify information including the following:

(i) Requester information (name, department, contact)

(ii) Portion of information security rules which the exceptional measure is requested for (the title of rule and article, etc.)

(iii) Period for applying the exceptional measure

(iv) Description of the exceptional measure (an alternative measure, etc.)

(v) Reporting procedure for terminating the exceptional measure

(vi) Reason for requesting the exceptional measure

(c) The judge must review the request for applying an exceptional measure made by the employee in accordance with the formulated judgment procedure and approve or disapprove the request. Also, when the judge makes a decision, he or she must formulate a request process record including the following information and present it to the chief information security officer.

(i) Name of the judge (name, title, department, contact)

(ii) Request information

- Requester information (name, department, contact)
- Portion of information security rules which the exceptional measure is requested for (the title of rule and article, etc.)
- Period for applying the exceptional measure
- Description of the exceptional measure (an alternative measure, etc.)
- Reporting procedure for terminating the exceptional measure
- Reason for requesting the exceptional measure

(iii) Result

- Approved or disapproved
- Reason for approval or disapproval
- Portion of information security rules which the exceptional measure is

approved for

- Period of the approved exceptional measure
- Description of the exceptional measure (an alternative measure, etc.)
- Reporting procedure for terminating the exceptional measure

(d) The employee must report to the judge who is responsible for the exceptional measure when he or she terminates the approved exceptional measure. However, this reporting is not required if the judge decides so.

(e) The permission authority must check whether the requestor has made a report on the expiry date of the term approved for the exceptional measure. If there is no such report submitted, the permission authority will be remind for requestor to make a report and necessary actions should be taken. However, it is not limited to when reporting is not required by the authority.

(f) The chief information security officer must formulate the ledger of request process records for exceptional measures and provide this to the head of information security auditors on their request for reference purposes.

1.2.2 Operation

1.2.2.1 Education for the Information Security Measures

Compliance Requirements

⑴ Education of the information security measures

[BASIC Requirements]

(a) The head of information security officers must educate the employees about information security rules.

(b) The head of information security officers must examine educational contents on information security rules for the employees and formulate educational materials.

(c) The head of information security officers must plan and develop the plan to educate on the information security measures and organize its implementation system so that the employees can participate in at least one education program per year.

(d) The head of information security officers must plan and develop the contents and system for education on the information security measures and organize the implementation system so that any employee who starts working or transfers to another department can participate in an educational program at their new workplace within three months

(e) The head of information security officers must establish the system to manage the achievement of participation of the employees on information security measures.

(f) The head of information security officers must inform the division/office information security officer of the achievement of participation of each employee on information security measures.

(g) The division/office information security officer must advise the employee who has not participated in any educational program for information security measures. In the case that the employee does not take his or her advice, the division/office information security officer must report this to the head of information security officers.

(h) The head of information security officers must report the achievement of participation of each employee on information security measures to the chief information security officer and the Information Security Council once a year.

[ENHANCED Requirements]

(i) The head of information security officers must plan the contents for training on the information security measures for the employees, and organize the system regarding the information security rules.

⑵ Participation in the educational programs on information security measures

[BASIC Requirements]

(a) The employee must participate in at least one educational program per year on information security measures in accordance with the plan to educate on the information security measures.

(b) The employee must ask the division/office information security officer how they can participate in an educational program on information security measures at his or her new workplace when they start working or transfer to another department.

(c) The employee must report the reason to the head of information security officers through the division/office information security officer in the case that he or she cannot participate in an educational program on information security measures for any reason that he or she is not responsible for.

[ENHANCED Requirements]

(d) The employee must participate in a training program on information security measures if participating in such a training program is formulated in the policy.

1.2.2.2 Failure Handling

Compliance Requirements

(1) Preparation for Possible Failure

[BASIC Requirements]

(a) The chief information security officer must establish the framework to prevent the damage from spreading and recover the situation from the failure (including incidents and failures. This is hereinafter referred to as “failure/accidents”) in the case of any failures that can violate information security.

(b) The head of information security officers must establish the failure/accidents report procedure that the employee uses to report to the information security officer and notifies the procedure to all the employees.

(c) The head of information security officers must establish the failure/accidents handling procedure.

(d) The head of information security officers must prepare the emergency network for the information systems that are considered to be especially important for the tasks. Distribute a information will including emergency contacts and means of communication for the responsible information system security officer and the responsible information system security administrator, and message contents.

[ENHANCED Requirements]

(e) The head of information security officers must establish a point of contact to receive information about failure/accidents from outside the government agency and announce the access to the contact to parties outside the government agency.

(2) Reporting and Taking Emergency Measures on Failures/accidents

[BASIC Requirements]

(a) If the employee comes to know that any failures/accidents have occurred, he or she must notify the relevant people and report to the information security officer in accordance with the reporting procedure specified by the head of information security officers.

(b) The employee must confirm whether the failure/accident handling procedure exists and follow the procedure if possible.

(c) If any failures/accidents have occurred and no relevant failure handling procedure exists or it is unknown whether such a procedure exists, the employee must try to prevent the damage from spreading until they are instructed how to handle it. The employee must follow the instructions once it is issued.

⑶ Cause Investigation and to Prevent the Recurrence of Failures/Accidents

[BASIC Requirements]

(a) If any failures/accidents have occurred, the information security officer must investigate the cause of failure/accident, prevent the recurrence, and writing the report to the chief information security officer.

(b) If the chief information security officer receives a report of any failures/accidents from the information security officers, the report must be reviewed to take necessary measures to prevent a recurrence.

1.2.3 Evaluation

1.2.3.1 Self-assessment of the Information Security Measures

Compliance Requirements

⑴ Formulating an annual plan for self-assessment

[BASIC Requirements]

(a) The head of information security officers must formulate an annual plan for self-assessment and obtain approval from the chief information security officer.

⑵ Preparing for the self-assessment

[BASIC Requirements]

(a) The information security officer must establish the self-assessment form and procedure for each employee.

⑶ Conducting the self-assessment

[BASIC Requirements]

(a) The information security officer must instruct the employees to conduct self-assessment in accordance with the annual self-assessment plan formulated by the head of information security officers.

(b) The employee must conduct self-assessment using the self-assessment form and procedure instructed by the information security officer。

⑷ Evaluating the result of self-assessment

[BASIC Requirements]

(a) The information security officer must confirm that the employees have conducted self-assessment and evaluate the results.

(b) The head of information security officers must confirm that the information security officer has conducted self-assessment and evaluate the results.

(c) The head of information security officers must report the result of self-assessment to the chief information security officer.

⑸ Making improvements based on the self-assessment

[BASIC Requirements]

(a) The employee must make any improvements that he or she believes possible within the scope of his or her authority based on the results of self-assessment, then report this to the information security officer.

(b) The chief information security officer must evaluate the results of self-assessment as a whole, and instruct the information security officers to make improvements as needed.

1.2.3.2 Auditing the Information Security Measures

Compliance Requirements

⑴ Formulating the audit plans

[BASIC Requirements]

(a) The head of information security auditors must develop the annual plan for information security audit and obtain approval of the chief information security officer.

⑵ Instructing the information security audit

[BASIC Requirements]

(a) The chief information security officer must instruct the head of information security auditors to conduct an audit in accordance with the annual plan for information security audit.

(b) The chief information security officer must instruct the head of information security auditors to conduct audits that are not defined in the annual plan for information security audit as needed to respond to changes in information security conditions.

⑶ Formulating the detailed audit plans

[BASIC Requirements]

(a) The head of information security auditors must develop the individual audit plans in order to conduct audits in accordance with the annual plan for information security audit and the instructions for auditing according to the changes of information security conditions.

⑷ Preparation for the information security audit

[BASIC Requirements]

(a) The head of information security auditors must select and appoint a person necessary for the audit work as an information security auditor from among those who are independent from the auditee.

(b) The head of information security auditors must partly outsource the audit work to a supplier outside the government agency as needed.

⑸ Conducting for the information security audit

[BASIC Requirements]

(a) The information security auditor must conduct audits under the directions of the head of information security auditors based on the audit plan.

(b) The information security auditor must confirm that the standards of government agency comply with these Standards for Measures.

(c) The information security auditor must confirm that the procedure complies with the standards of government agency.

(d) The information security auditor must confirm that the actual operations by the auditee are in compliance with the information security rules by confirming the adequacy of self-assessment, etc.

(e) The information security auditor must document audit working papers.

(f) The head of information security auditors must formulate the audit report based on the audit working papers and submit it to the chief information security officer.

⑹ Response to the results of the information security audit

[BASIC Requirements]

(a) The chief information security officer must instruct the information security officer of the division audited to take measures against any problems indicated in the audit report.

(b) The chief information security officer must instruct the information security officers in other departments to investigate whether similar problems exist and to solve them if any if he or she believes that it is highly likely that the departments other than the auditee one pose similar challenges or problems and quick investigation is required based on the audit report.

(c) The information security officer must develop the improvement plan for the problems for which resolution is requested by the chief information security officer based on the audit report etc.

(d) The chief information security officer must evaluate the validity of existing information security rules and order a review as needed based on the results of the audit.

1.2.4 Review

1.2.4.1 Reviewing the Information Security Measures

Compliance Requirements

(1) Reviewing the information security measures

[BASIC Requirements]

(a) The person who established the information security rules must consider whether reviewing the rules is required as need arises and if it is required, then he or she must review them.

(b) In the case that the employee finds any issues or problems in the information security rules, he or she must consult with the person who established them.

(c) The person who establishes the information security rules must take necessary measures when he or she is consulted with regard to any issues or problems regarding the rules.

1.2.5 Others

1.2.5.1 Outsourcing

Scope

This is applied to the information processing tasks out of the job functions provided based on Article 29 of the Accountancy Act which stipulates leases, contracts, and other agreements, including the following items:

- Software development (programming, system development, etc.)
- Information processing (statistics, tabulation, data entry, media conversion, etc.)
- Leasing
- Examination and research (examination, research, investigation, etc.)

Compliance Requirements

⑴ Establishing the mechanism to ensure information security common in the government agencies

[BASIC Requirements]

(a) The head of information security officers must establish the criteria to determine the scope of information systems that can be outsourced and the scope of information assets that may be accessed by the contractors.

(b) The head of information security officers must establish standard and procedures for the selection of outsourcer.

[ENHANCED Requirements]

(c) The head of information security officers must establish the procedure to evaluate the information security level of the contractor based on the international standards in order to select a contractor more stringently.

⑵ Clarifying the Information Security Measures to be implemented by the contractors

[BASIC Requirements]

(a) The information system security officer or the division/office information security officer must specify the information security measures that the contractor must implement in the outsourced works and notify the candidate contractors in advance.

(b) The information system security officer or the division/office information security officer must formulate the response procedure in the case information security is violated in contracted work and notify the candidate contractors in advance.

(c) The information system security officer or the division/office information security officer must establish a procedure to check how well the information security measures are implemented by the contractor and the response procedure in the event of poor implementation, and notify them to the candidate contractors in advance.

⑶ Selecting the outside contractor

[BASIC Requirements]

(a) The information system security officer or the division/office information security officer must to select a contractor based on the standard and procedures for selection.

[ENHANCED Requirements]

(b) The information system security officer or the division/office information security officer must check the information security level of the candidate contractors in accordance with the procedure to evaluate the information security level of the contractor based on the international standards and utilize it to make a selection.

⑷ Contracts pertaining to outsourced work

[BASIC Requirements]

(a) The information system security officer or the division/office information security officer must sign an outsourcing agreement with the contractor that stipulates implementation of the information security measures in the contracted work, nondisclosure (including prohibiting use of information for non-business purposes), response procedures in the case of information security breaches, procedures to check implementation of information security measures, or response procedures in the case of poor implementation of information security measures. Also, he or she should include the following items in the agreement as needed:

  (i) To take steps to make the contractor undergo the information security audit

  (ii) To take steps to make the contractor secure the service level

(b) The information system security officer or the division/office information security officer must specify the responsibilities of both organizations, build consensus, and request to present the confirmation document etc. regarding compliance with the information security requirements and the management framework. The following descriptions should be included in the confirmation document etc. as needed:

  (i) Specification of the person who engages in the outsourced work

  (ii) Detailed work that the person does in order to implement the information security measures

(c) The information system security officer or the division/office information security officer must determine whether to renew the outsourcing agreement based on the standard and procedure for selection on a case-by-case basis. Particular care needs to be taken for negotiated contracts.

(d) The information system security officer or the division/office information security officer must consider whether to change the services that are provided by the contractor (including maintenance and improvement of the policy for information security, operation procedures, and management procedure) based on the standard and procedures for selection.

(e) The information system security officer or the division/office information security officer must prohibit the outsoucer from subcontracting all or part of the outsourced works to a third party. However, it is not limited if receives an application from the outsoucer to do this and determines that information security is ensured against the potential dangers from subcontracting.

⑸ Procedures in implementing the outsourcing

[BASIC Requirements]

(a) In the case that the employee provides classified information or important specifications to the contractor, he or she must provide only the minimum necessary information and take the following measures.

  (i) In the case that the employee provides information to the contractor, he or she must provide it in a safe delivery method and record the provision of the information.

(ii) In the case that the provided information becomes unnecessary for the contractor due to the termination of the outsourcing, etc., the employee must have them return, dispose, or delete the information without fail.

(b) In the case that information security is violated in contracted work, the information system security officer or the division/office information security officer must have the contractor take necessary measures in accordance with the defined response procedure.

(c) The information system security officer or the division/office information security officer must check how the information security measures are implementated by the contractor in accordance with the defined procedure.

⑹ Procedures to terminate the outsourcing

[BASIC Requirements]

(a) The information system security officer or the division/office information security officer must confirm the information security measures implemented in the outsourced work when he or she terminates the outsourcing and adds the confirmation to the inspection.

1.2.5.2 Consistently Operation with the Business Continuity Plan (BCP)

Scope

This applies to the government agencies that establish or will establish BCP in accordance with “Central Government Agency Business Continuity Plan Version 1” (the Cabinet Office, June 2006).

Compliance Requirements

(1) Ensure a consistently of information security measures and plan for BCP in the government

[BASIC Requirements]

(a) If a government agency prepares BCP or standard countermeasures, the Information Security Council must review the documents for consistency.

(b) The chief information security officer, information security officer, information system security officer and division/office information security officer must review all the information systems whether these are related to BCP, which are planned to develop by the government agencies if any.

(c) The chief information security officer, information security officer, information system security officer and division/office information security officer must establish a common operation procedure based on BCP and standards of government agencies for information systems that were confirmed to be related to the BCP if government agencies have a plan to establish BCP as follows.

(i) The documents need to be reviewed within the extent of information security in order to operate the common elements of the BCP and the standards of government agencies in consistently at a normal state.

(ii) Emergency rules need to be prepared to continue the operation by identifying the compliance requirements of information security which could hinder the implementation of the BCP and the standards of government agencies in case of occurrence of any accidents.

(2) Reporting inconsistency between the BCP and the information security related rules

[BASIC Requirements]

(a) If there is a plan to prepare BCP by a government agency but it is difficult to determine whether this plan is difficult to implement due to inconsistency of requirements between the BCP and the information security rules, parties concerned must be notified with the information. In addition, the information security officer must also be notified of the fact for instructions according to the reporting procedure of failure and accidents, which was prepared by the head of information security officers has established.

Chapter 1.3 Measures for Information

1.3.1 Information Handling

1.3.1.1 Creating and Obtaining Information

Compliance Requirements

(1) Prohibiting creation or obtainment of Information for non-business purposes

[BASIC Requirements]

(a) The employee must not create or obtain any information for the purpose other than executing his or her governmental business

(2) Preparation of information classification and limitation for creation or obtain to use.

[BASIC Requirements]

(a) The employee must determine the classification and limitation of use of information prepared, or obtained by those who outside of the government agencies, according to the definition of the classification and limitation of use at the beginning of the management of the information.

(b) The employee reconsiders to determine whether the classification and limitation of use of the information defined by other needs to be changed at correction, addition or deletion of the original information.

(3) Labeling classification and marking

[BASIC Requirements]

(a) The employee must labeling the classification and limitation of use for the information (including the revised one, hereafter) in a way that the person who is allowed to view may recognize.

(4) Suceed of use classification and limitation

[BASIC Requirements]

(a) When the employee prepares information, its classification and limitation of use must be succeeded according to the confidentiality of the original information if the information referred or obtained have a certain classification or limitation of use.

1.3.1.2 Usage of Information

Compliance Requirements

(1) Prohibiting usage for non-business proposes

[BASIC Requirements]

(a) The employee must not use any information for a purpose other than executing his or her tasks.

(2) Handling the information based on classification and marking

[BASIC Requirements]

(a) The employee must handle information appropriately in accordance with the classification labeled on the information. In the case that marking is also labeled beside the classification, the instructions for marking must be followed.

(3) Succession for copying classification and limitation of use

[BASIC Requirements]

(a) The employee must continuously apply the classification and limitation of use concerning confidentiality of the original information for copying the information.

(4) Reviewing the classification and marking

[BASIC Requirements]

(a) If the employee believes that the original classification or limitation of use of the information is inappropriate at this point, and the classification or limitation of use which was determined by others needs to be reviewed, the person who made the decision (including those who succeeded the decision) or his/her superior ("authority" in this section hereinafter) must be consulted with.

(b) If the employee believes the information for classification and limitation of use that was provided by the employee needs to be reviewed, the classification or limitation of the information must be reconsidered and labeled accordingly. The employee must notify the persons who access the information beforehand, whenever possible.

(5) Handling classified information

[BASIC Requirements]

(a) The employee must not take classified information outside the government agency for the purpose other than executing his or her tasks.

(b) The employee must not leave classified information unattended.

(c) The employee must not make copies of confidentiality class-3 information more than necessary.

(d) The employee must not distribute confidential information more than necessary.

[ENHANCED Requirements]

(e) For confidentiality class-3, the employee must clearly indicate the term during which it should be treated as confidentiality class-3. Even during this term, the classification and limitation of use may be reviewed upon certain process if it is considered that the classification and limitation of use needs to be mitigated.

(f) The employee must place a serial number for documents of Confidentiality class-3 information to clearly identify where it is filed.

1.3.1.3 Maintenance of Information

Compliance Requirements

⑴ Maintaining the information based on classification

[BASIC Requirements]

(a) The employee must provide appropriate access control on classified information stored in the electronic storage media.

(b) The employee must manage the electronic storage media appropriately in accordance with the classification of the information saved.

(c) The employee must manage the written document containing confidential information or important specifications which are include input into or output from the information systems.

(d) The employee must consider whether encryption is required of confidential information will save for the electronic storage media, if it is required, the document must be encrypted with a password.

(e) The employee must consider whether encryption is required in the case that he or she stores confidential information in the electronic storage media and if it is required, then he or she must encrypt it.

(f) The employee must consider whether performing an electronic signature is required in the case that he or she stores critical information in the electronic storage media and if it is required, then he or she must perform an electronic signature.

(g) For electronic records or important specifications which are critical information or vital information, the employee must consider whether making a back-up or copy is required and if it is required, then he or she must make a back-up or copy of them.

(h) For back-ups or copies of electronic records or important specifications which are critical information or vital information, the employee must consider whether contingency planning is required and if so, then he or she must take appropriate measures to prevent all sites from being impacted by a disaster.

⑵ Information Retention Period

[BASIC Requirements]

(a) The employee must keep the information stored in the electronic storage media until the retention period expires in the case that such a period is set and delete it without delay in the case that the period does not require extension.

1.3.1.4 Transfer of Information

Compliance Requirements

⑴ Gaining approval and notifying of information transfer

[BASIC Requirements]

(a) The employee must gain approval from the division/office information security officer in the case that he or she transfers confidentiality class-3 information, integrity class-2 information, availability class-2 information, or important specifications.

(b) The employee must notify the division/office information security officer if electronic records of confidentiality class-2 information and integrity class-1 information as well as availability class-1 information or written documents including confidentiality class-2 information are transferred. However, the notification is not required for the information transfer for which the division/office information security officer considers that it is not required.

⑵ Selecting between transmitting and transporting the information

[BASIC Requirements]

(a) The employee must select to transmit or transport electronic records of confidential information in consideration of safety and notify the division/office information security officer. However, this notification is not required for transfer of electronic records of confidentiality class-2 information and integrity class-1 information as well as availability class-1 information, for which the division/office information security officer decides it unnecessary.

⑶ Selecting the transfer means

[BASIC Requirements]

(a) The employee must choose to transfer confidential information or important specifications in consideration of safety, and notify the division/office information security officer. However, the notification is not required for transfer of electronic records of confidentiality class-2 information and integrity class-1 information as well as availability class-1 information or written documents including confidentiality class-2 information, for which the division/office information security officer considers that it is not required.

⑷ Protection of documents

[BASIC Requirements]

(a) If the employee takes confidential information or important specifications in writing, appropriate security measures must be taken in accordance with the classification and limitation of use of information, etc.

⑸ Protecting the electronic records

[BASIC Requirements]

(a) In the case that the employee transfers electronic records of confidential information, he or she must consider whether protection by password is required and if it is required, then he or she must set a password for it.

(b) In the case that the employee transfers electronic records of confidential information, he or she must consider whether encrypting the information is required and if it is required, then he or she must encrypt it.

(c) In the case that the employee transfers electronic records of confidential information, he or she must consider whether performing an electronic signature is required and if it is required, then he or she must perform an electronic signature to the information.

(d) In the case that the employee transfers electronic records of confidential information, he or she must consider whether back-ups are required and if they are required, then he or she must make a back-up of the information.

(e) In the case that the employee transfers electronic records of vital information, he or she must consider whether any measures are required such as transferring the same electronic records on different routes so as to prepare for a possible hindrance due to lost or missing data or delays in transfer to the destination. If it is required, then he or she must take necessary measures.

[ENHANCED Requirements]

(f) In the case that the employee transfers electronic records of confidential information, he or she must encrypt it in a way to provide the encryption strength required, split it into pieces, and transfer it using different routes.

1.3.1.5 Provision of Information

Compliance Requirements

⑴ Releasing the information

[BASIC Requirements]

(a) The employee must confirm that the information is classified into confidentiality class-1 information when he or she releases the information.

(b) The employee must take measures to prevent the inadvertent leak of information from added pieces, etc. when he or she releases electronic records.

⑵ Providing the information to others

[BASIC Requirements]

In the case that the employee provides confidentiality class-3 information, integrity class-2 information, availability class-2 information, or important specifications to the person outside the government agency, he or she must gain approval from the division/office information security officer.

(a) If the employee discloses confidentiality class-3 and integrity class-2 or availability 2 or important specifications to those who outside of the government agencies, it is required to obtain permission of the division/office information security officer.

(b) If the employee discloses electronic records of confidentiality class-2 but integrity class-1 and availability 1 or documents of confidentiality class 2 to those who outside of the government agencies, it is required to obtain permission of the division/office information security officer. However, it is not limited when the division/office information security officer considers that it is not required.

(c) If the employee discloses information that should be protected or important specifications to those who outside the government agencies, necessary measures must be taken to properly use the information according to the classification and limitation of use of the information.

(d) In the case that the employee provides electronic records, he or she must take measures to prevent inadvertent leak of information from added pieces, etc.

1.3.1.6 Deleting of Information

Compliance Requirements

⑴ Deleting the electronic records

[BASIC Requirements]

(a) In the case that the employee disposes of electronic storage media, he or she must make all the information difficult to restore (hereinafter referred to as to “delete”).

(b) In the case that the employee provides the electronic storage media to others, he or she must delete unnecessary confidential information stored in the electronic storage media.

[ENHANCED Requirements]

(c) The employee must delete the confidential information stored in the electronic storage media in the case that he or she is required to do so considering the environment, etc.

⑵ Disposing the written documents

[BASIC Requirements]

(a) The employee must dispose the written document containing confidential information in a way to make it difficult to restore.

Chapter 1.4 Measures for Information Processing

1.4.1 Restriction of information processing

1.4.1.1 Restrictions on Information Processing outside the Government Facility

Compliance Requirements

⑴ Establishing procedures on the security measures

[BASIC Requirements]

(a) The head of information security officers must define the procedures on security measures for processing classified information outside the government agency.

(b) The head of information security officers must define the procedures on security measures for bringing the information systems that handle classified information outside the government agency.

⑵ Gaining approval, notifying, and management

[BASIC Requirements]

(a) If the employee processes confidentiality class-3, integrity class-2, or availability class-2 information outside the government agencies, it is required to obtain a permission of the information system security officer or the division/office information security officer.

(b) If the employee processes information that is confidentiality class-2 and integrity class-1 information as well as availability class-1 information outside the government agency, it is required to obtain a report of the information system security officer or the division/office information security officer. However, it is not limited when the information system security officer or division/office information security officer considers that it is not required.

(c) The information system security officer and the division/office information security officer must record processing of classified information that is done outside the government agency.

(d) If the information system security officer and the division/office information security officer do not receive a report from those who used the information after the expiration date of approval for processing confidentiality class-3 information, integrity class-2 information, or availability class-2 information outside the government agency, it is necessary to confirm the situation and to take necessary measures. However, it is not limited if the person who has given the approval considers that it is not required

(e) If the predetermined term ends for processing confidentiality class-2 information and integrity class-1 information as well as availability class-1 information outside the government agency, it is necessary to confirm the situation and take measures as required.

(f) In the case that the employee processes classified information outside the government agency, he or she must process the minimum information required for executing his or her tasks.

(g) If the employee takes the information system handling the confidentiality class-3, integrity class-2 or availability class-2 information outside the government facility, it is required to obtain the approval of the information system security officer and division/office information security officer.

(h) If the employee takes the information system handling the confidentiality class-2, integrity class-1 or availability class-1 information outside the government facility, it is required to obtain the report of the information system security officer and division/office information security officer. However, it is not limited However, it is not limited if the person who has given the approval considers that it is not required.

(i) The information system security officer and the division/office information security officer must record bringing the information systems that handle classified information outside the government agency.

(j) If the information system security officer or the division/office information security officer does not receive a report of expiration when the approved period for taking confidentiality class-3 information, integrity class-2 information, or availability class-2 information outside the government agency expires, it is required to confirm the status and take appropriate measures. However, it is not limited However, it is not limited if the person who has given the approval considers that it is not required.

(k) If the predetermined term expires for bringing outside the government agency information that is confidentiality class-2 information and integrity class-1 information as well as availability class-1 information, the information system security officer or the division/office information security officer must confirm the status and take appropriate measures as needed.

(l) In the case that the employee brings the information systems that handle classified information outside the government agency, he or she must take the minimum amount of information systems required for executing his or her tasks.

⑶ Implementing the Security Measures

[BASIC Requirements]

(a) The employee must take the security measures that are formulated for processing classified information outside the government agency.

(b) In the case that the approved period for processing confidentiality class-3 information, integrity class-2 information, or availability class-2 information outside the government agency expires, the employee must report this to the person who has given approval. However, this is not always required if the person who has given approval does not require reporting.

(c) The employee must take the security measures that are formulated for bringing the information systems that handle classified information outside the government agency.

(d) In the case that the approved period for bringing the information systems that handle confidentiality class-3 information, integrity class-2 information, or availability class-2 information outside the government agency expires, the employee must report this to the person who has given approval. However, this is not always required if the person who has given approval does not require reporting.

1.4.1.2 Restrictions on Information Processing Using Information Systems Not Supplied by the Government Agency

Compliance Requirements

⑴ Establishing procedures on the Security Measures

[BASIC Requirements]

(a) The head of information security officers must define the procedures on security measures for processing classified information using the information systems not supplied by the government (unsupplied information systems).

⑵ Gaining approval, notifying, and management

[BASIC Requirements]

(a) If the employee needs to process confidentiality class-3 information, integrity class-2, information or availability class-2 information using information systems provided by a non-government organization, it is required to obtain the approval of the information system security officer and the division/office information security officer.

(b) If the employee needs to process confidentiality class-2 information, integrity class-1, information and availability class-1 information using information systems provided by a non-government organization it is required, it is required to apply for the permission to the information system security officer and the division/office information security officer. However, it is not limited if information system security officer or division/office information security officer considers that it is not necessary.

(c) The information system security officer and the division/office information security officer must record processing of classified information which is done using the unsupplied information systems.

(d) If the information system security officer and the division/office information security officer do not receive a report of expiration when the approved term for processing confidentiality class-3 information, integrity class-2 information, or availability class-2 information using the unsupplied information systems expires, it is required to confirm the status and take appropriate measures. However, this is not always required if the person who has given approval does not require reporting.

(e) If the term is expired for processing confidentiality class-2 information and integrity class-1 information and availability class-1 information, the information system security officer and the division/office information security officer must confirm the status and take appropriate measures as needed.

⑶ Implementing the Security Measures

[BASIC Requirements]

(a) In the case that the employee processes classified information using the unsupplied information systems, he or she must take the security measures that are formulated for the relevant information systems.

(b) In the case that the approved period for processing class-3 information, integrity class-2 information, or availability class-2 information using the unsupplied information systems expires, the employee must report this to the person who has given approval. However, this is not always required if the person who has given approval does not require reporting.

Chapter 1.5 Basic Security Requirements of Information System

1.5.1 Security Requirements of Information Systems

1.5.1.1 Security Requirements of Information Systems

Compliance Requirements

(1) Planning the information system

[BASIC Requirements]

(a) The information system security officer must require the person who is responsible for information systems to establish the system to maintain security throughout their lifecycle.

(b) The information system security officer must decide the security requirements of the information systems.

(c) The information system security officer must define the measures in purchasing (including leasing) equipment, etc., developing software, configuring the information security functions, protecting against the threats to information security, and handling measures for components of information systems in order to meet the security requirements of information systems.

(d) If the information system security officer confirms that there are critical important security requirements for an information system to be designed, ST (ST: Security Target) assessment or ST verification is required according to the information security design specification by a third-party organization is required. However, it is not limited if it is confirmed that the critical security requirement amendment is minor according to the security design specification upon review, as long as the information system was updated, or the specification change were needed during its design phase.

(e) The information system security officer must define the monitoring procedure for information systems. If necessary when there is need to monitor the occurrence of an event that may or breach of security.

(f) The information system security officer must define the installation procedure and environmental requirements in terms of information security when the information system he or she has built goes into the operation phase.

[ENHANCED Requirements]

(g) If the information system security officer confirms that there are critical important security requirements for an information system to be designed, it is required to define the security function needed for the equipment and software to be procured as a product, based on the security function design requirement. If there are some candidate products which meet the function and other requirements, and some of the products have certified as IT security assessment and certification concerning the security functions, it will be selected as a component of the information system.

⑵ Configuration and operation of the information systems

[BASIC Requirements]

(a) The information system security officer must take the information security measures that have been specified based on the security requirements to configure and operate the information systems.

⑶ Moving and disposing of the information systems

[BASIC Requirements]

(a) In the case that the information system security officer moves or disposes of the information systems, he or she must consider whether deleting or saving the information, or disposing or reusing the information systems is required and take appropriate measures in either case.

⑷ Reviewing the information systems

[BASIC Requirements]

(a) The information system security officer must consider as appropriate whether reviewing the information security measures for the information systems is required, and if it is required, then he or she must carry out the review and take appropriate measures.

1.5. 2 Compliance with Regulations and Maintenance of Information Systems.

1.5.2.1Maintenance of Document related with the Information Systems

Compliance requirements

⑴ Maintenance of documents of the information system

[BASIC Requirements]

(a) The information system security officer must provide the following documents on the information system to be managed by him or her.

(i) Computers to configure the information system

- Information to identify the employee to manage the computer and user
- The type of the computer and the type and version of software
- Specification or design document of the computer

(ii) Communication line and communication equipment to configure the information system

- Information to identifying the communication line and the employee managing the communication equipment
- The type of the communication equipment and the type and version of the software
- Specification or design document of the communication line and communication equipment
- Configuration of the communication line
- Settings of the communication equipment access control
- Identification of the computer using the communication line and conformance of the identification codes of the computer user and the communication line
- Divisions to use the communication line

(iii) Procedure ensuring security of the information system components

- Procedures for ensuring the computer security
- Procedures for ensuring the services to be provided through the communication line
- Procedures for ensuring security of the communication line and communication equipment

(iv) Procedures of measures in the case of failure or accidents

(b) The information system security administrator must take information security measures for operating and managing the information system based on the document provided by the information system concerned.

⑵ Establishing the information system ledger

[BASIC Requirements]

(a) The head of information security officer must provide a file to record the following concerning the information system for all the information systems

(i) Name of the information system, name/contact information of the department or person who manage it

(ii) System configuration

(iii) Type of the outside government facility communication line available

(iv) Classification and limitation of use for the information to be handled

(v) Design/development, operation and maintenance of the information system

(b) The information system security officer must report the descriptions of the information system record to the head of information security officer when the information system is newly configured or updated.

1.5.2.2 Purchasing the equipment, etc.

Scope

This applies to purchases (including leases; hereinafter the same) of the equipment, etc.

Compliance Requirements

(1) Establishing the Regulations for procurement of equipment

[BASIC Requirements]

(a) The head of information security officers must formulate the selection criteria for the equipment, etc.

(b) The head of information security officer must specify the standards for selection as IT Security Assessment and Certification for procurement of the equipment if there are required specifications and the general assessment tendering system to be applied.

(c) The head of information security officers must formulate the confirmation and test procedure for the equipment, etc. in terms of information security measures.

(2) Compliance with the regulations for procurement of the equipment

[BASIC Requirements]

(a) In the case that the information system security officer selects the equipment, etc., he or she must consider whether the equipment, etc. meets the selection criteria and utilize the results to make a selection.

(b) The information system security officer must examine the equipment upon delivery according to the defined confirmation/examination procedures.

1.5.2.3 Software Development

Compliance Requirements

(1) Establishing the regulations for software development

[BASIC Requirements]

(a) The head of information security officer must establish the regulations required for the information system security officer for the following measures concerning the security software development.

(i) The information system security officer must establish the system for development to meet the security measures (compliance requirements (c) to (i).

(ii) If the information system security officer software development for outsource, he or she must selection of necessary information security measures (or compliance requirements of (c) to (i)) that should be implemented by the contractor and ensure that such implementation is assured by the contractor.

(iii) The information system security officer must define the procedure and environment for each phase of software development in terms of information security.

(iv) The information system security officer must consider whether the information for software development and testing should be separated from the information system in operation from terms of the information security, and separate it if considered to be required.

(v) The information system security officer must consider whether the security function is required according to the results of analysis on the information resources concerning the software to be development the classification and limitation of the information handled by the software when it is in operation. If it is required, he or she must properly design the security function and clearly describe it on the design document.

(vi) The information system security officer must consider whether a function to manage the security functions for operation of the software to be developed is required, and if it is required, then he or she must design the management function appropriately and clearly describe it in the design document.

(vii) The information system security officer must define the scope and procedure of review to confirm the validity of information security in software design and review it accordingly.

(viii)The information system security officer must consider whether a function to confirm the validity of information security in the data processed or input-output by the software to be developed is required and if it is required, then he or she must design the function appropriately and clearly describe it in the design document.

(ix) In the case that there are any important security requirements for the software to be developed, the information system security officer must request a security target (ST) evaluation and confirmation by the third-party organization for the purpose of the design of security functions to meet them. However, in the case that he or she undergoes the ST evaluation and confirmation for the information system that contains the relevant software or updates the software, or the specification changes in the process of development and the changes in important security requirements are found to be only minor in the reviewed security target, such evaluation and confirmation are not always required.

(x) The information system security officer must protect against unnecessary access and make a back-up of the source code that is formulated by the software developer.

(xi) The information system security officer must define the rule for coding in terms of information security.

(xii) The information system security officer must consider whether the source code developed is required to undergo the source code review to verify the applicability of the information security. If it is required conduct the source code review by defining the source code review range and method.

(xiii)The information system security officer must consider whether any testing is required in terms of security, and if it is required, then he or she must define the items and procedure of testing and conduct the test.

(xiv)The information system security officer must record the test that is conducted in terms of information security.

⑵ Compliance of software development related regulations

【BASIC Requirements】

(a) The information system security officer must develop software according to the software development related regulations.

1.5.2.4 Standard Procedures of Encryption and Electronic Signatures

Compliance Requirements

(1) Establishing the regulation for encryption and performing electronic signatures

[BASIC Requirements]

(a) The head of information security officers must define the algorithm and implementation system for encryption and performing electronic signatures to be used in the government agencies.

(i) Those which on the electronics government recommended list must be used if it is available.

(ii) If encryption or electronic signature is deployment the new development or update of the information system, the algorithm specified in the electronics government recommended encryption list must be used. However, some of those algorithms concerned must include specified in the electronics government recommended encryption list, at least one, for cases that the encryption or electronic signature is implemented.

(b) The head of information security officer must define the procedures of (i) and (ii) (“procedures for managing the key”, hereinafter).

(i) Procedures for creation of the key, validity, deletion, update and measures when the key is exposed etc.

(ii) Procedures for storing the key

【ENHANCED Requirements】

(c) The information security officer must define the procedure to obtain the backup of the key for decrypt information or its storage procedure (“backup procedures of the key”, hereinafter).

⑵ Compliance of encryption and electronic signature

【BASIC Requirements】

(a) The employee must follow the defined algorithm when encrypting information and applying an electronic signature.

(b) The employee must follow the defined management procedure of the key for ones to be used to restore encrypted information or with electronic signature, and manage it in an appropriate.

【ENHANCED Requirements】

(c) The employee must obtain the backup of keys according to the defined backup procedure of the key for restoration.

1.5.2.5 Preventing actions that lower the Information Security Level outside the Government Agency

Compliance Requirements

⑴ Establishing the regulations on the measures for lower the information security levels.

[BASIC Requirements]

(a) The head of information security officers must define the procedures for measures to prevent actions that would lower the level of information security outside the government agency.

⑵ Implementing on the measures for lower the information security levels.

[BASIC Requirements]

(a) The employee must take necessary measures according to the regulations for prohibited actions to deteriorate the information security standards outside the government facility.

1.5.2.6 Measures for using Domain Name

Compliance Requirements

⑴ Establishing the regulations of domain name to use

[BASIC Requirements]

(a) The head of information security officer must establish the regulations required for the employee to use a domain name according to the domain name system (domain name, hereinafter) as follows.

   (i) The employee must use the domain name to guarantee the following government domain name (“government domain name” hereinafter) if it is necessary to send the domain name to a person outside the government facility to access the website or sending e-mails (except those who resides overseas, hereinafter in this section).

      - Domain name ended up with go.jp

- Japanese domain name reserved as the one concerning administrative affairs

However, other domain names other than the government domain name may be notified if the following conditions are met only for sending e-mails or the description on the website under the name of the government domain name.

In specific, all the following conditions must be met for sending e-mails.

- An e-mail address with the government domain name or the electronic signature with the government domain name is clearly described as a contact for inquiries to the notification.
- The organization for managing the domain name to be notified must be clearly described.
- When the validity of the domain name to be notified was confirmed or the term to guarantee the validity must be clearly described.

All of the following conditions must be met for descriptions of the webpage under the government domain name.

- The name of organization for managing the domain name to be notified must be clearly described.
- When the validity of the domain name to be notified was confirmed or the term to guarantee the validity must be clearly described.

(ii) The employee must use the government domain name for sending e-mails to the person outside the government facility. However, it may not include the case when the employee is known by the person outside the government facility.

(iii) The employee must only use the government domain name server if he or she use the server for storing the information to allow the person outside the government facility to access the website.

⑵ Compliance with Regulations for Domain Name

[BASIC Requirements]

(a) The employee must take necessary measures according to the regulations for the usage of the domain name.

1.5.2.7 Daily Measures for Protection against Malware

Compliance Requirements

⑴ Establishing the Regulations for Malware Countermeasures

[BASIC Requirements]

(a) The head of information security officer must define the regulations to require the employees to protect the information system from malware as follows.

(i) The employee must not open files detected as malware by antivirus software and not read the data file with the application program etc.

(ii) The employee must always keep the applications and malware definition files used with antivirus software updated.

(iii) The employee must enable the automatic malware detection function provided by antivirus software, etc.

(iv) The employee must check for malware in all the electronic files using antivirus software, etc. periodically.

(v) The employee must check whether there is an infection by malware when he or she loads external data or software into the computers or provides data or software externally.

(vi) The employee must make efforts to prevent the information system from infecting any malwares.

(vii) The employee must disconnect the communication line to an infected computer and take necessary measures if the information system is at the risk of infection of any malwares.

⑵ Compliance with regulations for malware countermeasures

[BASIC Requirements]

(a) The employee must take daily measures to prevent the information system from being infection by malware according to the defined regulations for malware countermeasures.

Volume 2 Information system

Chapter 2.1 Measures based on Clarifying Information Security Requirements

2.1.1 Information Security Functions

2.1.1.1 Authentication Functions

Compliance Requirements

(1) Introducing the authentication functions

[BASIC Requirements]

(a) The information system security officer must consider whether authentication is required for every information system. He or she must determine that an information system that handles classified information requires authentication.

(b) The information system security officer must provide functions for identification and authentication for the information systems for which authentication is required.

(c) In the case that authentication information must be kept secret, the information system security administrator must manage to keep the authentication information unknown to others for the information systems for which authentication is required.

(i) The authentication information must be encrypted in the case that it is stored.

(ii) The authentication information must be encrypted in the case that it is communicated.

(iii) If the authentication information cannot be encrypted in the case that it is stored or communicated, the user must be notified that it is not encrypted when he or she sets, changes, or provides (enters) authentication information.

(d) For the information systems for which authentication is required, the information system security officer must establish a function to prompt users to change authentication information periodically in the case that he or she requires such changes to users along with either of the following functions:

(i) A function to check whether the users change the authentication information periodically

(ii) A function to refuse continued use of the information system in the case that the users do not change the authentication information periodically

(e) For the information systems for which authentication is required, the information system security officer must establish a function to stop authentication using the relevant authentication information or authentication information storage device or to stop use of information systems using a corresponding identification code in the case that he or she recognizes that the authentication information or authentication information storage device is used or can be used by another party.

(f) For the information systems for which authentication is required, the information system security officer must establish the following functions in the case that he or she uses authentication method by knowledge:

(i) A function to let the users set their own authentication information

(ii) A function to keep the authentication information set by the users in a state in which other parties cannot know it easily

(g) For the information systems for which authentication is required, the information system security officer must meet all the applicable requirements in the case that he or she uses an authentication method other than that based on knowledge, ownership, or biological information, after examining whether the following are applicable or not in defining the requirements.

(i) Any subject other than the legitimate subject must not be accepted (prevention of incorrect permission).

(ii) The legitimate subject must not be denied for any reasons for which it is not responsible (prevention of false denial).

(iii) The legitimate subject must not be able to grant (including issuance, renewal, and change; hereinafter the same in this section) or lend its authentication information to other parties easily (prevention of substitution).

(iv) The authentication information must not be easily duplicated (prevention of duplication).

(v) There must be means to invalidate logons individually at the discretion of the information system security administrator (assurance of invalidation).

(vi) The authentication must be available whenever necessary, without any interruption (assurance of availability).

(vii) In the case that any information or device needs to be provided from outside to add new subjects, such information or devices can be sufficiently provided during the life of the information system (assurance of continuity).

(viii)The authentication information must be able to re-issuance to the legitimate subject in a secure manner if the authentication information granted to it cannot be used (assurance of re-issuance).

(h) The information system security officer must not use the relevant biological information for the purpose other than that agreed by the user in advance if he or she uses authentication method based on biological information. Also, he or she must be careful not to invade the privacy of the user in using the relevant biological information.

[ENHANCED Requirements]

(i) For the information systems for which authentication is required, the information system security officer must establish a function to perform multiple factors authentication method.

(j) For the information systems for which authentication is required, the information system security officer must establish a function to notify the information for the last logon to the user who has logged on.

(k) For the information systems for which authentication is required, the information system security officer must establish a function to detect or prevent any attempts at illegitimate logon.

(l) For the information systems for which authentication is required, the information system security officer must establish a function to display a notification about the use of the information system before the user login to the information system.

(m) For the information systems for which authentication is required, the information system security officer must establish a function to prevent the users from re-using the same authentication information as that previously used in the case that he or she requires periodic changes in authentication information.

(n) For the information systems for which authentication is required, the information system security officer must establish a function to require that the users logon using an individual identification code before they login using the identification code in the case that the identification code with administrative rights is shared.

⑵ Identification code handling

[BASIC Requirements]

(a) The employee must not use the information system using an identification code other than the one provided upon authentication.

(b) The employee must not provide or allow others to use the identification code other than for the purpose of authentication.

(c) The employee must not leave the identification code that has been granted to him or her in a state in which it can be known by the parties who do not need to know it.

(d) The employee must notify the information system security administrator in the case that he or she does not need to use the identification code any longer. However, this reporting is not always required if the information system security officer has stated that individual reporting is not required.

[ENHANCED Requirements]

(e) The employee who is granted an identification code with administrative permissions must use it only when he or she executes the tasks as an administrator.

⑶ Authentication information handling

[BASIC Requirements]

(a) In the case that authentication information is used or can be used by others, the employee must report this to the information system security officer or the information system security administrator immediately.

(b) In the case that the information system security officer or the information system security administrator receives a report that authentication information has been used or can be used by others, he or she must take necessary measures.

(c) In the case that the employee uses authentication method based on knowledge, he or she must meet the following items

(i) The employee must keep his or her authentication information unknown to others in handling.

(ii) The employee must not provide what his or her authentication information is.

(iii) The employee must try to remember his or her authentication information.

(iv) The employee must select authentication information that cannot be guessed easily when he or she set it.

(v) In the case that the employee is instructed to change authentication information periodically by the information system security administrator, he or she must do so.

(d) In the case that the employee uses authentication method based on ownership, he or she must meet the following requirements:

(i) The employee must take security measures so that the authentication information storage device is not used in an unintended manner.

(ii) The employee must not provide his or her authentication information storage device to others.

(iii) The employee must manage not to lose the authentication information storage device. In the case that it is lost, he or she must report this to the information system security officer or the information system security administrator.

(iv) In the case that the employee does not need to use the authentication information storage device any longer, he or she must return this to the information system security officer or the information system security administrator.

2.1.1.2 Access Control Functions

Compliance Requirements

⑴ Introducing the access control functions

[BASIC Requirements]

(a) The information system security officer must consider whether access control is required for every information system. He or she must determine that an information system that handles classified information requires access control.

(b) For the information systems for which access control is required, the information system security officer must establish a function to provide access control.

[ENHANCED Requirements]

(c) For the information systems for which access control is required, the information system security officer must add a function to provide access control based on the attributes other than those of the user and the group the user belongs to.

(d) For the information systems for which access control is required, the information system security officer must establish a function to Mandatory Access Control (MAC).

⑵ Configuring Access control

[BASIC Requirements]

(a) The information system security officer must make an access control according to the classification and marking of the information to be stored in the information system for those which the employee is unable to make an access control.

2.1.1.3 Administration Functions

Compliance Requirements

⑴ Introducing the administration functions

[BASIC Requirements]

(a) The information system security officer must consider whether administration is required for every information system. He or she must decide that an information system that handles classified information requires administration.

(b) For the information systems for which administration is required, the information system security officer must establish a function to provide this administration.

[ENHANCED Requirements]

(c) For the information systems for which administration is required, the information system security officer must establish a function of the least privilege.

(d) For the information systems for which administration is required, the information system security officer must establish a function to re-issuance authentication information automatically.

(e) For the information systems for which administration is required, the information system security officer must establish a dual locking function.

⑵ Granting and managing identification code and authentication information

[BASIC Requirements]

(a) For the information systems for which administration is required, the information system security officer must decide to approve or disapprove the use of the shared identification code for each information system.

(b) The information system security officer must define the procedures including the following for administration concerning the information system.

   (i) The procedure to validate that the applicant is the legitimate subject if a subject makes a request for administration

   (ii) The initial distribution and changing procedure of authentication information

   (iii) The configure and changing procedure for access control information

(c) For the information systems for which administration is required, the information system security officer must designate a person who is responsible for the administration.

(d) The person doing administration must issue identification codes and authentication information only to the subject that has gained approval of using the information system.

(e) In the case that the person doing administration issues an identification code, he or she must notify the users whether the code is shared or not.

(f) The person doing administration must grant (including issuance, renewal, and change; hereinafter the same in this section) the identification code with administrative permissions only in the case that such identification code is required to execute the business or business responsibilities.

(g) The person doing administration must invalidate the identification code of an employee in the case that the employee does not need to use it any longer. Also, he or she must check whether unnecessary identification codes exist in the case that he or she adds or deletes an identification code due to personnel changes, etc.

(h) The person doing administration must have the employee return the authentication information storage device provided when the employee does not need to use it any longer.

(i) The person doing administration must configure access control only within the minimum necessary scope considering the business responsibilities and needs. Also, he or she must check whether inappropriate access control settings exist in the case that he or she adds or deletes an identification code due to personnel changes, etc.

[ENHANCED Requirements]

(j) The person doing administration must grant a single identification code to an employee for a single information system.

(k) The person doing administration must keep a record of which subject the identification codes have been granted. In the case that the person doing administration deletes the record, he or she must gain approval from the information security officer in advance.

(l) The person doing administration must not grant an identification code that has already been granted to one subject to any other subjects.

⑶ Applying alternative measures for identification code and authentication information

[BASIC Requirements]

(a) For the information systems for which administration is required, in the case that the information system security administrator receives a request for approval of using an alternative measure because the employee cannot use the identification code, he or she must confirm that the applicant is a legitimate user and consider whether the alternative measure is required, and if it is required, then he or she must provide it.

(b) For the information systems for which administration is required, in the case that the information system security officer or the information system security administrator receives a report of unauthorized use of an identification code, he or she must invalidate the system use with the identification code.

2.1.1.4 Audit Trail Management Functions

Compliance Requirements

⑴ Introducing the audit trail management functions

[BASIC Requirements]

(a) The information system security officer must consider whether audit trails are required for each information system.

(b) For the information systems for which audit trails are required, the information system security officer must establish a function to collect the audit trails.

(c) For the information systems for which audit trails are required, the information system security officer must define information’s for each event in order to collect the audit trails and the retention period of the audit trails.

(d) The information system security officer must define measures against the case that the authentication record is not tractable or at the risk to be unavailable for the information system that the authentication record needs to be obtained, and provide the function to the information system if it is required.

(e) For the information systems for which audit trails are required, the information system security officer must provide access control to prevent the obtained audit trails from being deleted, falsified, or accessed illegally.

[ENHANCED Requirements]

(f) For the information systems for which audit trails are required, the information system security officer must establish a function to aid automatic checking, analyzing, and reporting of the audit trails for the information system.

(g) The information system security officer must establish a function on the information system to notify any events that indicate possible information security infringement to the monitoring personnel, etc. immediately if such events are found in the obtained audit trails.

⑵ Obtaining and keeping the audit trails

[BASIC Requirements]

(a) For the information systems for which audit trails are required, the information system security administrator must record the audit trails using the function established for the information system by the information system security officer.

(b) For the information systems for which audit trails are required, the information system security administrator must define the period for which the obtained audit trails are kept and keep it until the period expires, and delete it without delay in the case that the period does not require extension.

(c) The information system security administrator must take measures against the case that is not tractable or at the risk to be unavailable for the information system that the audit trail needs to be obtained.

⑶ Studying, analyzing, and reporting the obtained audit trails

[ENHANCED Requirements]

(a) The information system security officer must examine and analyze the audit trails obtained for the information system that needs to be obtained on a regular basis, and take necessary information security measures according to the result or report to the information security officer.

⑷ Notifying the users about audit trail management

[BASIC Requirements]

(a) The information system security officer must explain the information system security administrator and the user in advance, concerning the information system that the audit trails needs to be obtained, stored, examined and analyzed.

2.1.1.5 Assurance Functions

Compliance Requirements

(1) Introducing the assurance functions

[BASIC Requirements]

(a) The information system security officer must consider whether the assurance measures are required for the information systems that handle classified information.

(b) For the information systems for which assurance measures are required, the information system security officer must establish the assurance functions.

2.1.1.6 Encryption and Performing Electronic Signatures (including key management)

Compliance Requirements

(1) Introducing the functions for encryption and performing electronic signatures

[BASIC Requirements]

(a) The information system security officer must consider whether encryption functions are required for the information systems that handle confidential information (except written documents (hereinafter the same in this section)).

(b) For the information systems for which encryption are required, the information system security officer must establish a function to provide encryption.

(c) The information system security officer must consider whether an electronic signature and review are required for the information systems that handle the classified information.

(d) For the information systems for which an electronic signature or review is required, the information system security officer must design a function to provide an electronic signature or review.

[ENHANCED Requirements]

(e) For the information systems for which encryption or electronic signature are required, the information system security officer must configure the cryptographic module as a component in a manner that it can be replaced.

(f) For the information systems for which encryption or electronic signature are required, the information system security officer must allow the select of multiple algorithms.

(g) For the information systems for which encryption or an electronic signature is required, the information system security officer must appropriately implement the selected algorithm in the software or hardware and select products that have obtained authentication based on cryptographic module tests and the authentication system so as to protect the key to use to decrypt the encrypted information or to apply an electronic signature, identification code, and authentication information.

(h) For the information systems for which encryption or performing an electronic signature is required, the information system security officer must store the key to use to decrypt the encrypted information or to perform an electronic signature in the cryptographic module with tamper-resistance in order to protect it from physical attacks by a third party.

⑵ Management for encryption and electronic signatures

[BASIC Requirements]

(a) For the information systems for which performing an electronic signature is required, the information system security officer must provide the information or a measure to validate the electronic signature to the relying party.

[ENHANCED Requirements]

(b) If the information system security officer determines that encryption or electronic signature is required, it is required to the collect information compromised of the algorithm selected for the information system as needed.

2.1.2 Threats to Information Security

2.1.2.1 Security Holes

Compliance Requirements

⑴ Building the information systems

[BASIC Requirements]

(a) The information system security officer must take measures of an announced security holes concerning software used on the computer and communication devices (except those which have no announced information of security holes, hereinafter the same in this section), when it was installed or started operation.

[ENHANCED Requirements]

(b) For the information systems that handle available information, the information system security officer must install computers and communication equipment in a redundant configuration so that the services can continue to be provided without disruption when action is taken in response to security holes.

(c) The information system security officer must take available measures for computers and communication equipment even in the case that there is no information about the announced security holes.

⑵ Operating the information systems

[BASIC Requirements]

(a) The information system security administrator must obtain information about the announced security holes relating to software used on the computers and communication equipment which he or she is responsible for as need arises.

(b) The information system security officer must establish the security hole measures for computers under management and software used for communication device, in case that the security hole related information is obtained upon making an analysis of the risk on the information system to verify the following:

   (i) Need of response

   (ii) Response procedure

   (iii) Temporary workaround procedure in the case that no response procedure exists

   (iv) Effects of response or temporary workaround procedures on the information systems

   (v) Schedule of response implementation

   (vi) Need of response testing

   (vii) Response testing procedure

   (viii)Response testing plan

(c) The information system security administrator must take measures against security holes based on the security hole response plan.

(d) The information system security administrator must record the items including date, work description, and worker for the measure against security holes that has been taken.

(e) The information system security administrator must obtain a file to use to solve the problem of security holes such as a patch or updated software version, etc. (hereinafter referred to as “security update file”) in a reliable manner. Also, he or she must validate integrity of the security update file in the case that any validation procedure is provided.

(f) The information system security administrator must investigate and analyze measures for security holes and software configurations periodically and respond in the case that he or she finds any computers or communication equipment in an inappropriate state.

(g) The information system security officer must share the obtained information about the security holes and the measures with other information system security officers as needed.

2.1.2.2 Malware

Compliance Requirements

⑴ Building the information systems

[BASIC Requirements]

(a) The information system security officer must install antivirus software, etc. on the computers (except for the computers which do not accept any antivirus software, etc.; hereinafter the same in this section.)

(b) The information system security officer must take measures against malware by using antivirus software, etc. for all imaginable routes for the malware.

[ENHANCED Requirements]

(c) For all the routes assumed for malware, the information system security officer must install antivirus software etc. of different manufacturers in combination.

(d) The information system security officer must take measures to prevent malware from spreading by communications.

⑵ Operating the information systems

[BASIC Requirements]

(a) The information system security administrator must try to collect information about malware and decide whether any response is required, and instruct the employees to take measures as needed.

(b) The information system security officer must confirm the status of malware measures as necessary for review.

2.1.2.3 Denial of Service Attacks

Compliance Requirements

(1) Building the information systems

[BASIC Requirements]

(a) For the information systems which handle available information (limited to information systems with computers, communication equipment or communication lines accessed via the Internet; hereinafter the same in this section), the information system security officer must use the functions provided on the computers and communication equipment that are necessary to provide services to protect against denial of service attacks.

【[ENHANCED Requirements]

(b) The information system security officer must build the information system so that the impact would be minimized in the case that a denial of service attack occurs.

(c) For the information systems which handle available information, the information system security officer must identify the monitoring scope and define the monitoring procedure and monitoring records' management period for the computers, communication equipment, or communication lines which suffer denial of service attacks.

(d) For the information systems that handle available information, the information system security officer must introduce any countermeasure device necessary to eliminate or mitigate the impact of denial of service attacks on the computers, communication equipment, or communication lines.

(e) For the information systems that handle available information, the information system security officer must maintain effective measures to protect against denial of service attacks.

(f) For the information systems that handle available information, the information system security officer must install the computers, communication equipment or communication lines that are required to provide services in a redundant configuration.

(g) For the information systems which handle available information, the information system security officer must consider that computers and communication equipment cannot protect from a denial of service attack caused by large-scale access and establish a response procedure and correspondence procedure in cooperation with the service provider of the communication lines which are connected to the Internet when denial of service attacks occur.

⑵ Operating the information systems

[ENHANCED Requirements]

(a) For the information systems that handle available information, the information system security administrator must monitor the computer, communication equipment, and communication line in accordance with the monitoring procedure and keep the monitoring record.

2.1.2.4 Stepping stone

Compliance Requirements

⑴ Building the information systems

[BASIC Requirements]

(a) The information system security officer must take measures to prevent the information systems (limited to information systems with computers, communication equipment or communication lines connected to communication lines extending out of the government facility such as Internet-related lines; hereinafter the same in this section) from being used as a stepping stone.

(b) The information system security officer must build the information system so that the impact would be minimized in the case that the information system is used as a stepping stone.

[ENHANCED Requirements]

(c) The information system security officer must define the monitoring procedure to monitor whether the information system is being used as a stepping stone or not and the retention period of the monitoring records.

⑵ Operating the information systems

[ENHANCED Requirements]

(a) The information system security administrator must monitor the information system in accordance with the monitoring procedure and keep the monitoring record.

Chapter 2.2 Measures for Components of Information Systems

2.2.1 Facilities and Environment

2.2.1.1 The secure area where computers and communication equipment are located

Compliance Requirements

(1) Managing entry and exit

[BASIC Requirements]

(a) The information system security officer must take measures to prevent suspicious individuals from entering the secure area.

(b) For the information systems that handle classified information, the information system security officer must physically isolate the secure area and take measures to manage entry and exit.

[ENHANCED Requirements]

(c) The information system security officer must take measures to authenticate the persons who enter the secure area.

(d) The information system security officer must take measures to authenticate the persons who exit the secure area.

(e) The information system security officer must take measures to prohibit the authenticated persons from letting unauthenticated persons enter or exit the secure area.

(f) The information system security officer must establish the procedure to approve the persons who enter the secure area continuously. It is also required to provide the record information including the person’s name, department, approved entry date, entry period, and rationale.

(g) In the case that there are any changes in the persons who have gained approval of entering the secure area, the information system security officer must update the above document with the changes. Also, he or she must record these changes.

(h) The information system security officer must take measures to record and monitor all entries to and exits from the secure area.

(2) Managing the visitors and delivery personnel

[ENHANCED Requirements]

(a) In the case that there is any visitor to the secure area, the information system security officer must take measures to confirm the name, department, purpose of the visit, and the name and department of the employee who receives the visit.

(b) In the case that there is any visitor to the secure area, the information system security officer must take measures to record the name, department and purpose of the visit, the name and department of the employee who receives the visit, the date of the visit, and the time of entry and exit.

(c) In the case that there is any visitor to the secure area, the information system security officer must establish the procedure by which the visited employee examines whether the visitor may enter the secure area.

(d) The information system security officer must take measures to limit the area where the visitors can enter.

(e) The information system security officer must take measures so that the visited employee attends to the visitor in the secure area.

(f) The information system security officer must take continuous measures to identify the visitors and the persons who have obtained approval of entering by appearance.

(g) In the case that exchange of items with delivery personnel occurs, the information system security officer must set either requirements:

  (i) Such exchange must be done outside the secure area.

  (ii) In the case that the delivery personnel enter the secure area, such exchange must be done in the area where computers, communication equipment, and storage media cannot be touched and the employee must be in attendance.

⑶ Securing the computers and communication equipment

[BASIC Requirements]

(a) For the information systems that handle classified information, the information system security officer must take measures to prevent the stealing or illegal moving of the computers to be located and used at a specific location.

[ENHANCED Requirements]

(b) For the information systems that handle classified information, the information system security officer must isolate computers and communication equipment from other information systems physically and not locate them in the same secure area.

(c) For the information systems that handle classified information, the information system security officer must take measures to prevent the stealing or illegal moving of the communication equipment to be located and used at a specific location.

(d) The information system security officer must take measures to protect the computers and communication equipment against illegal operation while the employee is away from them.

(e) For the information systems that handle confidential information, the information system security officer must take measures to protect the display of computers and communication equipment from others' eyes.

(f) For the information systems that handle confidential information, the information system security officer must take measures to protect the cables including power cables and communication cables used in the information systems against threats including damage and sniffing.

(g) For the information systems that handle confidential information, the information system security officer must take measures against information leakage caused by electronic waves.

(4) Managing security in the secure area

[BASIC Requirements]

(a) The employee must always keep his or her ID badge visible to other employees in the secure area.

[ENHANCED Requirements]

(b) The employee must bring the items used in the information systems that handle classified information into or out of the secure area after gaining approval from the information system security officer.

(c) The information system security officer must record the bringing into or out of the secure area of items used in the information systems that handle classified information.

(d) For the information systems which handle confidential information, the information system security officer must restrict bringing computers, communication equipment, electronic storage media, and recording devices (including the ones to record voice, video, and image) that are not used in the information systems into the secure area.

(e) The information system security officer must take measures to monitor the work done in the secure area.

(5) Measures against disasters and failures

[ENHANCED Requirements]

(a) For the information systems that handle vital information, the information system security officer must take physical measures to protect computers and communication equipment against natural and human-induced disasters.

(b) For the information systems which handle vital information, the information system security officer must take measures to stop power feeding to the computers and communication equipment as needed as well as assure the security of workers in the case that any disaster or failure occurs in the secure area.

2.2.2 Computers

2.2.2.1 Common Measures for Computers

Compliance Requirements

⑴ Installing the computers

[BASIC Requirements]

(a) The information system security officer must consider and ensure the system performance, including the future perspective, which will be required for the computer to handle the available information.

(b) For the information systems that handle classified information, the information system security officer must locate the computer in a secure area. However, this is not required for mobile PCs in the case that he or she gains approval from the information security officer.

[ENHANCED Requirements]

(c) For the computers that handle available information, the information system security officer must install the computers that are required to provide services in a redundant configuration.

⑵ Operating the computers

[BASIC Requirements]

(a) The employee must not use the computers for the purpose other than executing his or her tasks.

[ENHANCED Requirements]

(b) The information system security officer must periodically examine the state of each item of software used on the computers within his or her control and make improvements if any computers are found to be in an inappropriate state.

⑶ Disposing of the computers

[BASIC Requirements]

(a) In the case that the information system security officer disposes of the computers, he or she must delete all the information stored in the electronic storage media of the computer.

2.2.2.2 Terminals

Compliance Requirements

⑴ Installing the terminals

[BASIC Requirements]

(a) The information system security officer must define a list of software that may be used for the terminals. However, in the case that it is difficult to list the allowed software, he or she can list the denied software or list both of the allowed and the denied software.

(b) The information system security officer must enable the protection measures in the mobile PCs that handle classified information to be used outside the government agency so that they can operate with the same protection measures as the terminals to be used inside the government agency.

(c) The employee must gain approval from the information system security officer in the case that he or she needs to use a mobile PC.

(d) The information system security officer must provide the encryption for the information to be stored in electronic storage media for mobile PCs which contains confidential information.

(e) The information system security officer must define the measures to prevent theft for the mobile PCs that handle classified information.

[ENHANCED Requirements]

(f) The information system security officer must build the information systems using the terminals that do not allow the employees to save the information.

⑵ Operating the terminals

[BASIC Requirements]

(a) The employee must not use any other software than that which he or she is allowed to use on the terminal.

(b) In the case that the employee uses the mobile PCs that handle classified information, he or she must take measures to prevent theft.

(c) For the mobile PCs that handle confidential information, in the case that the employee takes the mobile PCs outside the government agency, he or she must consider whether encrypting the confidential information saved in the electronic storage media of the mobile PC is required and if it is required, then he or she must encrypt it.

(d) The employee must not connect his or her terminal to communication lines other than those to which the information system security officer has given approval for connecting.

[ENHANCED Requirements]

(e) The information system security administrator must synchronize the terminal time with the standard time in the information systems.

2.2.2.3 Server Devices

Compliance Requirements

⑴ Installing the servers

[BASIC Requirements]

(a) In the case that the information system security officer maintains the server via a communication line, he or she must consider whether encrypting the send or received information is required and if it is required, he or she must encrypt it.

(b) The information system security officer must define the software to be used to provide services and to operate and manage the servers.

(c) In the case that the information system security officer finds that any server application that is not included in the allowed software is running, he or she must stop the relevant server application. Also, even in the case that the server application is included in the allowed software, he or she must disable the functions that are not used.

[ENHANCED Requirements]

(d) The information system security officer must uninstall any software that is not included in the allowed software from the servers.

(e) The information system security administrator must distribute loads to multiple servers or make it redundant for those which required for providing services, among the servers for the available information.

⑵ Operating the servers

[BASIC Requirements]

(a) The information system security officer must confirm the changes in the configulation of servers periodically. Also, he or she must identify the impact of the changes on the servers and take measures.

(b) The information system security administrator must take necessary measures to restore the servers that handle avaiable information.

(c) The information system security administrator must record the information including the date of work, the server, the work description, and the worker for the operation and management of the server.

(d) The information system security administrator must synchronize the time of servers with the standard time of the information systems.

[ENHANCED Requirements]

(e) The information system security administrator must monitor the security state of the servers to detect any events including illegal activities or use.

(f) For the servers that handle available information, the information system security administrator must monitor the system status of the relevant server to detect any failures, etc.

2.2.3 Application Software

2.2.3.1 E-mail

Compliance Requirements

⑴ Introducing e-mail service

[BASIC Requirements]

(a) The information system security officer must configure the e-mail servers so that unsolicited bulk e-mail cannot be relayed.

(b) The information system security officer must provide the function for authentication of an employee when the e-mail sending and receiving to or the email server.

⑵ Operating e-mail service

【[BASIC Requirements]

(a) In the case that the employee sends or receives e-mail messages that contain information that is related to business, he or she must use the e-mail service provided by the e-mail server that is operated or outsourced by each government agency that he or she belongs to. However, this is not always required if he or she has gained approval for information processing in unsupplied information systems.

(b) The employee must display indicate the contents of an e-mail upon receipt to prevent the script from being operated by a computer.

2.2.3.2 Web

Compliance Requirements

⑴ Introducing the Web

[BASIC Requirements]

(a) In the case that the users enter strings, etc. in the services provided using the Web servers, the information system security officer must sanitize input data.

(b) The information system security officer must build the information systems so that the Web servers do not send to the Web clients any information that could be utilized in attacks.

(c) For the information systems which handle confidential information, the information system security officer must identify the information to protect against sniffing and consider whether encryption is required. If it is required, then must encrypt the information for the services provided using the Web servers.

[ENHANCED Requirements]

(d) For the information systems that handle confidential information, the information system security officer must identify the information to be stored on the Web servers and confirm that the relevant servers do not contain any confidential information.

(e) The information system security officer must use the digital certification to ensure the validity of Web servers.

⑵ Operating the Web

[BASIC Requirements]

(a) The employee must make the security settings of the web client properly to ensure the information security.

(b) In the case that the employee downloads software to the computers on which a Web client is running, he or she must confirm the source of the software using an electronic signature.

(c) The employee must confirm the following if he or she uploads confidential information to an online form with a website view.

(i) The information to be sent must be encrypted.

(ii) The website viewed must be provided by an organization assumed to be of the receiver of the information.

[ENHANCED Requirements]

(d) The information system security officer must limit the Web pages from outside the government agency that the employees can browse and review the limit periodically.

2.2.3.3 Domain Name System（DNS）

Compliance requirements

⑴ Introduting of DNS

[BASIC Requirements]

(a) The information system security officer must take measures to prevent the name solution from the DNS server to provide of the information system for available information.

(b) The information system security officer must define a procedure to operate and manage the domain information saved in the DNS server.

(c) The information system security officer must take measures not to respond to the name solution from outside of the government agencies but only respond to the solutions from in-house, on the DNS cache server.

(d) The information system security officer must take measures to prevent information leakage of the name solution to be used only in the government agencies on the DNS server.

[ENHANCED Requirements]

(e) The information system security officer must provide the electronic signature to the provided name solution related domain information on the DNS server that have the critical information system.

⑵ Operating the DNS

[BASIC Requirements]

(a) The information system security officer must maintain consistency of domain information between different DNS servers when there are configured multiple servers.

(b) The information system security officer must verify the domain information is correct according to the procedure to operate and manage the domain in control on the DNS server as necessary.

2.2.4 Communication Lines

2.2.4.1 Common Measures for Communication Lines

Compliance Requirements

(1) Building communication lines

[BASIC Requirements]

(a) In the case that the information system security officer builds a communication line, he or she must consider the risks in doing so.

(b) For the information systems that handle vital information, the information system security officer must consider and ensure the system capabilities to provide performance required for the relevant communication lines and communication equipment for the future.

(c) The information security officer must define the software necessary for communication equipment to be operated. However, this is not required in the case of communication equipment for which it is difficult to change software.

(d) The information system security officer must group the computers that are connected with the communication line and separate them on that communication line.

(e) The information system security officer must consider the communication requirements among the grouped computers and use the communication equipment and provide access control and route control in accordance with the communication requirements.

(f) The information system security officer must consider if it is necessary to encrypt the confidential information to be sended or received through the communication line for the information system to handle confidential information. If it is confirmed to be necessary, the encryption function must be provided.

(g) For the information systems that handle classified information, the information system security officer must consider the security of physical lines used for the communication line and select appropriate ones.

(h) The information system security officer must ensure security of the connections that are used in the services for remote maintenance or diagnosis work for the communication equipment.

(i) The information system security officer must locate the communication equipment in the secure area.

(j) In the case that a private line service provided by a carrier is used, the information system security officer must stipulate the items including security and service levels in the agreement.

[ENHANCED Requirements]

(k) The information system security officer must authenticate the communicating computers.

(l) For the information systems that handle vital information, the information system security officer must install the communication line or communication equipment that is required to provide the services in a redundant configuration.

⑵ Operating the communication line

[BASIC Requirements]

(a) In the case that the information system security administrator changes the software of the communication equipment, he or she must obtain approval from the information system security officer.

(b) For the management of operation of communication lines and communication equipment, the information system security administrator must record matters such as operated communication lines and communication equipment, the date and contents of the operation, and operators.

(c) In the case that security of the information system is difficult to ensure for any reason, the information system security officer must change the communication line from the shared configuration to the independent and closed configuration.

(d) The employee must not connect computers and communication equipment that are not approved by the information system security officer to the communication line.

(e) The information system security administrator must synchronize the time of the communication equipment with the standard time of the information systems.

[ENHANCED Requirements]

(f) The information system security officer must periodically examine the conditions of all the software necessary for the operation of communication equipment which he or she is responsible for, and when any equipment under inappropriate conditions is found, then he or she must work to improve the relevant inappropriate conditions. However, this is not required in the case of communication equipment for which it is difficult to change software.

⑶ Disposing of the communication lines

[BASIC Requirements]

(a) In the case that the information system security officer disposes of the communication equipment, he or she must delete all the information stored in the electronic storage media of the communication equipment.

2.2.4.2 Management of Communication Lines in the Government Facilities

Compliance Requirements

⑴ Building the communication lines in the government agencies

[ENHANCED Requirements]

(a) The information system security officer must take measures to confirm that the computers that are physically connected with the communication equipment have gained approval for connecting with the communication line before they are logically connected with the communication line.

⑵ Operating the communication line in the government agency

[ENHANCED Requirements]

(a) The information system security officer must review the configurations of access control when he or she changes the communication requirements and periodically.

(b) For the information systems that handle vital information, the information system security administrator must confirm and analyze the utilization and state of the communication line daily to measure or detect any degradation or abnormality in the communication line.

(c) The information system security administrator must monitor the information that is sent or received via the communication line in the government agency.

⑶ Measures on the lines

[BASIC Requirements]

(a) In the case that the information system security officer builds the VPN environment, he or she must consider whether measures including the following are required and if it is required, then he or she must take any of such measures.

   (i) Establishing the procedures to start or stop using the VPN environment
   (ii) Encrypting the information
   (iii) Identifying the communicating computers or authenticating the users
   (iv) Obtaining and managing the authentication records
   (v) Limiting the scope of communication lines which are accessible via VPN
   (vi) Assuring the confidentiality in the VPN connection method
   (vii) Managing the computers which use VPN

(b) In the case that the information system security officer builds the wireless LAN environment, he or she must consider whether measures it is necessary, as below, and take measures if it is required. In this case, the encryption of the data on the communication line in the wireless LAN environment for confidential information.

   (i) Establishing the procedures to start or stop using the LAN environment
   (ii) Encrypting the information
   (iii) Identifying the communicating computers or authenticating the users
   (iv) Obtaining and managing the authentication records
   (v) Limiting the scope of communication lines which are accessible via wireless VPN
   (vi) Prohibiting connection with another communication line while connecting with the wireless LAN
   (vii) Assuring the confidentiality in the wireless LAN connection method
   (viii)Managing the computers which connect with the wireless LAN

(c) In the case that the information system security officer builds the remote access environment via the public telephone network, he or she must consider whether measures including the following are required and if it is required, then he or she must take any of such measures.

   (i) Establishing the procedures to start or stop using the remote access environment
   (ii) Identifying and authenticating the communicating users or caller numbers
   (iii) Obtaining and managing the authentication
   (iv) Limiting the scope of communication lines which are accessible by remote access
   (v) Prohibiting connecting with another communication line while accessing remotely
   (vi) Assuring confidentiality in the remote access method
   (vii) Managing the computers which access remotely

2.2.4.3 Connecting with Communication lines outside the Government Agency

Compliance Requirements

(1) Connecting the communication lines inside the government agency and the communication

lines outside the government agency

[BASIC Requirements]

(a) The information system security officer must gain approval from the information security officer to connect a communication line inside the government agency with a communication line outside the government agency.

(b) In the case that the information security officer decides that the security of the information systems cannot be ensured when the communication line in the government agency's is connected with a communication line outside the government agency, he or she must change the communication line inside the government agency or the communication line outside the government agency from the shared configuration to the independent configuration.

⑵ Operating a communication line inside the government agency which is connected with a communication line outside the government agency

[BASIC Requirements]

(a) In the case that the information system security officer decides that security of the information systems cannot be ensured when a communication line in the government agency is connected with a communication line outside the government agency, he or she must change the communication line inside the government agency or the communication line outside the government agency from the shared configuration to the independent configuration.

(b) The information system security officer must review the configurations for access control when he or she changes the communication line and periodically.

(c) For the information systems that handle vital information, the information system security administrator must confirm and analyze the utilization and state of communication lines daily to measure or detect degradation or abnormality in the communication line.

(d) The information system security administrator must monitor the information that is sent or received via the communication lines in the government agency.

Chapter 2.3 Measures for Individual Consideration

2.3.1 Miscellaneous

2.3.1.1 Measures in Introducing IPv6 technology to Information Systems

Compliance Requirements

⑴ Vulnerability caused by mechanism for IPv6 transfer

[BASIC Requirements]

(a) In the case that the information system security officer introduces communications utilizing IPv6 technology (hereinafter referred to as "IPv6 communications") to the information systems, he or she must take necessary measures to prevent mechanism for the IPv6 transfer from posing any threat to information security.

⑵ Prevention and monitoring of unintended IPv6 communications

[BASIC Requirements]

(a) For all computers and communication equipment connected to communication lines for which IPv6 communications are not intended, the information system security officer must take measures to prevent IPv6 communications.

[ENHANCED Requirements]

(b) The information system security officer must monitor communication lines for which IPv6 communications are not intended, and when any IPv6 communications are detected, he or she must identify the equipment and take necessary measures to cut off the IPv6 communications.