NISD-K304-101

Management Standards for Information Security Measures for the Central Government Computer Systems

April 21, 2011

Established by the Information Security Policy Council

Table of Contents

Chapter 1.1 General 1
1.1.1.1 Positioning of Management Standards for Measures 1
(1) Positioning of these Management Standards for Measures as an enhancement of Information Security Measures for the Central Government Computer Systems 1
(2) Revision of these Management Standards for Measures and the Technical Standards for Measures 1
(3) Compliance with laws and regulations 1
1.1.1.2 How to use Management Standards for Measures and Technical Standards for Measures 2
(1) Structure 2
(2) Itemized measures 3
(3) Setting security levels 3
1.1.1.3 Classification of Information and Types of Marking 4
(1) Classification and marking 4
(2) Classification 4
(3) Types of marking 6
1.1.1.4 Evaluation Procedure 6
1.1.1.5 Definition of Terms 7
Chapter 1.2 Establishment of Organizations and Systems 12
1.2.1 Introduction 12
1.2.1.1 Establishment of Organizations and Systems 12
Compliance Requirements 12
(1) Designating the chief information security officer 12
(2) Designating the Information Security Committee 12
(3) Designating the chief information security auditor 12
(4) Designating information security officers 12
(5) Designating information system security officers 13
(6) Designating information system security administrators 13
(7) Designating division/office information security officers 14
(8) Designating the chief information security advisor 14
1.2.1.2 Assignment of Roles 14
Compliance Requirements 14
(1) Defining roles that must not be concurrently undertaken by the same person 14
(2) Approval or permission by superiors 14
1.2.1.3 Violation and Exceptional Measures 15
Compliance Requirements 15
(1) Handling violations 15
(2) Exceptional measures 15
1.2.2 Operations 17

1.2.2.1 Education for Information Security Measures 17
Compliance Requirements 17
(1) Enforcement of Education for information security measures 17
(2) Participation in Education for information security measures 17
1.2.2.2 Failure Handling 18
Compliance Requirements 18
(1) Preparation for possible failure 18
(2) Reporting and emergency measures in the event of failure, accidents, etc. 19
(3) Investigating the cause of failure, accidents, etc. and preventing recurrence 19
1.2.3 Evaluation 20
1.2.3.1 Self-assessment of Information Security Measures 20
Compliance Requirements 20
(1) Formulating an annual plan for self-assessment 20
(2) Preparing for self-assessment 20
(3) Conducting self-assessment 20
(4) Evaluating the result of self-assessment 20
(5) Making improvements based on self-assessment 20
1.2.3.2 Audit of Information Security Measures 21
Compliance Requirements 21
(1) Formulating audit plans 21
(2) Instructing information security audits 21
(3) Formulating audit plans for individual business operations 21
(4) Preparation for information security audits 21
(5) Conducting information security audits 21
(6) Responding to audit results 22
1.2.4 Review 23
1.2.4.1 Review of Information Security Review Measures 23
Compliance Requirements 23
(1) Reviewing information security measures 23
1.2.5 Others 24
1.2.5.1 Outsourcing 24
Scope 24
Compliance Requirements 24
(1) Establishing a common system among government agencies for information security 24
(2) Clarifying required information security measures to contractors 24
(3) Selecting contractors 25
(4) Outsourcing contracts 25
(5) Outsourcing procedures 26
(6) Procedures for the contract expiry 26
1.2.5.2 Consistently Operarion with Business Continuity Plan 26

Scope....26
Compliance Requirements....26
(1) Ensuring consistently between BCP and information security measures....26
(2) Reporting inconsistency between BCP and information security rules....27
Chapter 1.3 Measures for Information....28
1.3.1 Information Handling....28
1.3.1.1 Creation and Obtain of Information....28
Compliance Requirements....28
(1) Prohibiting creation or obtainment of non-business information....28
(2) Classification and marking at creation or obtainment of information....28
(3) Labeling classification and marking....28
(4) Succession of classification and marking at processing....28
1.3.1.2 Use of Information....28
Compliance Requirements....28
(1) Prohibiting the non-business use....28
(2) Handling information according to the classification and marking....29
(3) Succession of classification and marking at copying....29
(4) Reviewing classification and marking....29
(5) Handling classified information....29
1.3.1.3 Save of Information....30
Compliance Requirements....30
(1) Storing information according to the classification....30
(2) Information retention period....30
1.3.1.4 Transfer of Information....30
Compliance Requirements....30
(1) Approving and notifying information transfer....30
(2) Selecting from information transmission or transport....31
(3) Selecting the means of transfer....31
(4) Protecting storage media....31
(5) Protecting electromagnetic records....31
1.3.1.5 Provision of Information....32
Compliance Requirements....32
(1) Disclosing information....32
(2) Providing information to others....32
1.3.1.6 Deletion of Information....33
Compliance Requirements....33
(1) Deletion of electromagnetic records....33
(2) Disposing of written documents....33
Chapter 1.4 Measures for Information Processing....34
1.4.1 Use of Information Systems....34

1.4.1.1 Use of Information Systems....34
Compliance Requirements....34
(1) Managing identification codes....34
(2) Managing authentication information....34
(3) Granting and managing identification codes and authentication information....35
(4) Applying an alternative method for identification codes and authentication information....35
1.4.2 Restrictions on Information Processing....36
1.4.2.1 Restrictions on Information Processing outside Government Facilities....36
Compliance Requirements....36
(1) Establishing rules for safeguard....36
(2) Obtaining and managing approval and application....36
(3) Observing rules for safeguard....37
1.4.2.2 Restrictions on Information Processing Using Unsupplied Information Systems....38
Compliance Requirements....38
(1) Establishing rules for safeguard....38
(2) Obtaining and managing approval and application....38
(3) Observing rules for safeguard....38
Chapter 1.5 Basic Measures for Information Systems....40
1.5.1 Security Requirements for Information Systems....40
1.5.1.1 Security Requirements for Information Systems....40
Compliance Requirements....40
(1) Planning information systems....40
(2) Implementing and operating information systems....41
(3) Migrating and disposing information systems....41
(4) Reviewing information systems....41
1.5.2 Maintenance and Observance of Information System Rules....42
1.5.2.1 Maintenance of Documents and Inventories of Information Systems....42
Compliance Requirements....42
(1) Maintaining documents of information systems....42
(2) Maintaining inventories of information system....42
1.5.2.2 Procurement of Equipment, etc.....43
Scope....43
Compliance Requirements....43
(1) Establishing rules concerning procurement of equipment, etc.....43
(2) Observing rules concerning procurement of equipment, etc.....44
1.5.2.3 Software Development....44
Compliance Requirements....44
(1) Establishing rules concerning software development....44
(2) Observing rules concerning software development....45

1.5.2.4 Standard Procedure for Authentication, Access Control, Administration, Audit Trail Management, Assurance, etc. 45
Compliance Requirements 45
(1) Establishing Management concerning authentication, access control, administration, audit trail Management, assurance, etc. 45
(2) Observing rules concerning authentication, access control, administration, audit trail management, assurance, etc. 46
(3) Examining, analyzing, and reporting on obtained audit trails 46
1.5.2.5 Standard Procedure for Encryption and Electronic Signatures 47
Compliance Requirements 47
(1) Establishing rules concerning encryption and electronic signatures 47
(2) Observing rules concerning encryption and electronic signatures 47
1.5.2.6 Preventing Actions that Compromise the Information Security Level outside Government Agencies 48
Compliance Requirements 48
(1) Establishing rules for measures 48
(2) Observing the rules 48
1.5.2.7 Measures for the Use of Domain Names 48
Compliance Requirements 48
(1) Establishing rules for the use of domain names 48
(2) Observing rules for the use of domain names 49
1.5.2.8 Day-to-day Measures for Protection against Malware 49
Compliance Requirements 49
(1) Establishing rules concerning measures against malware 49
(2) Observing rules concerning measures against malware 50

Chapter 1.1 General

1.1.1.1 Positioning of Management Standards for Measures

(1) Positioning of these Management Standards for Measures as an enhancement of Information Security Measures for the Central Government Computer Systems

As a general rule, 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 standard of information security across all government agencies based on the "Information Security Standards for Government Agencies (stipulated by the Information Security Committee on April 21, 2011)" in order to reinforce information security measures of the whole government. These Management Standards for Measures and the Technical Standards for Measures prescribe measures which government agencies should take to assure and further improve information security within the unified framework of government agencies.

(2) Revision of these Management Standards for Measures and the Technical Standards for Measures

It is important to understand changes in circumstances precisely and review information security measures in order to maintain an appropriate level of information security. It is considered necessary that these Management Standards for Measures and the Technical Standards for Measures to be added and amended as they are used by each government agency for formulating its own standards and operational procedures according to its characteristics and for evaluating information security measures. Depending on the advancement of information technologies, information security measures prescribed in these Management Standards may also have to be changed.

Therefore, these Management Standards are periodically reviewed and enhanced as necessary to maintain their validity in the future. Each government agency must reflect changes made in these Management Standards for Measures and the Technical standards for Measures to their own standards appropriately.

(3) Compliance with laws and regulations

When taking information security measures, laws and regulations which stipulate handling of information and information systems (hereinafter referred to as "relevant laws and regulations") in addition to these Management Standards and Technical Standards. These Management Standards for Measures and the Technical Standards for Measures to not reference to these relevant laws and regulations since they must be observed regardless of information security measures. Also, the existing government's resolutions concerning information security measures must be observed.

1.1.1.2 How to use Management Standards for Measures and Technical Standards for Measures

(1) Structure

These Management Standards for Measures are comprised of three levels; chapter, section and item.

These Management Standards for Measures define the guidelines to be observed when developing organizations and systems to promote information security measures for the entire organization, establishing information security measures on each phase of information lifecycle, and establishing rules concerning information systems. Whereas the Technical Standards for Measures describe technical issues and define security requirements required to information systems; therefore, these will be reviewed more frequently.

Chapters in These Management Standards for Measures are "General", "Developing Organizations and Systems", "Measures for Information", "Measures for Information Processing", and "Basic Measures for Information Systems", whereas the Technical Standards for Measures contain "Measures Based on Information Security Requirements", "Measures for Information System Components", and "Measures for Individual Issues".

Each chapter consists of sections for measure items, and each section also consists of items for standards for the measures. The following describes the specific contents.

(a) Chapter 1.1 General

(b) Chapter 1.2 Developing Organizations and Systems

"Developing Organizations and Systems" in these Management Standards for Measures defines subjects such as implementation systems, assessment procedures, violations, and exceptions to clarify authority and responsibility of concerned employees when implementing information security measures on the entire organization.

(c) Chapter 1.3 Measures for Information

"Measures for Information" in these Management Standards for Measures focuses information lifecycle such as its creation, use, storage, transportation, provision, and deletion, and defines what employees should always do to protect information in each phase.

(d) Chapter 1.4 Measures for Information Processing

"Measures for Information Processing" in these Management Standards for Measures defines what should be done when using information systems, and what should be restricted when processing information outside the government agencies or using externally supplied information systems.

(e) Chapter 1.5 Basic Measures for Information Systems

"Basic Measures for Information Systems" in these Management Standards for Measures defines what should be done in each phase of the information system lifecycle such as planning, implementation, operation, migration, disposal, and review, and rules to assure information security concerning information systems to ensure rules prescribed in the

Technical Standards for Measures are appropriately adhered.

(f) Chapter 2.1 General

(g) Chapter 2.2 Measures based on Clarifying Information Security Requirements
"Measures Based on Information Security Requirements" in the Technical Standards for Measures explains security functions which should be implemented in information systems such as access control, and defines what should be done to protect information systems from threats such as security holes, malware, and denial of service attacks.

(h) Chapter 2.3 Measures for Information System Components
"Measures for Information System Components" in the Technical Standards for Measures defines what should be done for information systems from the viewpoint of characteristics and lifecycle of information systems such as computer and communication lines.

(i) Chapter 2.4 Measures for Individual Issues
"Measures for Individual Issues" in the Technical Standards for Measures focuses individual information security issues in implementation of new technologies that require particular considerations, and defines the guidelines.

(2) Itemized measures

These Management Standards for Measures and the Technical Standards for Measures set itemized compliance requirements for measures each government agency should take.

(3) Setting security levels

The required information security measures vary depending on importance of the information asset and seriousness of the threat. Also, intensity of measures should be determined according to the characteristics of given information system and its purposes. Therefore, these Management Standards for Measures and the Technical Standards for Measures define the intensity of measures and guidelines for each target item. This intensity is represented by "security levels" and they are defined as follows:

(a) "BASIC Requirements" are measures which must be taken for the given information and the information systems which handle the information

(b) "ENHANCED Requirements" are measures which should be taken for especially important information and the information systems which handle the information if the respective government agency considers necessary.

Government agencies must select an appropriate security level for each target item based on the characteristics of the given information system and purposes, with careful considerations to risks.

1.1.1.3 Classification of Information and Types of Marking

(1) Classification and marking

Handling requirements for information in government administration vary depending on the purpose and use of the information. Therefore, information is classified and marked in order to apply appropriate measures and assure information security according to its importance.

Classification and marking should be properly defined to acknowledge how the information creator or owner considers the information should be handled, and clarify the importance and required security measures of the information.

Classification and marking can also improve the information users' awareness of day-to-day information security measures. In other words, it compels employees to recognize the necessity of measures for information and information security continuously through classifying and marking information each time they create or obtain one, and taking measures according to the classification and marking each time they handle information. Therefore, employees must be notified to understand and observe the classification and marking.

(2) Classification

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

Although the following classifications are used in requirements in these Management Standards of Measures, each government agency may change or add as necessary. However, when changing or adding classifications, each government agency must confirm the relationships between classifications and requirements for given measures must be the same or higher than those described in these Management Standards for Measures and the Technical Standards for Measures. Also, when changing or adding classifications, the government agency must define the method to communicate how their own classifications correspond to those in these Management Standards for Measures and the Technical Standards for Measures when exchanging information with other government agencies. For example, the government agency may use classifications described in these Management Standards for Measures and the Technical Standards for Measures when providing information to other government agencies.

(a) The following describes information classifications for confidentiality, integrity, and availability.

Classifications for confidentiality

Classification	Description of classification
Confidentiality class-3 information	Among information for administrative use, items which are considered confidential.
Confidentiality class-2 information	Among information for administrative use, items whose disclosure may infringe citizens' rights or administrative operations although they are not considered confidential.
Confidentiality class-1 information	Information other than Confidentiality class-2 information or Confidentiality class-3 information.

Information which comes under Confidentiality class-2 information or Confidentiality class-3 information is called "confidential information".

Classifications for integrity

Classification	Description of classification
Integrity class-2 information	Among information for administrative use (except written information), items whose falsification, errors, and damage may infringe citizens' rights or correct administrative operations (except negligible cases).
Integrity class-1 information	Information other than Integrity class-2 information (except written information)

Note that Integrity class-2 is called "critical information".

Classification for availability

Classification	Description of classification
Availability class-2 information	Among information for administrative use (except written information), items whose loss or unavailability infringe citizens' rights or stable administrative operations (except negligible cases).
Availability class-1 information	Information other than Integrity class-2 information (except written information.)

Note that Availability class-2 information is called "vital information".
Also, confidential information, critical information, and vital information are collectively called "classified information".

(3) Types of marking

Information is classified from three aspects: namely confidentiality, integrity, and availability, and types of marking are defined for each aspect. "Marking" means restrictions to ensure proper handling of information such as to prohibit copying, taking out, or distribution, to oblige encryption, or to force disposal after reading.

(a) Types of marking are defined separately for confidentiality, integrity, and availability. Types of marking can be specified as appropriate.

1.1.1.4 Evaluation Procedure

Information security measures must not be transient but be continuously feasible without delay. Therefore, each government agency must carry out information security audit periodically or as necessary based on these Management Standards for Measures and the Technical Standards for Measures to confirm the following.

(a) Standards for measures implemented by the government agency comply with the Management Standards for Measures and Technical Standards for Measures. (Design compliance check)

(b) Actual operations conform to the standards for measures implemented by the government agency. (Operational compliance check)

(c) Standards for measures implemented by the government agency are appropriate for the given risks, efficient, and feasible. (Design adequacy check)

(d) Actual operations are valid and effective for the given risks. (Operational adequacy check)

The most important objective in the information security audit at government agencies is to confirm the design and operational compliance. If any design or operational adequacy issues which need improving are found as a result of the audit, they should be noted as issues for further examination. Since these Management Standards for Measures and the Technical Standards for Measures define the parson in charge and guidelines, the appointed employees should carry out self-check to confirm the status of measure application according to their roles. It is essential that each employee fulfill his or her duties for information security measures, and self-assessment is adopted to ensure effectiveness of measures. Therefore, when auditing, government agencies should examine if the self-check is appropriately carried out in order to confirm the operational conformity. If the audit finds any discrepancy between the status of measure application and the result of self-assessment, the cause of the discrepancy should be analyzed and the self-assessment should be corrected.

While each government agency is responsible for application of information security measures in general, they must report the application status and audit results to the NationalInformationSecurityCenter to facilitate information security measure promotion for the entire government organization. Also, each government agency must create an information

security report to disclose its information security status. In addition, the NationalInformationSecurityCenter must examine and assess each government agency's rules associated with information security, and the status of measure application based on the evaluation index in these Management Standards for Measures and the Technical Standards for Measures periodically or as required. The scope of applicable information systems shall be discussed and determined between the NationalInformationSecurityCenter and each government agency.

1.1.1.5 Definition of Terms

- "Access control" means to restrict objects to which a subject is allowed access.
- "Secure area" means an area inside of an office or a server room where computers and communication equipment are located, and is protected by structural and environmental measures against information security violation caused by intruders and natural disasters.
- "Transfer" → See "Information transfer"
- "Contractor" means a party who is contracted to carry out part of, or all of information processing tasks such as design, implementation, or operations of information systems.

- "Outsourcing" means contracting out part of, or all of information processing tasks such as design, implementation, or operations of information systems to a party external to government agencies.
- "Availability" means to assure a state where authorized people can access information and related assets as necessary without interruption.
- "Integrity" means to assure a state where information is not damaged, falsified, or deleted.
- "Equipment, etc." means information equipment and software.
- "Confidentiality" means a state where only authorized people can access information.
- "Employees" means legal employees (government officials who work in government agencies) and those who are under supervision of government agencies (for example, dispatched workers though it depends on individual work conditions) the municipal governments who handle information and information systems managed by the given government agency.
- "Shared identification code" means an identification code that is shared among multiple subjects. One identification code is granted to a single subject as a general rule; however, one identification code may be shared among multiple subjects due to restrictions of information systems or the way the system is used. These shared identification codes are called shared identification codes.
- "Storage media" means media in which information is recorded or written. Storage media includes written document, and any paper or other tangible objects on which information

recognizable by human such as characters or diagrams are written (hereinafter referred to as "written document"), and those on which information unrecognizable by human is recorded electronically or magnetically and are processed by computers (hereinafter referred to as "electromagnetic storage media"). The electromagnetic storage media can be internal such as ones built into computers or communication equipment, or external such as external hard disks, CD-R, DVD, MO, USB memory, and flash memory.

- "Administration" means to manage information related to authentication (including identification codes and authentication information) and access control permissions.

- "Service" means a set of functions that is composed of a single or multiple functions provided by applications running on servers to the connected computers.
- "Least privilege" means a function to restrict the range to grant administrative permission to the minimum necessary.
- "Identification" means to identify the subject accessing an information system.
- "Identification code" means a code used by an information system 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 appropriate management of the given information system and their loss or disclosure will disrupt administrative operations.
- "Subject" means a person who accesses information systems, other information systems, and devices. A subject is mainly intended to be human; however, other information systems and devices can be subjects which access information systems when multiple information systems and devices work in coordination.
- "Authentication" means to verify whether the subject who presents an identification code is the legitimate subject who is granted the identification code. Information systems authenticate the subject when an identification code is presented with authentication information in a correct manner. Although "authentication" has connotation of an official or third party testimony, it is not restricted to mans in these Management Standards for Measures and the Technical Standards for Measures.
- "Authentication information" means information that a subject presents to an information system in order to be authenticated. A password is typical authentication information.
- "Authentication information storage device" means a device that stores authentication information and is owned or carried by the legitimate subject. Information systems authenticate the subject in possession of this device in ownership-based authentication.
  An IC card is a typical authentication information storage device.
- "Standards for measures implemented by government agency" or "Standards of government agency" means information security standards which comply with these Management Standards for Measures and the Technical Standards for Measures and are applied to all information assets of the given government agency.

- "Information" means information recorded within information systems, information recorded in external electromagnetic storage media, and information on written documents related to information systems. Therefore, unfinished documents are also included. Information on written documents includes ones which describe electromagnetically recorded information (ones describing information entered into and output from information systems), and documents concerning information system design.
- "Information system" means systems for information processing and communications.
- "Information security rules" means standards for measures implemented by government agency, and the procedures which define how to apply measures prescribed in the standards to information systems and operations.
- "Information transfer" means to transmit electromagnetically recorded information and to transport electromagnetic storage media or written documents that contain information to outside the government agency.
- "Information erasure" means to make information unrecoverable in order to prevent leakage of disposed information. Information is not unrecoverable if the information can be recovered by undoing deletion or using a recovery tool.
- "Software" means procedures and commands to operate computers that are written in a form computers can understand. This includes operating systems and applications running on operating systems.

- "Terminal" means a computer that an employee directly operates (including the operating system and connected peripheral devices) such as a PC and PDA.
- "Communication line" means physical and logical mechanisms to connect computers and to communicate information using prescribed communication protocol.
- "Communication equipment" means a device connects lines and controls information exchanged between computers via lines. This includes repeater hubs, switching hubs, routers, and firewalls.
- "Computers" means computers in general such as servers and terminals including their operating systems and connected peripheral devices.
- "Marking" means restrictions to ensure appropriate handling of information such as to prohibit copying, taking out, or re-distribution, to oblige encryption, or to force disposal after reading.

- "Outside the government agency" means outside the organization or building managed by government agencies.
- "Communication line outside the government agency" means a logical communication line connecting computers that are not managed by the government agency and being used for communications between these computers regardless of the physical presentation of the line (wired or wireless, physical or virtual, under control of government agencies or third parties)

and the deployed communication equipment.

- "Information processing outside the government facility" means information processing for administrative operations carried out outside the government facilities. This can be online information processing by connecting to information systems in government agencies from outside, as well as offline processing.
- "Unsupplied information system" means information systems that are not supplied by government agencies. These include information systems on private PCs and those provided by assignor agencies for their dispatched workers.
- "Information processing using unsupplied information system" means processing information using information systems which are not supplied by government agencies for administrative operations. This includes the use of devices as well as the use of services which are provided by these devices. These services signify ones such as personally contracted e-mail services which may be used to send business e-mails or receive e-mails forwarded from e-mail services managed by government agencies.
- "Inside the government agency" means inside the organization or building managed by government agencies.
- "Communication line inside the government agency" means a logical communication line connecting computers that are managed by the government agency and being used for communications between these computers regardless of the physical presentation of the line (wired or wireless, physical or virtual, under control of government agencies or third parties) and the deployed communication equipment.
- "Malware" means software in general which causes unsolicited results to computers such as computer viruses and spyware.
- "Malware definition file" means the data which antivirus software, etc. uses to distinguish malware.

- "Erasure" → See "Information erasure"
- "Labeling, etc." means to make information's classification clear to all who handle the information. This means to display the classification on information in general; however, any other acts to make information's classification common knowledge are also included. For example, acknowledging all users of a specific information system by describing classification of the information recorded in the system in a regulation is also included.

- "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 to take alternative measures for appropriate business continuity when there is a justifiable reason not to take prescribed measures such as the situation does not allow the responsible employees to comply with the relevant information security rules. Exceptional measures must be applied and approved.
- "Login" means an act where a subject requests authentication. Because login is followed by authentication, legitimacy of the subject is unknown at the login stage.
- "Logon" means the state where the subject who requested authentication has been authenticated by the information system as a result of login.

Chapter 1.2 Establishment of Organizations and Systems

1.2.1 Introduction

1.2.1.1 Establishment of Organizations and Systems

Compliance Requirements

(1) 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 tasks associated with information security measures in the government agency.

(2) Designating the Information Security Committee

[BASIC Requirements]

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

(b) The Information Security Committee must formulate standards of the government agency complying with the Management Standards for Measures and obtain approval from the chief information security officer.

(3) Designating the chief information security auditor

[BASIC Requirements]

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

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

(4) Designating information security officers

[BASIC Requirements]

(a) The chief information security officer must determine management units for implementing information security measures and designate an information security officer for each unit. A head of information security officers must be designated to direct these information security officers.

(b) The head of information security officers must formulate technical standards for information security standards of government agency based on the Technical Standards for Measures under the direction of the head of information security officers. This formulation can be delegated to a person appointed by the chief information security officer.

(c) Information security officers must direct administrative tasks associated with information security measures in the given unit.
(d) The head of the information security officers must develop administrative procedures for information security measures at the start and end of employment, and personnel changes.
(e) Information security officers must periodically ensure that administrative procedures for information security measures at the start and end of employment, and personnel changes are adhered.
(f) The chief information security officer must report designation and change of any information security officers to the head of information security officers.
(g) The head of information security officers must establish a communication network for all information security officers.

⑸ Designating information system security officers

[BASIC Requirements]

(a) Information security officers must designate an information system security officer for each information system in the given unit by the planning phase of the information system.
(b) The information system security officer must direct administrative tasks associated with information security measures for the given information systems.
(c) The information security officer must report designation and change of any information system security officers to the head of information security officers.
(d) The head of information security officers must establish a communication network for all information system security officers.

⑹ Designating information system security administrators

[BASIC Requirements]

(a) Information system security officers must designate an information system security administrator for each unit required for the administrative tasks for the given information system.
(b) Information system security administrators must implement information security measures for the given unit of administrative tasks.
(c) Information system security officers must report designation and change of any information system security administrators to the head of information security officers.
(d) The head of information security officers must establish a communication network for all information system security administrators.

(7) Designating division/office information security officers

[BASIC Requirements]

(a) Information security officers must designate a division/office information security officer for each division or office.

(b) Division/office information security officers must direct administrative tasks associated information security measures in the given division or office.

(c) Information security officers must report designation and change of any division/office information security officers to the head of information security officers.

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

(8) Designating the chief information security advisor

[BASIC Requirements]

(a) The chief information security officer must designate a chief information security advisor with expertise and experience in information security.

(b) The chief information security officer must specify job descriptions of the chief information security advisor for application of information security measures.

1.2.1.2 Assignment of Roles

Compliance Requirements

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

[BASIC Requirements]

(a) Employees must not undertake the following roles concurrently in information security operations.

(i) The person who submits the application and the person who approves the application (hereinafter referred to as "approval authority, etc.".)

(ii) The person who is audited and the person who audits.

(2) Approval or permission by superiors

[BASIC Requirements]

(a) Employees must apply for approval of the superior of the approval authority, etc. when they consider it 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, approval from the approval authority, etc. is not required after obtaining approval from the superior of the approval authority, etc.

(b) After granting approval in the above case, the employee must take necessary measures in accordance with requirements for approval authority, etc.

1.2.1.3 Violation and Exceptional Measures

Compliance Requirements

(1) Handling violations

[BASIC Requirements]

(a) Employees must report to the responsible information security officer when they become aware of any serious breach of information security rules.

(b) The information security officer must instruct the violator and concerned parties to take necessary measures to maintain information security when he/she is informed of, or becomes aware of any serious breach of information security rules.

(c) The information security officer must report to the chief information security officer when he/she is informed of, or becomes aware of any serious breach of information security rules.

(2) Exceptional measures

[BASIC Requirements]

(a) The Information Security Committee must designate a person who judges whether to approve applications for exceptional measures (hereinafter referred to as "the judge") and develop the judgment procedure.

(b) Employees must apply for approval for exceptional measures to the judge following the formulated procedures. However, employees may make retrospective application immediately afterwards in the case of emergency where an alternative measures have to be taken promptly or where it is unavoidable not to take the prescribed measures. Employees must clarify information including the following items in the application.

(i) Applicant's information (name, department, contact)

(ii) Item of information security rules for which the exceptional measures are requested (the title of the rule and the article, etc.)

(iii) Period for applying the exceptional measures

(iv) Description of the exceptional measures (the alternative measures, etc.)

(v) Reporting procedure for terminating the exceptional measures

(vi) Reason for requesting the exceptional measures

(c) The judge must review applications for exceptional measures submitted by employees in accordance with the formulated judgment procedure and determine whether or not to approve. Also, the judge must create the exceptional measure application record including the following items after making the decision and report to the chief information security officer.

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

(ii) Application details
- Applicant's information (name, department, contact)
- Item of information security rules for which the exceptional measures are requested (the title of the rule and the article, etc.)
- Period for applying the exceptional measures
- Description of the exceptional measures (the alternative measures, etc.)
- Reporting procedure for terminating the exceptional measures
- Reason for requesting the exceptional measures

(iii) Result of the examination
- Approved or disapproved
- Reason for approval or disapproval
- Item of information security rules for which the exceptional measures are approved (the title of the rule and the article, etc.)
- Period of the approved exceptional measures
- Description of the approved exceptional measures (the alternative measures, etc.)
- Reporting procedure for terminating the exceptional measures

(d) Employees must report to the judge who approved the exceptional measure when application of the exceptional measures has come to an end. However, this is not applicable if the judge did not request reporting.

(e) The judge must check whether the applicant has reported on the expiry date of the approved exceptional measures. If there has been no report, the judge must request the report and take necessary measures. However, this is not applicable if the judge did not request reporting.

(f) The chief information security officer must establish a ledger for exceptional measure applications and make this available for the head of information security auditors as required.

1.2.2 Operations

1.2.2.1 Education for Information Security Measures

Compliance Requirements

(1) Enforcement of Education for information security measures

[BASIC Requirements]

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

(b) The head of information security officers must examine training menus according to the roles of employees and prepare the training materials.

(c) The head of information security officers must plan and develop the plan for information security measure training and establish the implementation system to offer the training at least once a year according to the roles of the employee.

(d) The head of information security officers must plan and develop the information security measure training and establish the implementation system to enable a transferred employee to receive the training for his or her new role within three months.

(e) The head of information security officers must establish the system to manage the status of employees' participation in the information security measure training.

(f) The head of information security officers must inform division/office information security officers of the employees' participation status of the information security measure training.

(g) Division/office information security officers must oblige employees to receive information security measure training.

(h) Division/office information security officers must advise employees who have not participated in information security measure training to receive it. If the employee does not follow the advice, the division/office information security officer must report this to the head of information security officers.

(i) The head of information security officers must report the employees' information security measure training participation status to the chief information security officer and the Information Security Committee once a year.

(j) The head of information security officers must examine the necessity of information security measure training on rules, and establish the training menu and system if it is considered necessary.

(2) Participation in Education for information security measures

[BASIC Requirements]

(a) Employees must participate in information security measure training at least once a year according to the training plan.

(b) Employees must check how to receive information security measure training with the division/office information security officer when assigned to or transferred to a new office.

(c) Employees must report to the head of information security officers through the division/office information security officer if he/she is unable to receive information security measure training for a reason for which he/she is not responsible.

(d) The employee must participate in information security measure training according to the training rules if they are in place.

1.2.2.2 Failure Handling

Compliance Requirements

(1) Preparation for possible failure

[BASIC Requirements]

(a) The chief information security officer must establish a system to prevent damage from spreading and recover from the failure or accident in the event of an information security failure or accident (including an incident and malfunction. Hereinafter referred to as "failure, accident, etc.").

(b) The head of information security officers must establish a reporting procedure for failure, accident, etc. and inform this procedure to all employees.

(c) The head of information security officers must establish a measure application procedure in the event of failure, accidents, etc.

(d) The head of information security officers establish an emergency communication network which includes emergency contacts, communication methods, and communication contents for information systems which are deemed especially critical for business in the event of failure, accidents, etc.

(e) The head of information security officers must examine the necessity of training on measures against failure, accident, etc. and establish the contents and system if it is deemed necessary.

(f) Employees must participate in training on measures against failure, accidents, etc. according to rules if rules on such training are already established.

[ENHANCED Requirements]

(g) The head of information security officers must establish a point of contact to receive reports on failure, accidents, etc. from other government agencies and inform the contact method to other government agencies.

(2) Reporting and emergency measures in the event of failure, accidents, etc.

[BASIC Requirements]

(a) Employees must inform concerned parties and their information system security officer according to the reporting procedure formulated by the head of information security officers when failure, an accident, etc. comes to their notice.

(b) Employees must confirm whether the measure application procedure for failure, accidents, etc. is available, and act as the procedure specify where possible.

(c) Employees must endeavor to prevent damage from spreading while waiting for the instruction if the measure application procedure is not available for the given failure, accident, etc. or its availability cannot be confirmed. Employees must follow the instruction when it is given.

(3) Investigating the cause of failure, accidents, etc. and preventing recurrence

[BASIC Requirements]

(a) Information security officers must investigate the cause when failures, accidents, etc. have occurred, develop the measures to prevent the recurrence, and report the results to the chief information security officer.

(b) The chief information security officer must examine the contents of the report on failure, accidents, etc. submitted by the information security officer, and take necessary measures to prevent the recurrence.

1.2.3 Evaluation

1.2.3.1 Self-assessment of Information Security Measures

Compliance Requirements

(1) 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.

(2) Preparing for self-assessment

[BASIC Requirements]

(a) Information security officers must establish the self-assessment form and procedure for each employee.

(3) Conducting self-assessment

[BASIC Requirements]

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

(b) Employees must conduct self-assessment using the self-assessment form and procedure prepared by their information security officer.

(4) Evaluating the result of self-assessment

[BASIC Requirements]

(a) Information security officers must confirm that employees have conducted self-assessment and evaluate the results.

(b) The head of information security officers must confirm that information security officers have 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.

(5) Making improvements based on self-assessment

[BASIC Requirements]

(a) Employees must improve where they can within their authority based on the results of self-assessment, and report this to their information security officer.

(b) The chief information security officer must evaluate the overall results of self-assessment and instruct information security officers to make improvements where necessary.

1.2.3.2 Audit of Information Security Measures

Compliance Requirements

(1) Formulating audit plans

[BASIC Requirements]

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

(2) Instructing information security audits

[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.

(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 as required in response to changes in information security conditions.

(3) Formulating audit plans for individual business operations

[BASIC Requirements]

(a) The head of information security auditors must formulate audit plans for individual business operations in accordance with the annual plan and audit instructions due to changes in information security conditions.

(4) Preparation for information security audits

[BASIC Requirements]

(a) The head of information security auditors must select and appoint information security auditors who are independent from the department which is audited.

(b) The head of information security auditors must consider the necessity of outsourcing part of the audit and do so if it is deemed necessary.

(5) Conducting information security audits

[BASIC Requirements]

(a) Information security auditors must conduct the audit according to the instructions from the head of information security auditors and the audit plan.

(b) Information security auditors must confirm that the standards of government agency comply with these Management Standards for Measures and the Technical Standards for Measures.

(c) Information security auditors must confirm that the audit procedure complies with the standards of government agency.

(d) Information security auditors must confirm that operations in the audited department comply with information security rules by checking the adequacy of self-assessment, etc.

(e) Information security auditors must document the audit results.

(f) The head of information security auditors must create an audit report based on the documented audit results and submit it to the chief information security officer.

⑹ Responding to audit results

[BASIC Requirements]

(a) The chief information security officer must instruct the information security officer of the audited department to take measures against any issues pointed out in the audit report.

(b) If the chief information security officer considers that issues similar to ones pointed out in the audit report probably exist in other departments, and it must be confirmed urgently, he/she must instruct information security officers in other departments to investigate whether similar issues exist and to resolve them if they do.

(c) The information security officers must formulate the improvement plan for the issues whose resolution is requested by the chief information security officer based on the audit report.

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

1.2.4 Review

1.2.4.1 Review of Information Security Review Measures

Compliance Requirements

(1) Reviewing information security measures

[BASIC Requirements]

(a) Persons who established information security rules must examine whether the rules should be reviewed in a timely manner and review them if it is deemed necessary.

(b) Employees must consult the persons who established information security rules if he/she considers there is an issue or problem in these rules.

(c) The persons who established information security rules must take necessary measures when they are notified of any issues or problems in these rules.

1.2.5 Others

1.2.5.1 Outsourcing

Scope

Among services provided based on leases, contracts, and other agreements, this section applies to operations concerning information processing such as the following.

- 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

(1) Establishing a common system among government agencies for information security

[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 standards and procedures for selecting contractors.

[ENHANCED Requirements]

(c) The head of information security officers must establish the evaluation procedure for information security levels of contractors based on the international standards in order to select contractors more stringently.

(2) Clarifying required information security measures to contractors

[BASIC Requirements]

(a) Information system security officers or division/office information security officers must define information security measures that contractors must comply and notify them to candidates in advance.

(b) Information system security officers or division/office information security officers must establish a remedial procedure in the event of information security violation in outsourced operations and notify them to candidates in advance.

(c) Information system security officers or division/office information security officers must establish a procedure to check if the information security measures are complied by contractors and countermeasures against poor implementation, and notify them to candidates in advance.

(3) Selecting contractors

[BASIC Requirements]

(a) Information system security officers or division/office information security officers must to select contractors based on the standards and procedures for selection.

[ENHANCED Requirements]

(b) Information system security officers or division/office information security officers must check information security levels of candidates in accordance with the evaluation procedure for contractors' information security levels established based on the international standards, and take it into consideration when selecting a contractor.

(4) Outsourcing contracts

[BASIC Requirements]

(a) Information system security officers or division/office information security officers must confirm that the contract covers information security measures for outsourced operations, confidentiality (including prohibition of the use of information for non-business purposes), remedial procedures for information security violation, means to check information security implementation and countermeasures against poor implementation before exchanging the contract. Also, he/she must include the following items in the contract as required.

(i) Agreement to undergo information security audits

(ii) Service level assurance

(b) Information system security officers or division/office information security officers must clarify and agree on responsibilities of both parties, and obtain written confirmation on the means and management system of information security compliance from the contractor. Also, he/she must confirm the contractor includes the following items in the confirmation as required.

(i) Name of the person(s) who engages in the outsourced operations

(ii) Specific actions the person takes to implement the required information security measures

(c) Information system security officers or division/office information security officers must examine outsourcing contracts each time at renewal based on the standards and procedure and must not renew contracts carelessly.

(d) Information system security officers or division/office information security officers must examine the appropriateness when making changes in services provided by contractors (including information security policies, implementation procedures, maintenance and improvement of management methods) based on the standards and procedure.

(e) Information system security officers or division/office information security officers must obtain contractors' assurance for information security measures against threats which may arise from subcontracting if the contractor is subcontracting part of the services to third parties.

(5) Outsourcing procedures

[BASIC Requirements]

(a) When providing classified information or important specifications to contractors, employees must restrict the information to the minimum necessary and take the following measures.

(i) Take a safe delivery method and obtain the record

(ii) Oblige the contractor to return, dispose, or erase (to make all information difficult to recover. Hereinafter the same.) information when the provided information is no longer required by the contractor.

(b) In the event of information security violation in the outsourced operations, information system security officers or division/office information security officers must oblige the contractors to take necessary measures in accordance with the agreed remedial procedure.

(c) Information system security officers or division/office information security officers must confirm that information security rules are observed by contractors in accordance with the agreed procedure.

(6) Procedures for the contract expiry

[BASIC Requirements]

(a) Information system security officers or division/office information security officers must confirm information security measures implemented in outsourced operations at the expiry of the contract and take it into consideration when inspecting the deliverables.

1.2.5.2 Consistently Operarion with Business Continuity Plan

Scope

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

Compliance Requirements

(1) Ensuring consistently between BCP and information security measures

[BASIC Requirements]

(a) The Information Security Committee must ensure consistency when establishing BCP and the standards of government agency for their government agency.

(b) The chief information security officer, information security officers, information system security officers, and division/office information security officers must review all the information systems to determine their relevance to BCP when establishing BCP for the government agency.

(c) The chief information security officer, information security officers, information system security officers, and division/office information security officers must establish a common operation procedure for information systems relevant to BCP as follows based on the BCP and standards of government agency when establishing BCP.

(i) Review the procedure from an information security viewpoint for operational consistency of common elements between BCP and standards of government agency in a normal time.

(ii) Check if there are any information security measures which may hinder implementation of BCP or standards of government agency in an emergency situation and establish rules under emergency conditions to secure operational consistency.

⑵ Reporting inconsistency between BCP and information security rules

[BASIC Requirements]

(a) If an employee recognizes any difficulties in executing a planned BCP due to inconsistency between the BCP and information security rules, the employee must report to the concerned parties and request an instruction to his/her information security officer in accordance with the reporting procedure for failure, accidents, etc. established by the head of information security officers.

Chapter 1.3 Measures for Information

1.3.1 Information Handling

1.3.1.1 Creation and Obtain of Information

Compliance Requirements

(1) Prohibiting creation or obtainment of non-business information

[BASIC Requirements]

(a) Employees must not create or obtain any information other than business purposes.

(2) Classification and marking at creation or obtainment of information

[BASIC Requirements]

(a) Employees must determine the classification and marking of information based on the definition of classification and marking at the beginning of its management when the information is created, or obtained from external sources.

(b) Employees must re-classify the information when he/she considers the existing classification and marking should be updated due to amendment, addition, or deletion of the original information based on the definition.

(3) Labeling classification and marking

[BASIC Requirements]

(a) Employees must label the classification and marking of information (including re-classification. Hereinafter the same.) in the means which can be recognized by authorized users.

(4) Succession of classification and marking at processing

[BASIC Requirements]

(a) When creating information, employees must apply the same classification and marking as the referenced or obtained information if the original information is already classified.

1.3.1.2 Use of Information

Compliance Requirements

(1) Prohibiting the non-business use

[BASIC Requirements]

(a) Employees must not use any information for non-business purposes.

(2) Handling information according to the classification and marking

[BASIC Requirements]

(a) Employees must handle information appropriately in accordance with the labeled classification. Employees must also handle information appropriately in accordance with the marking if it is labeled beside the classification.

(3) Succession of classification and marking at copying

[BASIC Requirements]

(a) Employees must apply the same classification and marking on copied information as the original.

(4) Reviewing classification and marking

[BASIC Requirements]

(a) If an employee believes that the existing classification or marking is inappropriate at the time and should be reviewed, he/she must consult with the person who determined the classification or marking (including persons who succeeded it) or the person's superior (hereinafter referred to as "determined parties" in this section).

(b) If an employee believes that his/her own classification or marking requires review, determine the new classification or marking and label it on the information. The employee must also notify the persons who have accessed the information where possible.

(5) Handling classified information

[BASIC Requirements]

(a) Employees must not take classified information outside the government facility for non-business purposes.

(b) Employees must not leave classified information unattended.

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

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

[ENHANCED Requirements]

(e) Employees must display the duration which the given information should be handled as confidentiality class-3. If an employee believes that the classification or marking of information should be downgraded even during the specified period, he/she must follow the necessary procedure to review the classification and marking.

(f) Employees must assign a sequence number for confidentiality class-3 documents and clearly their locations.

1.3.1.3 Save of Information

Compliance Requirements

(1) Storing information according to the classification

[BASIC Requirements]

(a) Employees must store information appropriately according to its classification and marking.

(b) Employees must set appropriate access control on classified information stored in electromagnetic storage media.

(c) Employees must examine whether a password is required when storing confidential information in electromagnetic storage media and set a password if it is deemed necessary.

(d) Employees must examine whether encryption is required when storing confidential information in electromagnetic storage media and encrypt the information if it is deemed necessary.

(e) Employees must examine whether an electronic signature is required when storing critical information in electromagnetic storage media and add an electronic signature if it is deemed necessary.

(f) Employees must examine whether a backup or copy is required for electromagnetic records or important specifications that are classified as critical or vital information, and take a backup or copy if it is deemed necessary.

(g) Employees must examine if the storage of backups of electromagnetic records or copies of important specifications that are classified as critical or vital information is safe against disasters, etc., and take appropriate measures as required.

(2) Information retention period

[BASIC Requirements]

(a) Employees must keep information stored in electromagnetic storage media until the retention period expires if it is specified, and erase it without delay if there is no need to extend the retention period.

1.3.1.4 Transfer of Information

Compliance Requirements

(1) Approving and notifying information transfer

[BASIC Requirements]

(a) Employees must obtain approval from their division/office information security officer when sending confidentiality class-3, integrity class-2, or availability class-2 information, or important specifications.

(b) Employees must notify their division/office information security officer when sending electromagnetic storage media which is confidentiality class-2, integrity class-1, and availability class-1, or confidentiality class-2 documents. However, this is not applicable if the division/office information security officer considers it is not required.

⑵ Selecting from information transmission or transport

[BASIC Requirements]

(a) Employees must select from transmission or transport when sending classified information in electromagnetic format with considerations to safety and notify their division/office information security officer. However, this is not applicable if information is confidentiality class-2, integrity class-1, availability class-1, and in electromagnetic format, and also the division/office information security officer considers it is not required.

⑶ Selecting the means of transfer

[BASIC Requirements]

(a) Employees must select the means of transfer when sending classified information or important specifications with considerations to safety and notify their division/office information security officer. However, this is not applicable if the information is confidentiality class-2, integrity class-1, availability class-1, and in electromagnetic format, or confidentiality class-2 documents, and the division/office information security officer considers it is not required.

⑷ Protecting storage media

[BASIC Requirements]

(a) Employees must take appropriate safety measures when carrying storage media containing confidential information according to the classification and marking of the information.

⑸ Protecting electromagnetic records

[BASIC Requirements]

(a) Employees must examine whether a password is required when sending confidential information in electromagnetic storage media and set a password if it is deemed necessary.

(b) Employees must examine whether encryption is required when sending confidential information in electromagnetic storage media and encrypt the information if it is deemed necessary.

(c) Employees must examine whether an electronic signature is required when sending critical information in electromagnetic storage media and add an electronic signature if it is deemed necessary.

(d) Employees must examine whether a backup is required when sending critical information in electromagnetic storage media and take a backup if it is deemed necessary.

(e) Employees must examine whether a copy of data should also be sent via a different route when sending vital information in electromagnetic storage media to avoid troubles due to a loss or delay in transport, and take appropriate measures if it is deemed necessary.

[ENHANCED Requirements]

(f) Employees must use the required strength of encryption, divide the information into some blocks, and transmit them via different routes when sending confidential information in electromagnetic storage media.

1.3.1.5 Provision of Information

Compliance Requirements

(1) Disclosing information

[BASIC Requirements]

(a) Employees must confirm that the information is classified as confidentiality class-1 when disclosing information.

(b) Employees must take measures to prevent inadvertent leakage from supplemental information, etc. when disclosing information in electromagnetic format.

(2) Providing information to others

[BASIC Requirements]

(a) Employees must obtain permission from their division/office information security officer when providing confidentiality class-3, integrity class-2, or availability class-2 information, or important specifications to external parties.

(b) Employees must notify the division/office information security officer when providing information which is confidentiality class-2, integrity class-1, and availability class-1 in electromagnetic format, or confidentiality class-2 documents to external parties. However, it is not required if the division/office information security officer considers it is not necessary.

(c) When providing classified information or important specifications to external parties, employees must take measures to ensure that the information is appropriately handled by external parties according to the classification and marking.

(d) Employees must take measures to prevent inadvertent leakage from supplemental information, etc. when providing information in electromagnetic format.

1.3.1.6 Deletion of Information

Compliance Requirements

(1) Deletion of electromagnetic records

[BASIC Requirements]

(a) Employees must erase all the contained information when disposing of electromagnetic storage media.

(b) Employees must erase the contained unnecessary confidential information when providing electromagnetic storage media to others.

[ENHANCED Requirements]

(c) Employees must erase confidential information from electromagnetic storage media if it is deemed necessary due to its surrounding environment, etc.

(2) Disposing of written documents

[BASIC Requirements]

(a) Employees must make them difficult to restore when disposing of written documents.

Chapter 1.4 Measures for Information Processing

1.4.1 Use of Information Systems

1.4.1.1 Use of Information Systems

Compliance Requirements

(1) Managing identification codes

[BASIC Requirements]

(a) Employees must not use information systems with any identification codes other than the one assigned to themselves for authentication.

(b) Employees must not allow others to use their identification code for authentication.

(c) Employees must not leave their identification codes in a state where irrelevant parties may see.

(d) Employees must notify the information system security administrator when they no longer require the identification code. However, this is not applicable if the information system security officer resolved that individual reporting is not required.

[ENHANCED Requirements]

(e) Employees who are granted an identification code with administrative permissions must restrict its use to only when carrying out administrative tasks.

(2) Managing authentication information

[BASIC Requirements]

(a) Employees must report to their information system security officer or information system security administrator immediately if their authentication information is used, or may be used by a third party.

(b) Information system security officers and information system security administrators must take necessary measures when authentication information is used, or may be used by third parties.

(c) Employees must manage knowledge-based authentication information as follows.

(i) Employees must keep their own authentication information secret.

(ii) Employees must not tell their authentication information to others.

(iii) Employees must try to remember their authentication information.

(iv) Employees must set authentication information that cannot be guessed easily by others.

(v) Employees must change their authentication information periodically if instructed so by their information system security administrator.

(d) Employees must manage as follows when using ownership-based authentication.

(i) Employees must take safety measures to avoid the authentication information storage device being used unintentionally.

(ii) Employees must not provide or lend their authentication information storage device to others.

(iii) Employees must endeavor to avoid losing their authentication information storage device. If it is lost, employees must report to their information system security officer or information system security administrator immediately.

(iv) Employees must return the authentication information storage device to their information system security officer or information security administrator when they no longer require the device.

(e) Information system security officers must not use information obtained for authentication for any purposes without prior agreement with the information owner.

(3) Granting and managing identification codes and authentication information

[BASIC Requirements]

(a) For information systems which require administration, information system security officers must determine whether to permit the use of shared identification codes for each information system.

(b) For information systems which require administration, Information system security officers must define the administrative procedure including the following items.

(i) The procedure to authenticate the applicant as a legitimate subject when an applicant requests administration

(ii) The procedure for initially granting and changing authentication information

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

(c) For information systems which require administration, information system security officers must designate administrators.

(4) Applying an alternative method for identification codes and authentication information

[BASIC Requirements]

(a) For information systems which require administration, if an employee's identification code becomes unusable and he/she requests for an alternative method, the information system security administrator must confirm legitimacy of the applicant, examine the necessity, and provide an alternative method if it is deemed necessary.

(b) For information systems which require administration, information system security officers and information system security administrators must immediately stop the employee to use the identification code if they become aware of illegal use of an identification code.

1.4.2 Restrictions on Information Processing

1.4.2.1 Restrictions on Information Processing outside Government Facilities

Compliance Requirements

(1) Establishing rules for safeguard

[BASIC Requirements]

(a) The head of information security officers must define security measures for processing classified information outside government facilities.

(b) The head of information security officers must define security measures for taking information systems which handle classified information outside government facilities.

(2) Obtaining and managing approval and application

[BASIC Requirements]

(a) Employees must obtain permission from their information system security officer or division/office information security officer when processing confidentiality class-3, integrity class-2, or availability class-2 information outside government facilities.

(b) Employees must notify their information system security officer or division/office information security officer when processing information which is confidentiality class-3, integrity class-1, and availability class-1 outside government facilities. However, it is not required if the information system security officer or division/office information security officer considers it is not necessary.

(c) Information system security officers and division/office information security officers must record processing of classified information outside government facilities.

(d) Information system security officers and division/office information security officers must confirm the status and take necessary measures if they do not receive any report from the applicant when the approved duration for processing confidentiality class-3, integrity class-2, or availability class-2 information outside government facilities has expired. However, this is not required if the approver resolved that reporting is not required.

(e) Information system security officers and division/office information security officers must confirm the status and take necessary measures if they do not receive any report from the applicant when the approved duration for processing information which is confidentiality class-2, integrity class-1, and availability class-1 outside government facilities has expired.

(f) Employees must restrict confidential information processing outside government facilities to the minimum necessary for business operations.

(g) Employees must obtain permission from their information system security officer and division/office information security officer when taking information systems that handle confidentiality class-3, integrity class-2, or availability class-2 information outside government facilities.

(h) Employees must notify their information system security officer and division/office information security officer when taking information systems that handle information which is confidentiality class-2, integrity class-1, and availability class-1 outside government facilities. However, it is not required if the information system security officer or division/office information security officer considers it is not necessary.

(i) Information system security officers and division/office information security officers must keep records when information systems that handle classified information are taken outside government facilities.

(j) Information system security officers and division/office information security officers must confirm the status and take necessary measures if they do not receive any report from the applicant when the approved duration for taking information systems that handle confidentiality class-3, integrity class-2, or availability class-2 information outside government facilities has expired. However, this is not required if the approver resolved that reporting is not required.

(k) Information system security officers and division/office information security officers must confirm the status and take necessary measures if they do not receive any report from the applicant when the approved duration for taking information systems that handle information which is confidentiality class-2, integrity class-1, and availability class-1 outside government facilities has expired.

(l) Employees must restrict taking information systems that handle confidential information outside government facilities to the minimum necessary for business operations.

(3) Observing rules for safeguard

[BASIC Requirements]

(a) Employees must take the formulated security measures for classified information processing outside government facilities.

(b) Employees must report to the approver when they no longer process confidentiality class-3, integrity class-2, or availability class-2 information outside government facilities. However, this is not required if the approver resolved it is not necessary.

(c) Employees must take the formulated security measures for taking information systems that handle classified information outside government facilities.

(d) Employees must report to the approver when they no longer take information systems that handle confidentiality class-3, integrity class-2, or availability class-2 information outside government facilities. However, this is not required if the approver resolved it is not necessary.

1.4.2.2 Restrictions on Information Processing Using Unsupplied Information Systems

Compliance Requirements

(1) Establishing rules for safeguard

[BASIC Requirements]

(a) The head of information security officers must define security measures for processing classified information using unsupplied information systems.

(2) Obtaining and managing approval and application

[BASIC Requirements]

(a) Employees must obtain permission from their information system security officer or division/office information security officer when processing confidentiality class-3, integrity class-2, or availability class-2 information using unsupplied information systems.

(b) Employees must notify their information system security officer or division/office information security officer when processing information which is confidentiality class-2, integrity class-1, or availability class-1 using unsupplied information systems. However, it is not required if the information system security officer or division/office information security officer considers it is not necessary.

(c) Information system security officers and division/office information security officers must record classified information processing using unsupplied information systems.

(d) Information system security officers and division/office information security officers must confirm the status and take necessary measures if they do not receive any report from the applicant when the approved duration for processing confidentiality class-3, integrity class-2, or availability class-2 information using unsupplied information systems has expired. However, this is not required if the approver resolved that reporting is not required.

(e) Information system security officers and division/office information security officers must confirm the status and take necessary measures if they do not receive any report from the applicant when the approved duration for processing information which is confidentiality class-2, integrity class-1, and availability class-1 using unsupplied information systems has expired.

(3) Observing rules for safeguard

[BASIC Requirements]

(a) Employees must take the formulated security measures for processing classified information using unsupplied information systems.

(b) Employees must report to the approver when they no longer process confidentiality class-3, integrity class-2, or availability class-2 information using unsupplied information systems. However, this is not required if the approver resolved it is not necessary.

[ENHANCED Requirements]

(c) Information system security officers must personally and periodically confirm if the formulated security measures are observed when processing classified information using unsupplied information systems.

Chapter 1.5 Basic Measures for Information Systems

1.5.1 Security Requirements for Information Systems

1.5.1.1 Security Requirements for Information Systems

Compliance Requirements

(1) Planning information systems

[BASIC Requirements]

(a) Information system security officers must request persons responsible for information systems to establish a method to maintain security throughout the information system's lifecycle.

(b) Information system security officers must define security requirements for information systems. Requirements for systems which provide online application and notification services between citizens, organizations, and the government must be formulated based on the "Guidelines on Risk Assessment and Digital Signature/Authentication for e-Government".

(c) Information system security officers must define measures for hardware procurement (including leasing), software development, information security function configuration, information security threats, and information system components in order to meet the security requirements of information systems.

(d) When purchasing component products for an information system, the information system security officer must examine the necessity of selecting the "IT Security Evaluation and Certification Scheme" certified devices and software. If it is deemed necessary and there are multiple candidate products which are equipped with required security functions, he/she must select a certified product which also satisfies the required assurance level.

(e) Information system security officers must examine the necessity of monitoring the information system for information security violation or threats, and formulate the necessary measures if it is deemed necessary.

(f) Information system security officers must define the installation procedure and environmental requirements in terms of information security when an implemented information system starts its operation.

[ENHANCED Requirements]

(g) Information system security officers must request for ST evaluation and ST confirmation (ST: Security Target) by a third party organization on the Security Design Specifications of the system if he/she recognizes important security issues in the information system being implemented. However, it is not applicable if the information system is being updated or there have been specification changes during the implementation, and changes in important security requirements in the revised security design specification are negligible.

(2) Implementing and operating information systems

[BASIC Requirements]

(a) Information system security officers must take security measures formulated based on the security requirements when implementing and operating information systems.

(3) Migrating and disposing information systems

[BASIC Requirements]

(a) Information system security officers must examine whether the information should be erased or saved, and whether the information system should be disposed of or recycled, and take appropriate measures when migrating or disposing of information systems.

(4) Reviewing information systems

[BASIC Requirements]

(a) Information system security officers must examine the necessity of reviewing security measures for information systems as required, and if it is deemed necessary, review and take necessary measures.

1.5.2 Maintenance and Observance of Information System Rules

1.5.2.1 Maintenance of Documents and Inventories of Information Systems

Compliance Requirements

(1) Maintaining documents of information systems

[BASIC Requirements]

(a) Information system security officers must maintain documents containing the following information on information systems under their management.

(i) Computers composing the information system

- Information to identify the employees managing the computers and the users
- Computer models and the type and version of the software
- Specifications or design documents of the computers

(ii) Communication lines and communication equipment composing the information system

- Information to identify the employee managing the communication line and communication equipment
- Communication equipment models and the type and version of the software
- Specifications or design documents of the communication line and communication equipment
- Configuration of the communication line
- Access control configuration on the communication equipment
- Identification codes of the computers using the communication line, and computer users with their identification codes
- Departments using the communication line

(iii) Security procedure for the information system components

- Security procedures for the computers
- Security procedures for services provided via the communication line
- Security procedures for the communication line and communication equipment

(iv) Response procedures in the event of failure or accidents

(b) Information system security administrators must take security measures for operating and managing information systems under their management according to the established document.

(2) Maintaining inventories of information system

[BASIC Requirements]

(a) The head of information security officers must maintain inventories of all systems with the following items.

(i) Name of the information system

(ii) Department in charge, and the name and contact of the information system security officer in charge
(iii) System configuration
(iv) Type of the communication line outside the government facility
(v) Classification and marking of the information handled
(vi) Design, development, operations, and maintenance of the information system

An inventory with the following items must be maintained when outsourcing information processing.

(vii) Business name
(viii) Department in charge, and the name and contact of the information system security officer in charge
(ix) Contractor
(x) Contract duration
(xi) Business purpose overview
(xii) Domain name (when using services provided via the Internet)
(xiii) Classification and marking of the information handled

(b) Information system security officers must report the descriptions of the information system inventory to the head of information security officers when an information system is newly implemented or updated.

1.5.2.2 Procurement of Equipment, etc.

Scope

This section applies to procurement of equipment, etc. (including leasing; hereinafter the same).

Compliance Requirements

(1) Establishing rules concerning procurement of equipment, etc.

[BASIC Requirements]

(a) The head of information security officers must formulate the selection criteria for equipment, etc.
(b) The head of information security officers must specify in the selection criteria that the IT Security Evaluation and Certification Scheme certification should be taken into consideration when there are required specifications for security functions and the procurement is made through a general assessment tendering system. required specifications
(c) The head of information security officers must formulate the check and inspection procedure at the delivery of equipment, etc. from the viewpoint of information security.

(2) Observing rules concerning procurement of equipment, etc.

[BASIC Requirements]

(a) Information system security officers must confirm equipment's applicability to the selection criteria and use the result to aid the selection.

(b) Information system security officers must inspect the delivered equipment, etc. according to the defined check and inspection procedures.

1.5.2.3 Software Development

Compliance Requirements

(1) Establishing rules concerning software development

[BASIC Requirements]

(a) The head of information security officers must establish rules concerning security of software development that information system security officers should observe.

(i) Information system security officers must establish a development system to satisfy security measures (compliance requirements (1) (a) from (iii) to (xiv)).

(ii) When outsourcing software development, information system security officers must select the necessary items from security measures (compliance requirements (1) (a) from (iii) to (xiv)) and oblige the contractor to assure compliance on these items.

(iii) Information system security officers must define the development procedure and environment for software development processes in terms of information security.

(iv) Information system security officers must examine whether development and testing of software should be separated from the live information systems from the information security viewpoint, and separate them if it is deemed necessary.

(v) Information system security officers must examine the necessity of security functions in newly developing software with considerations to assumed security threats on associated information assets in operations, and classification and marking of information handled by the software. If it is deemed necessary, he/she must appropriately design the security functions and clearly describe them in the design document.

(vi) Information system security officers must examine the necessity of administrative functions over the security functions which will be implemented for newly developing software. If it is deemed necessary he/she must appropriately design the administrative functions and clearly describe them in the design document.

(vii) Information system security officers must define the scope and method of reviews to confirm adequacy of information security in software design, and carry out reviews accordingly.

(viii) Information system security officers must examine the necessity of functions to confirm adequacy of information security in input and output data of newly developing software. If it is deemed necessary, he/she must appropriately design the method and clearly describe it in the design document.

(ix) Information system security officers must request for ST evaluation and ST confirmation (ST: Security Target) by a third party organization on the Security Design Specifications of the system if he/she recognizes important security issues in the information system being developed. However, this is not applied if an information system which includes the given software is undergoing ST evaluation and ST confirmation, or if the software is being updated or there have been specification changes during the development, and changes in important security requirements in the revised security design specification are negligible.

(x) Information system security officers must protect the source code created by software developers from unnecessary access and obtain a backup.

(xi) Information system security officers must define coding rules from the information security viewpoint.

(xii) Information system security officers must examine the necessity of reviews on the created source code to confirm adequacy of information security. If it is deemed necessary, he/she must define the scope and method of the source code review and carry out the review accordingly.

(xiii) Information system security officers must examine the necessity of tests from the security viewpoint. If it is deemed necessary, he/she must define the test items and method, and carry out the test accordingly.

(xiv) Information system security officers must maintain a record of tests that are conducted from the information security viewpoint.

(2) Observing rules concerning software development

[BASIC Requirements]

(a) Information system security officers must observe software development rules.

1.5.2.4 Standard Procedure for Authentication, Access Control, Administration, Audit Trail Management, Assurance, etc.

Compliance Requirements

(1) Establishing Management concerning authentication, access control, administration, audit trail Management, assurance, etc.

[BASIC Requirements]

(a) The head of information security officers must formulate rules concerning how to determine the necessity of authentication, access control, administration, audit trails, assurance, etc. including the following items.

(i) Information system security officers must examine all information systems if the system requires authentication. He/she must consider that authentication is required for any information systems which handle classified information.

(ii) Information system security officers must examine all information systems to determine if the system requires access control. He/she must consider that access control is required for any information systems which handle classified information.

(iii) Information system security officers must examine all information systems to determine if the system requires administration. He/she must consider that administration is required for any information systems which handle classified information.

(iv) Information security officers must examine all information systems if the system requires audit trails.

(v) For information systems which require audit trails, information security officers must define information items to be obtained as the audit trail and its retention period.

(vi) For information systems which require audit trails, information system security officers must explain to the information system security administrator and users about recording of the audit trail, its retention, and possibility of its examination and analysis in advance.

(vii) For information systems which handle classified information, information system security officers must examine if assurance measures are required.

⑵ Observing rules concerning authentication, access control, administration, audit trail management, assurance, etc.

[BASIC Requirements]

(a) Information security officers and information system security officers must implement information systems based on rules concerning how to determine the necessity of authentication, access control, administration, audit trail management, assurance, etc. of their government agency.

⑶ Examining, analyzing, and reporting on obtained audit trails

[ENHANCED Requirements]

(a) For information systems which requires audit trails, information system security officers must examine and analyze the obtained audit trails periodically or as required, and take necessary information security measures or report to their information security officer according to the results.

1.5.2.5 Standard Procedure for Encryption and Electronic Signatures

Compliance Requirements

(1) Establishing rules concerning encryption and electronic signatures

[BASIC Requirements]

(a) The head of information security officers must define the algorithm and operational method for encryption and electronic signatures for their government agency including the following items.

(i) If possible, use those on the "e-Government Recommended Ciphers List"

(ii) Use algorithms on the "e-Government Recommended Ciphers List" when newly implementing an information system, or introducing encryption or electronic signature at an update. If enabling a selection from multiple algorithms for encryption or electronic signatures, include at least one from the "e-Government Recommended Ciphers List".

(iii) Examine the necessity of an emergency response plan in the case where the algorithm is compromised. Define an emergency response plan if it is deemed necessary.

(b) The head of information security officers must formulate the procedure of the following (i) and (ii) for the key which is used to decrypt encrypted information (excluding documents; hereinafter the same in this section) and to add electronic signature (hereinafter referred to as the "key management procedure, etc.).

(i) Procedure for key generation, expiry, disposition, update, and measures for disclosure, etc.

(ii) Procedure for key storage

[ENHANCED Requirements]

(c) Information security officers must define the backup procedure and storage procedure of the key for decrypt encrypted information ("key backup procedures, etc.", hereinafter).

(d) The head of information security officers must specify in the algorithm and operational method for encryption and electronic signatures for the government agency the use of the electronic certificate which is applicable, meets the purpose of electronic signatures, and is issued by the Government Public Key Infrastructure (GPKI), if available when deploying electronic signatures.

(2) Observing rules concerning encryption and electronic signatures

[BASIC Requirements]

(a) Employees must follow the specified algorithm and method when encrypting information and adding electronic signatures.

(b) Employees must follow the formulated management procedure of the key used to decrypt encrypted information or to add electronic signatures, and manage it appropriately.

[ENHANCED Requirements]

(c) Employees must obtain a backup of the key used to decrypt encrypted information according to the defined key backup procedure, etc.

1.5.2.6 Preventing Actions that Compromise the Information Security Level outside Government Agencies

Compliance Requirements

(1) Establishing rules for measures

[BASIC Requirements]

(a) The head of information security officers must define the procedure to prevent actions that would compromise the information security level outside the government agencies.

(2) Observing the rules

[BASIC Requirements]

(a) Employees must take necessary measures according to the rules for preventing actions to compromise the information security level outside the government agencies.

1.5.2.7 Measures for the Use of Domain Names

Compliance Requirements

(1) Establishing rules for the use of domain names

[BASIC Requirements]

(a) The head of information security officers must establish rules for employees concerning the use of domain names under the domain name system (hereinafter referred to as "domain names") including the following items.

(i) Employees must use domain names with the following criteria to guarantee that they are government domain names (hereinafter referred to as "government domain names") when announcing a domain name in order for persons outside government agencies (excluding overseas residents; hereinafter the same in this section) to access or transmit to.

- Domain names which end with ".go.jp"

However, domain names other than government domain names may be used only for e-mail transmission or displayed on web pages under government domain names if the following conditions are met.

All the following conditions must be met for e-mail transmission.

- An e-mail address with a government domain name is also given as a contact address for queries, or an electronic signature by a government domain name is added.
- The name of organization which manages the displayed domain name is given.
- The date when validity of the displayed domain name was confirmed, or the guaranteed duration of validity is given.

Also, all the following conditions must be met for displaying the address on web pages under government domain names.

- The name of organization which manages the displayed domain name is given.
- The date when validity of the displayed domain name was confirmed, or the guaranteed duration of validity is given.

(ii) Employees must use a government domain name for sending e-mails to anyone outside government agencies. Excluding the case where the employee is already known to the recipient.

(iii) Employees must only use servers with government domain names when storing information in order to allow access to users outside government agencies.

(2) Observing rules for the use of domain names

[BASIC Requirements]

(a) Employees must take necessary measures according to the rules for the use of domain names.

1.5.2.8 Day-to-day Measures for Protection against Malware

Compliance Requirements

(1) Establishing rules concerning measures against malware

[BASIC Requirements]

(a) The head of information security officers must define rules for employees to take the following measures in order to prevent malware infection.

(i) Employees must not execute any executable files which have been identified as malware by antivirus software, and must not read such data files into application programs, etc.

(ii) Employees must always keep application programs and malware definition files used with antivirus software up-to-date.

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

(iv) Employees must periodically scan all electronic files for malware using antivirus software, etc.

(v) Employees must scan data and software for malware after receiving them from external sources before taking them into computers, or before providing them to external parties.

(vi) Employees must endeavor to prevent malware infection.

(vii) Employees must immediately disconnect the computer from the communication line and take necessary measures if they suspect the computer may have been infected by malware.

(2) Observing rules concerning measures against malware

[BASIC Requirements]

(a) Employees must take measures to prevent malware infection according to the formulated rules for measures against malware.