Information Security Policy
of the Institute for Global Environmental Strategies

Established on 7 March 2019
Amended on 1 April 2021

1. General Provisions

1.1 Basic Policy for Information Security

(1) Basic policy for information security

Based on the *Regulations on Document Management* (Regulations No.4) of the Institute for Global Environmental Strategies (hereafter referred to the "Institute") and the *Common Standards for Information Security Measures for Government Agencies* (published by the National center of Incident readiness and Strategy for Cybersecurity or NISC of Japan on 25 July 2018), the Institute will make the best efforts to protect the Institute's information assets from all possible threats.

(2) Scope of the Policy

(a) The Policy shall apply to officers and Users of the Institute, as well as all persons who are engaged in the Institute's work under the contracts with Institute (hereafter referred to as "Users").

(b) The Policy shall apply to the following information:

(i) Information used by Users to perform their duties, which is recorded on the information systems procured or developed by the Institute, or information recorded on the external storage media (including information printed out from, or input in the system);

(ii) Information for use of Users, recorded on other information systems or other external storage media (including the information printed out from, or input in the system; and

(iii) In addition to (i) and (ii), information concerning the design or operational management of the system procured or developed by the Institute.

(c) The Policy shall apply to all information systems which process the information stipulated herein.

(3) Revisions of the Policy

The Policy shall be regularly reviewed and necessary additions and amendments shall be made according to information technology development.

(4) Compliance with laws and regulations

When taking information security measures, laws and regulations, including those by IGES which stipulate handling of information and information systems (hereinafter referred to as "relevant laws and regulations" should be respected in addition to the Policy. The Policy provides no reference to such relevant laws and regulations, as they should be respected regardless of information security measures. Equally the Japanese government's resolutions set forth in response to changing environment of information security as well as the Institute's Regulations etc. should be duly observed. The Institute shall establish implementation plans and other procedures of the Policy.

1.2 Classification of Information and Handling Restrictions

(1) Classification of information

The Policy classifies information in three aspects namely confidentiality, integrity, and availability, whose definition are shown in Tables 1 to -3. When changing or adding classifications, the Institute

shall ensure the relationships between classifications and requirements for given measures to be the same or higher than those described in the Policy. The Institute should appropriately notify the classifications set forth in the Policy, as well as its own corresponding classification, when providing information to other organisations.

Table 1: Classifications for confidentiality

Classification	Classification criteria
Confidentiality Class-3 Information	Among information for work, items which include information considered confidential and required to be handled accordingly
Confidentiality Class-2 Information	Among information for work except for Confidentiality Class-3 Information, items which include information which should be regarded as Non-Disclosure Information stipulated in Article 5 of the Act on Access to Information Held by Administrative Organisations (Act No. 42 of 1999; hereinafter referred to as "Information Disclosure Act")
Confidentiality Class-1 Information	Information which does not include items which should be regarded as Non-Disclosure Information stipulated in Article 5 of the Information Disclosure Act.

Information which comes under Confidentiality Class-2 Information and Confidentiality Class-3 Information is called “Confidential Information”.

Table 2: Classifications for integrity

Classification	Classification criteria
Integrity Class-2 Information	Among information for work (except for written information), items whose manipulation, errors, and damage may infringe other’s rights or hamper proper Institute operations (except for negligible cases).
Integrity Class-1 Information	Information other than Integrity Class-2 information (except for written information)

Note that Integrity Class-2 Information is called “Critical Information.”

Table 3: Classifications for availability

Classification	Classification criteria
Availability Class-2 Information	Among information for work (except for written information), items whose disappearance, loss, or unavailability may infringe other’s rights or stable Institute’s operations (except for 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, information classified as any of Confidential Information, Critical Information, or Vital Information is called “Classified Information.”

(2) Types of handling restrictions

“Handling restrictions” means restrictions to ensure proper handling of information by Users, such as to prohibit copying, removing, and distributing information, as well as mandatory encryption and disposal of the data after use. Users should appropriately handle the information according to its classification, and follow the types of handling restrictions to demonstrate proper and practical handling of the information. The Institute should set forth the basic definitions of handling restrictions from perspectives of three aspects, namely confidentiality, integrity, and availability (Annex A.1).

2. Basic Framework of Information Security

2.1 Introduction and Plan

2.1.1 Establishment of organisations and systems

(1) Designation of the Administrator of Information Security (hereafter referred to as "Administrator")

The Administrator shall be designated to direct tasks associated with information security measures at the Institute.

(2) Establishment of the Information Security Committee

The Administrator shall establish the Information Security Committee, which consists of Information Security Managers (hereafter referred to as "ISM") from the Institute's headquarters and satellite offices, etc. promoting information security and as necessary an Information Security Advisor, whose function is to deliberate provisions such as the Information Security Policy.

(3) Designation of the Information Security Auditor

The Administrator shall designate an Information Security Auditor who directs tasks associated with audits conducted under the direction of the Administrator.

(4) Designation of the Head Information Security Manager (Head ISM) and other Information Security Managers

(a) The Administrator shall designate Information Security Manager (Head ISM) and his/her Deputy in Strategic Management Office at Institute's headquarters to carry out information security for the whole Institute, including information system security, in a centralized manner. The Administrator shall designate Satellite ISMs for Tokyo Sustainability Forum (TSF), Kansai Research Centre (KRC), Kitakyushu Urban Centre (KUC), Bangkok Regional Centre (BRC), Intergovernmental Panel on Climate Change Task Force on National Greenhouse Gas Inventories Technical Support Unit (IPCC-TSU), Asia Pacific Network for Global Change Research Secretariat (APN Secretariat), IGES Japanese Center for International Studies in Ecology (JISE Center) and Leader of SMO-ICT team to support information security for the whole Institute led by Head ISM and his/her Deputy.

(b) Satellite ISMs shall be in charge of administrative tasks for information security and information system security at each satellite office under the instruction of Head ISM.

(c) Head ISM shall designate a project-level ISM (hereafter referred to as "Project ISM") as necessary who directs information security-related work.

(5) Designation of Information Security Support

The Administrator shall designate Information Security Support with expertise and experience in information security (IT service provider to the Institute under contract).

(6) Organisation for information security

Administrator shall establish organisation and roles for information security at the Institute

(7) Preparedness for the information security incidents

(a) The Administrator shall establish a Computer Security Incident Response Team (CSIRT).

(b) The Administrator shall designate Head ISM in charge of CSIRT. The person who is in charge of CSIRT shall respond to incidents receiving technical support from the Information Security

Support (IT service provider to the Institute under contract).

(c) The Administrator shall establish a reporting system through which all concerned persons immediately report to him or her in the event of a security information incident.

(8) Roles that should not be concurrently undertaken by the same person:

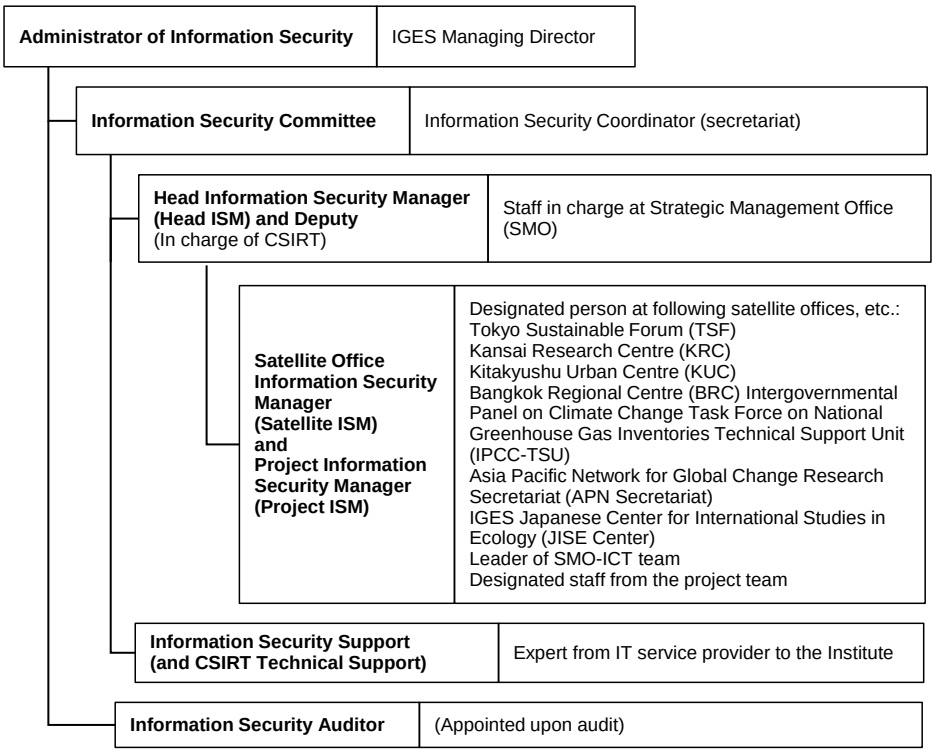
(a) Users shall not concurrently undertake the following roles when implementing information security measures.

(i) A submitter of an application for approval and a person who approves the application.

(ii) An auditee and an auditor

(b) When applying for approval, etc., if Users themselves are the approvers, or if it is irrelevant for the approval authority, etc. to decide whether the application should be approved or denied, such approval, etc. should be submitted to, and granted by, their supervisors or other persons deemed relevant.

Organisation for information security at the Institute



2.1.2 Establishment of the Information Security Policy and implementation plan of measures

(1) Establishment of the Institute's Information Security Policy

The Administrator shall establish the Institute's Policy through deliberations by the Information Security Committee. The Policy shall be established based on the risk assessment of the works and information handled by the Institute, as well as the information systems owned by the Institute.

(2) Implementation of plan for security measures

The Administrator shall establish a plan to comprehensively implement information security measures (hereinafter referred to as the "Security Plan") through deliberations by the Information Security Committee including below:

(i) Education on information security

(ii) Self-check of information security measures
(iii) Information security audit
(iv) Initiatives to promote technical measures related to information systems
(v) Any other important initiatives related to information security measures listed in the preceding items

2.2 Operation

2.2.1 Enforcement of information security related provisions

(1) Implementation and maintenance of operational procedures for information security measures
   (a) The Head ISM (unless otherwise specified in the Policy) shall maintain the operational procedures for information security measures at the Institute and direct tasks concerning the operational procedures, as well as report the maintenance status to the Administrator.
   (b) The Head ISM shall maintain personnel management rules for information security measures.
   (c) Those who are in charge of managing information security shall complete necessary tasks assigned by the Administrator.
   (d) The ISMs shall report to the Head ISM, if there are any issues or problems with information security related provisions reported by Users.
   (e) The Head ISM shall monitor the implementation of the information security measures and as necessary report it to the Administrator.

(2) Handling violations
   (a) Users shall report to the ISMs when they become aware of any serious breach of information security related provisions.
   (b) The Head ISM shall instruct the violator and concerned parties to take necessary measures to maintain information security when he or she is informed of, or becomes aware of any serious breach of the Information Security Policy, and shall report to the Administrator.

2.2.2 Exceptional measures

(1) Maintenance of exceptional measures

The Administrator as necessary shall designate a person who examines applications for exceptional measures (hereinafter referred to as "the Permission Authority") and shall establish the examination procedure. The Head ISM shall keep a record of exceptional measures.

(2) Operation of exceptional measures
   (a) Users shall follow the stipulated examination procedures when submitting applications for exceptional measures to the Permission Authority (Head ISM). For tasks should be executed immediately and can be handled in highest consideration of the provisions, where taking measures other than those prescribed in the information security related Policy or not taking prescribed measures is unavoidable, applications for such exceptional measures shall be promptly submitted afterwards.
   (b) The Permission Authority (Head ISM) shall examine applications for exceptional measures submitted by Users in accordance with the stipulated approval procedures and determine whether or not to approve.
   (c) The Permission Authority (Head ISM) shall establish records of exceptional measure application and report them to the head information security officer.

(d) The Head ISM shall review information security measures for necessary revisions or additions based on the application status of exceptional measures, and report them to the Administrator as necessary.

2.2.3 Handling of information security incidents

(1) Preparedness for information security incidents

(a) The Head ISM shall establish reporting procedures, including points of contact within the Institute in the event of information security incidents (including potential incidents), and shall inform all Users of these procedures.

(b) The Head ISM shall establish procedures for measures including sharing information with other organisations in the event of information security incidents (including potential incidents).

(c) In preparation for information security incidents, the Head ISM shall establish an emergency communication network for the information systems deemed especially critical to execute the work.

(d) The Head ISM shall examine the necessity of training on measures against information security incidents.

(2) Handling of information security incidents

(a) Users shall report to Head ISM, Deputy Head ISM or Information Security Support (IT service provider to the Institute) and follow their instructions in the event of information security incidents (including potential incidents).

(b) The CSIRT shall check the reported information security incident (including potential incident) and verify whether or not it is an information security incident.

(c) The CSIRT shall immediately report to the Administrator in the event of information security incidents.

(d) The CSIRT shall provide the relevant information security officers concerning the information security incident with instructions or advice on emergency measures to prevent spread of damage and to recover from the incident.

(e) The CSIRT shall report to the police when necessary if the event of information security incidents is considered as a cyber-attack (including potential incident).

(f) The CSIRT shall keep a record of the handling of the information security incident.

(3) Prevention of recurrence of information security incidents and sharing of lessons learned

(a) Information security officers shall, upon receiving instructions or advice from CSIRT on emergency measures and recovery, investigate the cause of information security incidents based on such instructions or advice, and review the measures for prevention and report them to the Administrator.

(b) The Administrator shall examine the report on information security incidents submitted by information security officers, and take necessary measures to prevent recurrence.

(c) The CSIRT shall share the lessons learned from consequences of the incident handling with the ISMs etc.

2.3 Assessment and Education

2.3.1 Assessment and education of information security measures

(1) Assessment and education of Users' information security measures at the individual level

(a) The Head ISM shall regularly manage Users' information security at the individual level with the aid from Information Security Support based on the Security Plan and as needed instruct

Users with improvements.

(b) The Head ISM shall revise the assessment plan when situations surrounding information security require additional components by Users.

(c) The Head ISM shall ensure that Users duly participate in education of information security measures.

(d) The Head ISM shall analyse and evaluate the results of the education of information security and report them to the Administrator as needed.

(2) Conducting self-checks

(a) Head ISM shall instruct Users to conduct self-checks as needed in accordance with the annual self-check plan.

(b) The Head ISM shall analyse and evaluate the results of self-check by Users to identify common problems across offices and report them to the Administrator as needed.

2.3.2 Information security audit

(1) Conducting information security internal audit

The Head ISM shall regularly conduct internal audits with the aid from Information Security Support, plan improvement measures where cross-cutting improvement measures within the Institute are needed, and report the results and necessity of the audit to the Administrator.

(2) Conducting information security audit

(a) The Information Security Auditor shall conduct audits including the following items, and provide the Administrator with an audit report containing the following items.

(i) The audit shall confirm that the matters stipulated in the Institute's Policy are in accordance with the *Common Standards for Information Security Measures for Government Agencies*.

(ii) The audit procedures shall be in accordance with the Institute's Policy.

(iii) The audit shall confirm if operations where auditees are located (headquarters and satellite offices etc. of the Institute) are in accordance with the Policy. .

(b) The Administrator shall instruct Head ISM and ISMs to take improvement measures against any issues based on the audit report.

(c) The Head ISM shall plan and take measures where cross-cutting improvement measures within the Institute are needed and report the results to the Administrator.

2.4 Review

2.4.1 Review of information security measures

The Administrator shall comprehensively evaluate the information security operation and the results of assessment, education and audits, and conduct a necessary review on the Institute's Policy and Security Plan, taking into account the changes in the environment surrounding information security, and after deliberations of the Information Security Committee.

3. Information Handling

3.1 Information Handling

(1) Maintenance of provisions related to information handling

The Head ISM shall maintain the provisions of information handling which contains the

following items and notify them to Users.

(i) Definitions of "classifications and handling restrictions of information"

(ii) Procedures of labeling, etc. of "classifications and handling restrictions of information"

(iii) Procedures of maintenance and review of "classifications and handling restrictions of information"

(2) Prohibition of use or handling of information for non-work related purposes

Users shall limit the use or handling of the information within the scope of their work.

(3) Determination and labeling, etc. of classifications and handling restrictions of information

(a) When preparing information or at the start of managing information prepared by parties other than the Institute, Users shall determine the classifications and handling restriction of information in accordance with its definitions, and take necessary actions of labeling, etc.

(b) When preparing or duplicating information, Users shall maintain the same confidentiality classification and handling restrictions as the original, if the obtained or referred original information is already classified according to its level of confidentiality.

(c) If the existing classifications and handling restrictions deem necessary to be reviewed for amendments, additions, deletions, and for other reasons, Users shall consult with a person, or his or her senior, who determines the classifications and handling restrictions (including those who follow the determination- hereinafter referred to as the "classifying authority" in this section), and conduct reviews based on the outcome of such consultation.

(4) Use and storage of information

(a) Users shall appropriately handle information in accordance with the classification and handling restrictions, which is labeled, or otherwise specified.

(b) Users shall obtain permission from their information system security officers and division/office information security officers when processing confidentiality Class-3 information outside of the areas requiring control measures.

(c) Users shall take necessary security management measures when processing Classified Information outside of the areas requiring control measures.

(d) Users shall appropriately manage information in accordance with the classification and handling restrictions of information, such as setting access control when saving information.

(e) Users shall follow the prescribed procedures when handling information using external storage media, such as USB (Universal Serial Bus) memory and so on.

(5) Provision and disclosure of Information

(a) When disclosing information, Users shall make sure the information is classified as Confidential Class-1 information.

(b) When providing information to parties outside of the scope of viewing restrictions, Users shall consult with the classifying authority and follow his or her decision. In addition, Users shall ensure that the information is properly handled in accordance with the prescribed classification and handling restrictions at the parties' sites. To achieve this Users shall take measures such as to assuredly inform the parties of points to be noted when handling such information.

(c) When providing or disclosing information in electronic or magnetic format, Users shall take measures to prevent inadvertent information leakage.

(6) Transportation and transmission of information

(a) When transporting an external storage media which stores or contains Classified Information

to places outside the areas requiring control measures, Users shall select the means of transportation with considerations to security and take appropriate measures to ensure security in accordance with the classification and handling restrictions of the information. In case that the media is transported only to an area pre-designated by the Head ISM, where defined as the areas required handling restrictions by other organisations, such area shall be regarded as an area requiring control measures.

(b) When transmitting classified information in electronic or magnetic format such as e-mail, Users shall select the means of transmission with considerations to security, and take appropriate measures to ensure security in accordance with the classification and handling restriction of information.

(7) Deletion of information

(a) Users shall immediately erase the information stored in an external storage media when it becomes unnecessary for their work.

(b) When disposing of an external storage media, Users shall erase all the information stored, making it completely unrestorable and ensuring there is no remaining information in the media.

(c) When disposing of confidential information in written format, Users shall make it unrestorable.

(8) Backup of information

(a) Users shall take backup of information in an appropriate manner in accordance with the classification of information.

(b) Users shall determine the place, manner, period for storage and so on, of the backup information, and appropriately manage it in accordance with the classification and handling restriction of information.

(c) Users shall appropriately delete, erase or dispose of the information with exceeded storage period, in accordance with the provisions set forth in paragraph (7) of this section.

3.2 Information Handling Areas

(1) Determine the standards for measures for the areas requiring control measures

(a) The Head ISM shall determine the scope of the areas requiring control measures.

(b) The Head ISM shall determine the standards for measures for the areas requiring control measures according to the characteristics of each area which include the following items

(i) Physical measures to prevent easy access to the areas by unauthorized persons, including maintenance and installation of facilities such as lockable doors and partitions.

(ii) Entrance and exit management systems to restrict unauthorized persons to enter the areas, as well as to prevent illegal actions by authorized persons while they are in the areas.

(2) Determine the measures to be implemented in each area

(a) ISMs shall determine areas per unit where they implement measures for facilities and environments based on the standards set forth by the Head ISM.

(b) ISMs shall determine measures to be implemented in the areas they manage, considering the matters such as the standards set forth by the head information officer, surrounding environment, type of administrative tasks, and information handled in such areas.

(3) Implementation of measures for the areas requiring control measures

(a) ISMs shall implement measures determined in the areas they manage. As for the measures need to be carried out by Users, area information security officers shall take actions to ensure that

Users duly understand and recognize such measures.

(b) ISMs shall implement physical measures to protect information systems which handle vital information from disasters.

(c) Users shall use the areas in accordance with the measures determined by ISMs. Users shall ensure those who belong to parties other than the Institute use the areas in accordance with the prescribed measures when allowing such external parties to enter the areas.

4. Outsourcing

4.1 Outsourcing

4.1.1 Common matters concerning outsourcing

(1) Establishment of provisions related to outsourcing

The Head ISM shall establish provisions related to outsourcing which include the following items.

(i) Criteria for determining the scope of information and information systems that may be accessed by outsourcing parties (hereafter referred to as Outsourcing Criteria).

(ii) Criteria and procedures for selecting outsourcing parties.

(2) Contracts related to outsourcing.

(a) Head ISM shall outsource tasks in accordance with the Outsourcing Criteria.

(b) When outsourcing tasks, Head ISM shall select outsourcing parties in accordance with the Outsourcing Criteria. Implementation of the below specified information security measurements by outsourcing parties shall be the terms of selection, which should be included in the contractual specifications.

(i) Prohibition of use of information by outsourcing parties for non-task related purposes.

(ii) Implementation and management systems of information security measures carried out by outsourcing parties.

(iii) Management systems to prevent any alternation of data and so on, made against the Institute's intention, by outsourcing parties and their employees, or subcontractors or any other parties, while executing outsourced tasks.

(iv) Information of outsourcing parties including their capital ties, executives, the sites where outsourced tasks are processed, professional affiliations and expertise (qualifications and training experience on information security), experience and nationality of employees of the outsourcing parties.

(v) Measures (including framework and procedures) for information security incidents

(vi) Systems for checking implementation status of information security measures as well as other matters in the contract.

(vii) Remedial actions in case of insufficient implementation of information security measures.

(c) Head ISM shall examine matters such as the classification of information handled by the outsourcing parties and include the following items in the contractual specifications as necessary.

(i) Agreement to undergo information security audits

(ii) Service level assurance

(d) In case that outsourcing parties will subcontract a part of outsourced tasks, Head ISM shall make sure the outsourcing parties implement the above specified measures (b) and (c), to ensure a sufficient level of information security against the threats caused by subcontracting. In addition, Head ISM shall include in the contractual specifications the term that outsourcing parties give to the Institute information necessary to verify the implementation of information security measures in subcontractors, and receive the approval by the Institute.

(3) Implementation of measures by outsourcing parties

(a) Head ISM or Project ISM shall check implementation status of information security measures implemented by outsourcing parties based on the contract.

(b) Head ISM or Project ISM shall take necessary measures such as temporal suspension of the outsourcing, and then make outsourcing parties to take the measures based on the contract, in case that they become aware, or are informed by Users, of information security incidents or use of information for non-task related purposes by outsourcing parties while executing outsourced tasks.

(c) Head ISM or Project ISM shall ensure the information handled by outsourcing parties to be returned or erased upon the termination of the contract.

(4) Information handling when outsourcing tasks

Users, especially Project ISMs who handle outsourcing shall comply with the following requirements when providing information and so on, to outsourcing parties.

(i) When providing classified information to outsourcing parties, it should be restricted to the minimum and a prescribed safe delivery method should be used.

(ii) When the provided classified information is no longer required by outsourcing parties, it should be made sure that the outsourcing parties will duly return or erase the information.

(iii) A report should immediately be made to Head ISM in the event of information security incidents or use of information for non-task related purposes while outsourced operations are being performed.

4.1.2 Use of external services on general terms and conditions

(1) Establishment of provisions related to use of external services on general terms and conditions

(a) The Head ISM shall establish provisions related to use of external services which contain the following items, and stipulate that no confidential information should be handled when using such services:

(i) Scope of work which allows use of external services on general terms and conditions

(ii) Types of external services which can be used for work

(iii) Procedures for use and operational steps

(b) ISMs shall designate persons in charge of each service when using external services on general terms and conditions.

(2) Implementation of measures for use of external services on general terms and conditions

When applying for the use of external services on general terms and conditions, Users shall make sure that the risks of using such services are tolerable, by checking the terms and conditions and other terms of the services, and ensure that the appropriate measures are implemented upon using those services.

4.1.3 Dissemination of information via social media services

Measures for dissemination of information via social media services

(a) The Head ISM shall establish information security measures related to operational procedures which include the following items, giving the fact that the social media services are used with the accounts managed by the Institute. The Head ISM shall also stipulate that no confidential information should be handled when using such services:
    (i) Measures to prevent impersonation, such as to clearly indicate the organisation which manages the accounts, in order to assure the information disseminated from the accounts of the Institute genuinely originates from the Institute.
    (ii) Measures to prevent unauthorised access, such as proper management of passwords and other information for user/entity authentication

(b) When using social media services at the Institute for information dissemination, ISMs shall appoint personnel in charge of each social media service.

(c) When using social media services to provide Vital Information to the public, Users shall make such information available for viewing on the Institute's websites.

4.1.4 Using cloud services

Measures for using cloud services

(a) The Head ISM shall determine whether or not to entrust information handling, considering classification and restriction of handling information when using the cloud services.

(b) The Head ISM shall select outsourcing parties by evaluating the risk of applying laws and ordinances other than domestic laws to the information handled by the cloud services, and as necessary, specify the place where contracted projects are performed and the applicable law and jurisdiction provided for in the contracts.

(c) The Head ISM shall consider the measures to transition the operations smoothly at the time of discontinuation or termination of the cloud services, and make them requirements for selecting outsourcing parties.

(d) The Head ISM shall establish security requirements after designing security in such a way as to overlooking entire distribution route of information, with taking the characteristics of the cloud services into consideration, so that security over the entire distribution channels of information including the cloud service part is appropriately ensured.

(e) The Head ISM shall evaluate and determine comprehensively and objectively that the reliability of the cloud services and the outsourcing parties of such services is sufficient, from the contents of reports of the information security audit for the cloud service, the application status of various certification/authentication systems, etc.

5. Lifecycle of Information Systems

5.1 Maintenance of Documents and Inventories of Information Systems

5.1.1 Maintenance of documents and inventories of information systems

(1) Maintenance of information system inventories

(a) The Head ISM shall keep a record of the matters concerning the security requirements for all the information systems in the information system inventories.

(b) When newly constructing or updating an information system, the Head ISM shall record or

state the contents of the security requirements described in the information security inventory of said system.

(2) Maintenance of documents related to information systems

The Head ISM shall maintain documents required to implement information securities measures for the information systems under their management, containing all the items specified below.

(i) Information of the server equipment and terminals composing the information systems

(ii) Information of the communication lines and communication equipment composing the information systems

(iii) Procedures to maintain the security level of information security of each component of the information systems

(iv) Procedures when detecting information security incidents

5.1.2 Establishment/maintenance of provisions related to procurement of equipment, etc.

Maintenance of provisions related to procurement of equipment, etc.

(a) The Head ISM shall establish the criteria for selecting equipment, etc. The criteria should contain, if necessary, a scheme which enables government agencies to monitor the management of equipment to ensure no malicious alternation is made throughout the lifecycle of equipment, such as its development phase.

(b) The Head ISM shall maintain the checking and inspection procedures upon delivery of equipment, etc., in consideration of information security measures.

5.2 Measures at Each Phase of Information System Lifecycle

5.2.1 Planning, and definition of requirements for information systems

(1) Ensuring the implementation of frameworks

(a) The Head ISM shall request the Administrator for managing information systems to ensure the implementation frameworks which enable to maintain the information security throughout the information system's lifecycle.

(b) When constructing a system based on the common platform system, the Head ISM shall maintain said system, and request the Administrator to establish frameworks in accordance with the operational management provisions and so on, operate and manage the common platform system.

(2) Formulation of security requirements for information systems

(a) The Head ISM shall develop security requirements including the following items, based on the matters such as purpose of constructing the information system, task requirements for the targeted tasks and so on, as well as classification of information handled by said system, after determining whether it is necessary to isolate said system from the internet or from systems connected to the internet (including cloud service).

(i) Requirements for security functions to be incorporated to the system such as user/entity authentication, access control, authority control, log management, and encryptions

(ii) Requirements for operational management functions such as monitoring, while the information systems are in operation (if data for monitoring is encrypted, this shall be

decrypted if necessary)

(iii) Requirements for measures against vulnerabilities of the information systems

(b) When constructing an information system connected to the internet, the Head ISM shall decide the communication lines to connect and define security requirements for multiple protection to diminish risks of leakage, manipulation and so forth, caused through the internet such as targeted attacks.

(c) The Head ISM shall refer to the "List of Requirements for Ensuring Security in Procurement of IT Products[1]" when procuring an equipment, and shall analyse the threats in the environments where the equipment is used, and formulate security requirements to counter the information security threats in said equipment, etc.

(d) When constructing systems based on the common platform system, the Head ISM shall formulate security requirements in accordance with the operational management provisions and so on related to the security measures for such common platform system, in order to maintain the level of information security of entire common platform system.

(3) Measures when outsourcing construction of information systems

When outsourcing construction of information systems, the Head ISM shall oblige the outsourcing parties to ensure compliance on the following requirements by implementing measures such as indicating them in the procurement specifications

(i) Appropriate implementation of information security requirements

(ii) Systems tests conducted from perspectives of information security

(iii) Information security measures in the environment and process of information system development.

(4) Measures when outsourcing operation and maintenance of information systems

(a) When outsourcing operation and maintenance of information systems, the Head ISM shall ensure the outsourcing parties to comply with the requirements for proper operation of the system's security functions, by indicating these requirements in the procurement specifications, and so on.

(b) When outsourcing operation and maintenance of information systems, the Head ISM shall ensure that the outsourcing parties promptly report any changes made in the system's security functions of the outsourcing parties for appropriate understanding to the security measures by the outsourcing parties.

5.2.2 Procurement and construction of information systems

(1) Measures when selecting equipment, etc.

The ISSM shall validate if the equipment, etc.is conformed to its selection criteria and use the result as one of the factors for its selection.

(2) Measures when constructing information systems

(a) When constructing information systems, the ISSM shall implement measures deemed necessary from perspectives of information security.

(b) When the constructed information systems are operationised, the ISSM shall take necessary information security measures for its procedures and migrating environment.

(3) Measures for inspections on delivery

[1] "List of security criteria for IT products procurement" (Ministry of Economy, Trade and Industry, available in Japanese "IT 製品の調達におけるセキュリティ要件リスト")

(a) The ISSM shall conduct validations and inspection at the time of delivery, following the inspection procedures prescribed in the specifications and so on, in order to ensure the procured equipment, etc. and the received information systems are conforming to the requirements for information security measures.

(b) The ISSM shall ensure that necessary information security measures are incorporated in the operationalised information system when the constructed system is taken over from the system constructor/developer to the parties in charge of system operation.

5.2.3 Operation and maintenance of information security

Measures for information systems during operation and maintenance

(a) The Head ISM shall appropriately operate the security functions incorporated to the system during its operation and maintenance.

(b) For the systems constructed based on the common platform system, the Head ISM shall appropriately operate the information systems under the operational management framework in accordance with the segregation of duties with other organisations which maintain, operate and manage the common platform system. The Head ISM shall also operate the information systems following the common platform system's operational management provisions and so on, in order to maintain the level of information security of entire common platform system.

(c) The Head ISM shall manage the records of operation and maintenance, in order to facilitate tracing of incidents such as malicious activities and unintended access to the systems.

(d) The Head ISM shall develop information security measures in emergencies if the Institute possesses information systems that support priority work of the Institute under emergencies.

(e) The Head ISM shall ensure that the information security measures in emergencies are implementable at training sessions, maintenance improvement, or other occasions.

5.2.4 Update and disposal of information systems

Measures for updating and disposal of information systems

When updating or disposing of information security systems, the Head ISM shall implement the following measures, taking into account of classifications and handling restrictions of the information stored in said systems.

(i) Information security measures for transferring data when updating information security systems.

(ii) Erasure of unnecessary data when disposing of information security systems

5.2.5 Revision of security measures for information systems

Revision of security measures for information systems

The Head ISM shall revise security measures and take necessary measures when information systems face new threats or other emerging conditions that require revision to the operation or monitoring of the information systems.

6. Security Requirements for Information Systems

6.1 Security Functions of Information Systems

6.1.1 User/entity authentication functions

(1) Implementation of the user/entity authentication functions

(a) The Head ISM shall implement the user/entity identification and authentication functions when identification and verification of authorised users/entities are necessary.

(b) The Head ISM shall set up criteria for user/entity authentication functions when online procedures are developed for applications, notification, etc. used between the Institute and the general public/the private sector upon the assessment of risks from online procedures.

(c) The Head ISM shall implement measures to prevent malicious activities caused by leakage of user/entity authentication information and so on, as well as the measures against unauthorised attempts of user/entity authentication.

(2) Management of the identification code and the user/entity authentication information

(a) The Head ISM shall implement measures to appropriately give identification code and user/entity authentication information to all the entities who access information systems, and manage them.

(b) The Head ISM shall implement measures to prevent malicious use of identification code and user/entity authentication information, soon after it becomes no longer necessary for the entity to use the information system.

6.1.2 Access control functions

Implementation of access control functions

(a) The Head ISM shall implement a function which enables only the authorised persons to set access control according to the characteristics of information systems, and the classification and handling restrictions of information handled in the systems.

(b) The Head ISM shall appropriately operate access control functions so as to surely restrict the entities who permit the access to information systems and information.

6.1.3 Authority control

Authority control

(a) The Head ISM shall set functions that allow only authorised persons to set access restrictions in accordance with the characteristics of the information systems, information classification, handling restrictions of information, etc.

(b) The Head ISM shall take measures to minimise damages in case the identification code and the user/entity authentication information of the authorised persons are stolen by a malicious third party, and to prevent them from inappropriate use or misuse by Users inside the Institute.

6.1.4 System logs retrieval and management

Event logs retrieval and management

(a) The Head ISM shall retrieve logs of information systems which are necessary to verify the information systems are appropriately used and free from unauthorised access and operation.

(b) After determining the purpose to retrieve logs according to the characteristics, the Head ISM shall determine items such as equipment, etc. in which logs should be retrieved, types of information recorded in the log, storage periods, log information handling methods from a viewpoint of classified information handling, as well as measures to implement when log retrieval is not possible, and appropriately manage the logs.

(c) The Head ISM shall establish a function to examine or analyze the logs retrieved from the information systems, and perform examinations or analysis to detect unauthorised access and

operations, etc. by malicious third parties, and so on.

6.1.5 Encryption and digital signatures

(1) Implementation of encryption and digital signature functions

(a) The Head ISM shall take the following measures to prevent leakage and manipulation of information handled by information systems:

(i) Examine the necessity of encryption functions for the information systems handling confidential information, and duly implement them when it is deemed necessary.

(ii) Examine the necessity of digital signature and verification functions for the information systems handling critical information, and implement them when it is deemed necessary.

(b) The Head ISM shall refer to the "e-Government Recommended Ciphers List" whose security and performance is confirmed by CRYPTREC (the Cryptography Research and Evaluation Committees) and shall establish operational methods of encryption and digital signature algorithm used on information systems, and safe protocol using it and operation method, which include the following items:

(i) For encryption and digital signature algorism used by employees and safe protocol using it, ensure the one in the "e-Government Recommended Ciphers List" (CRYPTREC) is to be applied where possible.

(ii) When introducing encryption or digital signature upon implementations or updates of information systems, apply algorithms in the "e-Government Recommended Ciphers List" and safe protocol using it, expect for unavoidable circumstances.

(iii) Establish emergency response procedures in the event that the algorithm is compromised or in the event that a vulnerability is found in safe protocol using it.

(iv) Establish procedures for managing keys for decryption of encrypted information, and for granting digital signatures

(c) When assigning a digital signature, information security officers shall ensure use of the digital certificate issued by the Government Public Key Infrastructure, if the one which is applicable and serves the purpose of digital signature is available with the GPKI, after examining the algorithm and operational methods of encryption and digital signature applied at their own government agencies.

(2) Management of encryption and digital signature

The Head ISM shall take the following measures to ensure proper use of encryption and digital signature

(i) For the information systems which assign digital signatures, securely provide the verifiers of signatures with information and methods of verifying the validity of the signatures

(ii) For the information systems which perform encryption, or those which perform assignment or verification of digital signatures, regularly obtain information on threats which compromise the algorithm selected for such operations or raise vulnerability in protocol, and share it with employees as necessary.

6.2 Measures against Information Security Threats

6.2.1 Measures against software vulnerabilities

Implementation of measures against software vulnerabilities

(a) When installing or starting operations of servers, terminals, and communication line equipment, the Head ISM shall implement measures against publicly disclosed vulnerabilities of the software used on said equipment.

(b) When the publicly disclosed information about vulnerabilities is yet to be known, and applicable measures for servers, terminals, and communication line equipment are available, the Head ISM shall implement such measures.

(c) When the information about vulnerabilities of the software used on servers, terminals, and communication line equipment becomes available, the Head ISM shall apply security patches, or establish plans for addressing software vulnerabilities and implement measures, after examining the effects upon software updates and so on.

(d) The Head ISM shall regularly verify the implementation status of measures against vulnerabilities of software, including the tailor made software used on servers, terminals, communication line equipment, and establish countermeasures such as applying security patches and upgraded software if any vulnerabilities with no relevant measures are identified.

6.2.2 Measures for protection against malware

Implementations of measures against malware

(a) The Head ISM shall install anti-malware software and other tools on server equipment and terminals. However, this shall not apply when there is no readily-available anti-malware software which is operational on said server equipment and terminals.

(b) The Head ISM shall take measures against malware, such as installing anti-malware software to protect all possible malware infection routes.

(c) The Head ISM shall regularly examine the implementation status of measures against malware as needed and take necessary measures.

6.2.3 Measures against denial-of-service attacks

Implementation of measures for denial-of-service attacks

(a) For information systems (referring to only those systems accessed through the internet, hereinafter the same in this section) handling vital information, the Head ISM shall implement measures for denial-of-service attacks, by using the functions incorporated in the equipment necessary for providing such services, like server equipment, terminals, and communication line equipment, or the methods offered by private business providers, and so on.

(b) For information systems handling vital information, the Head ISM shall construct information systems equipped with tools which minimise impacts of denial-of-service attacks.

(c) For information systems handling vital information, the Head ISM shall identify equipment to be monitored among the server equipment, terminals, communication line equipment, and communication lines which are subject to denial-of-service attacks, and conduct monitoring.

6.2.4 Measures against targeted attacks

Implementation of measures for targeted attacks

(a) The Head ISM shall implement measures for information systems which reduce targeted

attacks intrusions against the organisation (gateway measures).

(b) The Head ISM shall implement measures for information systems to immediately detect and respond to the intruded attacks, and to make expansion of the intrusion harder, as well as to detect and respond to unauthorised communication with external entities (internal measures).

6.3 Creation and provision of applications and contents

6.3.1 Measures upon creating applications and contents

(1) Establishment of provisions related to creation of applications and contents

The Head ISM should maintain provisions to prevent actions which cause deterioration of information security level of the systems other than those of their own government agencies when providing applications and contents.

(2) Formulation of security requirements for applications and contents

(a) The Head ISM shall include the following items in the specifications of applications and contents, in order not to deteriorate the level of information security of the users other than those of their own government agencies.

(i) Applications and contents to be provided shall contain no malware.

(ii) Applications and contents to be provided shall contain no vulnerability.

(iii) The contents shall not be provided in the executable program format, unless there is no other way to provide them.

(iv) If there are any means to verify that the applications and contents are authentic and free from manipulation, such as digital certificate and likewise is available, these shall be provided to the recipients of the applications and contents.

(v) When developing applications and contents, methods of providing them shall be selected to ensure the users of the operation system (OS) and software will not be prompted to change the setting which might deteriorate the information security level, including the changes which force them to use the OS version and software, etc. with vulnerabilities.

(b) Applications and contents should be developed ensuring not to contain such functions which allow the third parties to obtain the information of service users and other parties against their will, which are not essential for utilising the service.

(c) When outsourcing applications and contents development and creation, employees shall include the requirements in the preceding items in the procurement specification.

6.3.2 Measures upon providing applications and contents

(1) Use of the Institute's domain name

(a) The Head ISM shall specify the use of the Institute's domain name in the information systems specifications, so that the users other than those of the Institute can confirm that the websites are actually provided by the Institute itself. However, this shall not apply to what is set forth in section 4.1.3.

(b) When outsourcing the creation of a website targeting the users other than those of the Institute, the use of the Institute's name shall be specified in the procurement specifications, as stated in the preceding items.

(2) Prevention of users from being lured to malicious websites

The Head ISM shall implement measures to prevent Users from being lured, through pages such as search engine sites, to malicious websites which impersonate the Institute.

(3) Notification of applications and contents

(a) When notifying Users of applications and contents, Users shall implement the measures in order to ensure that general users are led to use said applications and contents.

(b) When notifying users of applications and contents provided by the parties other than the Institute, Users shall keep the validity of URL and so on in notification.

7. Information Systems Components

7.1. Terminals, Server Equipment

7.1.1. Terminals

(1) Measures when introducing terminals

(a) For terminals which handle classified information, the Head ISM shall implement measures against physical threats such as theft and unauthorised removal of terminals, unauthorised use of terminals by malicious third parties, as well as unauthorised viewing of display devices of terminals.

(b) To eliminate the possible increase in vulnerability due to use of variety of software, the Head ISM shall specify the software which is approved, or prohibited to be used on the terminals.

(2) Measures when operating the terminals

(a) The Head ISM shall periodically conduct a review of software which is approved, or prohibited to be used on the terminals.

(b) The Head ISM shall periodically verify the status of all software used on the terminals under their management, and implement corrective measures when identifying any terminal in inappropriate status, and so on.

(3) Measures when terminating the operation of terminals

(a) The Head ISM shall erase all the information stored on the external storage media of the terminal when terminating its operation.

(4) Measures for the terminals that are provided by the Institute and deal with Confidential Information (only for use outside the areas requiring control measures) and those for introducing and operating terminals that are provided by other than the Institute

(a) The Head ISM shall establish rules for the following security measures for the terminals that are provided by the Institute and deal with Confidential Information (only for use outside the areas requiring control measures) and those for introducing and operating terminals that are provided by other than the Institute

(i) Technical measures for preventing the information from being stolen, lost or stolen by malicious program infection, etc.

(ii) Measures for preventing the information from being stolen by malicious program infection, etc. from the use of terminals provided by other than the Institute

(b) The Head ISM shall specify the persons in charge of implementing security measures for information handling for the Institute's work through terminals provided by other than the Institute (hereafter referred to as "Terminal Managers." At the Institute, the Satellite ISMs

shall act as Terminal Managers.

(c) The following persons shall take security measures specified in (a) (i) for the use of the terminals by Users who handle Confidential Information:
  (i) Head ISM: Terminals provided by the Institute (only for use outside the areas requiring control measures)
  (ii) Terminal Managers (Satellite ISMs): Terminals provided by other than the Institute

(d) Terminal Managers shall ensure that Users take security measures for (a) (i) (except for those Users who cannot implement) and (a) (ii) when Users handle Confidential Information in the terminals provided by other than the Institute.

(e) Users shall take security measures for (a) (i) (except for those Users who cannot implement) and (a) (ii) when Users handle Confidential Information in the terminals provided by other than the Institute.

7.1.2. Server equipment

(1) Measures when introducing server equipment

(a) For server equipment which handles classified information, the Head ISM shall implement measures against physical threats such as theft and unauthorised removal of server equipment, unauthorised use of server equipment, as well as unauthorised viewing of display devices of server equipment.

(b) To prevent situations where services are suspended due to failure, excessive access, and other problems with information systems which handle vital information, the Head ISM shall ensure system's availability by setting up the server equipment for such services in a redundant configuration, and so on.

(c) To eliminate the possible increase in vulnerability due to use of variety of software, the Head ISM shall specify the software which is approved, or prohibited to be used on the server equipment.

(d) The Head ISM shall implement measures to prevent leakage of information sent and received while the server equipment maintenance is being performed via communication lines.

(2) Measures when operating the server equipment

(a) The Head ISM shall periodically conduct a review of software which is approved, or prohibited to be used on the server equipment.

(b) The Head ISM shall periodically verify the software and configuration of all server equipment under their management, and implement corrective measures when identifying any server equipment in inappropriate status, and so on.

(c) The Head ISM shall implement measures to monitor the server equipment in case it is necessary to detect the occurrence of unintended incidents such as malicious acts and unauthorised access to the server equipment. However, this shall not be applied if such monitoring is deemed unnecessary judging by the usage environment of the server equipment.

(d) For server equipment handling vital information, the Head ISM shall implement measures which enable to recover the operation in case where the server equipment becomes unavailable.

(3) Measures when terminating the operation of server equipment

The Head ISM shall delete all information stored on the external storage media of server equipment when terminating its operation.

7.1.3. Multifunction devices and equipment for specific purposes

(1) Multifunction devices

(a) When procuring multifunction devices, the Head ISM shall establish appropriate security requirements according to functions, installation environments, as well as classification and handling restrictions of information handled by such devices.

(b) The Head ISM shall implement measures for information security incidents against multifunction devices while in operation, by taking actions such as to appropriately set up the functions available on said devices.

(c) The Head ISM shall delete all information stored on the external storage media of multifunction device when terminating its operation.

(2) Equipment for specific purposes

For equipment for specific purposes, if there are possible threats depending on information handled, methods of use, and connection types of the communication lines and so on, the Head ISM shall implement measures suitable for the characteristics of said equipment

7.2. E-mail, Web, and others

7.2.1 E-mail

Measures when introducing e-mail services

(a) The Head ISM shall set up the e-mail servers, ensuring no unauthorised e- mail relaying occurs.

(b) The Head ISM shall provide functions of user/entity authentication when sending and receiving e-mails between e-mail clients and servers.

(c) The Head ISM shall implement measures to prevent e-mail spoofing.

(d) The Head ISM shall take security measures of encryption between e-mail servers to prevent the e-mails from tapped or falsified via internet.

7.2.2 Web

(1) Measures when introducing and operating webservers

(a) For management and setting of webservers, the Head ISM shall implement measures to ensure information security, including the following items.

(i) Unnecessary functions of webservers shall be suspended or restricted

(ii) Personnel responsible for editing web contents shall be limited.

(iii) Manage web contents to ensure no senseless nor prohibited contents shall be published.

(iv) Terminals used for editing web contents shall be restricted, and ID codes and user/entity authentication information shall be appropriately managed.

(v) If it is necessary to prevent information leakage caused by tapping and other incidents during communication, such as when communicating service users' personal data, the functions for encryption and authentication by digital certificates shall be provided.

(b) The Head ISM shall verify the information saved on webservers, and ensure no information unnecessary for providing services is stored therein.

(2) Measures when developing and operating web applications

When developing web applications, the Head ISM shall implement measures to eliminate known vulnerabilities of existing web applications. In addition, these measures shall be periodically reviewed during operation for any oversights, and appropriate action should be taken when identifying such oversights.

7.2.3 Domain Name Systems (DNS)

(1) Measures when introducing the DNS

(a) For the content servers which provide name resolution to information systems handling vital information, the Head ISM shall implement measures to ensure there is no interruption to the name resolution.

(b) For the cache servers, the Head ISM shall implement measures to ensure appropriate responses to the name resolution queries.

(c) When the content servers are used to provide the resolution of the names exclusive to their own government agency, the Head ISM shall implement measures to ensure no such information managed in said content server is leaked outside of the government agencies.

(2) Measures when operating the DNS

(a) When installing multiple DNS content servers, the Head ISM shall maintain consistency among the servers with regards to the information of the domains under their management.

(b) The Head ISM shall periodically verify the accuracy of the information about the domains managed on the DNS content servers.

7.2.4 Database

Measures when implementing or operating the database

(a) The Head ISM shall appropriately perform authority control of administrator's privileges to prevent malicious operations which are internally performed.

(b) The Head ISM shall implement appropriate measures to specify the users who access data stored in database.

(c) The Head ISM shall implement measures to detect malicious operations which are performed by a user having authority to access internal data.

(d) The Head ISM shall implement measures to prevent malicious operations of data, which abuses the vulnerabilities of database or equipment, etc.

(e) The Head ISM shall appropriately encrypt the data which have to be prevented from leaking caused by malicious method or theft of electric and magnetic storage media.

7.3 Communication Lines

7.3.1 Communication lines

(1) Measures when installing communication lines

(a) During the communication lines installation, the Head ISM shall select appropriate line types according to the classification and handling restrictions of the information handled by the information systems connected to the communication lines, and implement measures necessary for said lines to prevent impacts of information security incidents.

(b) The Head ISM shall have the communication lines equipped with the functions to perform access control and route control on the server equipment and terminals.

(c) The Head ISM shall implement measures to ensure the confidentiality of communication contents, if assuring the confidentiality thereof is deemed necessary when connecting

information systems handling confidential information to the communication lines.

(d) The Head ISM shall implement measures which enable them to confirm that the information system is the one approved to be connected to the communication lines.

(e) The Head ISM shall install communications line equipment in the areas requiring control measures. However, when it is difficult to install them in said areas, measures such as physical protections to keep the equipment from destruction and unauthorized operation by malicious third parties shall be implemented.

(f) The Head ISM shall implement measures to ensure continuous operation of communication lines connected to the information systems handling vital information.

(g) When connecting the internal communication lines to the external communication lines such as internet access lines and public communication lines, the Head ISM shall implement measures to ensure the information security of the internal communication lines and the information systems connected to them.

(h) The Head ISM shall implement measures to monitor communication contents sent and received between the internal communication lines and the external communication lines.

(i) The Head ISM shall specify the software required for operating communication line equipment and maintain/establish authorization procedures for changing software. This shall not be applied to the communication line equipment whose software is difficult to change.

(j) The Head ISM shall ensure information security of remote access, where communication line equipment is remotely accessed for maintenance and diagnosis.

(k) When using communication line services of telecommunication carriers, the Head ISM shall establish agreements, upon signing a contract with the outsourcing parties who construct information systems, on measures to ensure the level of information security of said line services as well as its service level.

(2) Measures when operating communication lines

(a) The Head ISM shall implement measures required to prevent information security incidents during the operation of communications line equipment.

(b) The Head ISM shall appropriately perform route control and access control, and review its settings when any change made to the communication lines and the requirements for establishing communication. This review shall also be conducted periodically.

(c) The Head ISM shall periodically check the status of software required for operating communications line equipment, and implement corrective measures if any improper status is detected, such as unauthorised software is installed on the equipment.

(d) In the event of incidents which endanger information security of certain information system, the Head ISM protect other information systems which share the communication lines with the endangered information system, by changing the line configuration to establish a closed and independent communication line, separated from the shared ones.

(3) Measures when terminating the operation of communication lines

(a) When terminating the operation of communication line equipment, the Head ISM shall take appropriate measures, such as erasing all the information recorded on the external storage media on said equipment to prevent leakage of information stored during the operation, in case that such equipment composing the communication lines are reused or discarded after

terminating its operation.

(4) Measures when introducing remote access environments

(a) When constructing a remote access environments which enables the connection to the information system of the government agency through the communications lines outside of government agencies, the Head ISM shall ensure information security of path and the system to access, for example, by installing the virtual private network (VPN) lines.

(5) Measures when introducing wireless LAN environments

When constructing the internal communication lines with wireless local area network (LAN) technologies, the Head ISM shall, on top of implementing the common measures for communication line construction, encrypt the communication routes to ensure the confidentiality of communication contents, then implement other measures required to ensure information security.

7.3.2 Internet Protocol version 6 (IPv6) communication lines

(1) Measures related to information systems with IPv6 communications

(a) When constructing information systems using IPv6 technologies for communication, the Head ISM shall select, when possible, a Phase-2 compliant product based on the IPv6 Ready Logo Program, as the equipment, etc. to procure.

(b) For information systems to be constructed are expected to perform communication with IPv6 technology, the Head ISM shall take into account the characteristics of IPv6 communication and so on, and review the threats and vulnerabilities including the following items, and shall implement necessary measures.

(i) Threats related to direct IP reachability via global IP addresses

(ii) Threats related to unauthorised access due to incomplete settings of IPv6 communication environments, and so on.

(iii) Vulnerabilities due to lack of consideration for the required process when IPv4 and IPv6 communications coexist in the information system.

(iv) Vulnerabilities due to lack of consideration for the required IPv6 addresses handling on the applications.

(2) Control and monitor for unintended IPv6 communications

When connecting server equipment, terminals and communications line equipment to communication lines for which no IPv6 communication is intended, the ISSM shall implement measures to control IPv6 communications in order to prevent information security threats caused by unauthorised IPv6 communications received from said lines, such as arrival of unexpected IPv6 communication packets as a result of automatic tunneling functions.

8. Use of Information Systems

8.1 Use of Information Systems

(1) Establishment of provisions related to the use of information systems

(a) The Head ISM shall establish provisions related to information security when using information systems at the Institute.

(b) For classified information, the Head ISM shall establish provisions and approval procedures

of security control measures for the cases that such information is processed outside of the areas requiring control measures, taking into account the risks of information leakage from the terminals and communication lines which are taken away from said areas.

(c) The Head ISM, when accepting the connection of the terminals that connect the communication lines outside the areas requiring control measures (including terminals provided by other than the Institute) with the Institute's communication lines inside the areas requiring control measures, shall establish provisions and procedures of security measures that considers the risks of malicious programme infection from the connection.

(d) The Head ISM shall establish procedures for handling information using external storage media, such as USB memories.

(i) Users shall use the external storage media that are provided by the Institute or those provided by the party that complies with the provisions for handling information specified under the contract with the Institute.

(ii) External storage media provided by the party in the above (i) shall be used only for the purpose of transferring information between the party and the Institute, and the necessary security measures shall be taken when information is put into or taken out of the said media.

(e) The Head ISM shall establish approval procedures for taking the external storage media that contains Confidentiality Class-3, Critical or Vital Information out of the areas under the control of the Institute.

(2) Measures to encourage information systems users to comply with the provisions

The Head ISM shall examine, from perspectives of information security risks and work efficiency, the scope of support functions which encourage employees to comply with the provisions, and shall construct the information systems equipped with such functions.

(3) Basic measures for the use of information systems

(a) Users shall not use information systems for non-work related tasks.

(b) Users shall not connect the information systems at the Institute to the communication lines other than the ones so authorised by the Head ISM.

(c) Users shall not connect the information systems which are not authorised by the Head ISM, to the internal communication lines at the Institute.

(d) Users shall not use any software prohibited to use on information systems. If using unauthorised software is required to execute work, an approval from the Head ISM shall be granted.

(e) Users shall not connect unauthorised equipment, etc.to information systems,

(f) In such cases when a User leaves the area where information systems are installed and there is a risk for unauthorised operation by third parties, he or she shall implement measures to protect the systems from unauthorised use.

(g) When processing data on mobile devices which handle Classified Information, Users shall implement the prescribed security control measures.

(h) Users shall receive approval from the Head ISM for the following cases of terminal use:

(i) When Confidential Class-3, Critical, or Vital Information is handled on the terminal provided by the Institute outside the areas requiring control measures

(ii) When Classified Information is handled on the terminal provided by entities other

than the Institute

(i) Users shall receive approval from the ISMs (Headquarters or Satellite) or ISSM and take the specified security measures when the terminal (including those provided by entities other than the Institute) that is being connected to the non-Institute communication line outside the areas requiring control measures is connected to the Institute's communication lines inside the areas requiring control measures.

(j) Users shall receive approval from the Head ISM when taking the external storage media that contains Confidentiality Class-3, Critical or Vital Information out of the areas requiring control measures.

(4) Measures when using e-mail and web

(a) When sending and receiving e-mails containing confidential information, Users shall use e-mail services provided by the servers which are operated by, or outsourced by the Institute.

(b) When sending information by e-mail to the parties other than the Institute, Users shall use the Institute's domain name as the domain name of such e-mail's sender address. However, this does not apply when such Users are already known to the recipients of said e-mail.

(c) When receiving suspicious e-mails, Users shall handle them following the prescribed procedures.

(d) When it is necessary to review the web client settings, Users shall not make any setting changes which might impact on the information security.

(e) When downloading the software to the server equipment or terminals on which the web client is running, Users shall check the integrity of the software by verifying its distributor's digital signatures.

(f) When inputting and submitting the confidential information in a web form on the website they are viewing, Users shall ensure the following:

(i) The contents to be submitted will be encrypted.

(ii) The website genuinely belongs to the organisation where the contents are intended to.

(5) Handling of identification codes and user/entity authentication information

(a) Users shall not use the information system by accessing the system through user/entity authentication with identification codes other than the ones assigned to them.

(b) Users shall appropriately manage the identification codes assigned to them.

(c) If a User is granted an identification code with administrator privileges, the use of such identification code shall be limited to only when they execute administrator's tasks.

(d) Users shall manage their user/entity authentication information with utmost care.

(6) Measures for the use of encryption and digital signatures

(a) Users shall follow the prescribed algorithms and methods when encrypting information, as well as assigning the digital signatures to the information.

(b) Users shall follow the prescribed key management procedures, and appropriately manage the keys for decrypting the encrypted information, as well as those for assigning digital signatures to information.

(c) Users shall take the backup of the key, following the prescribed backup procedures of the keys for decrypting the encrypted information.

(7) Prevention of malicious software infection

(a) Users shall make efforts to implement measures against malicious software infection.

(b) In case that a User becomes aware that an information system could have been infected by malicious software, he or she shall implement necessary measures, such as to immediately disconnect the infected information system from the communication lines.

8.2 Use of Terminals provided by entities other than the Institute

8.1.1 Use of terminals provided by entities other than the Institute

(1) Use of terminals outside the Institute

The Head ISM shall determine the use of terminal provided by entities other than the Institute considering the classification and handling restriction of the information that the said terminal is expected to handle, the security measures of the Institute, the fact that the terminal is managed primarily by the User of the terminal, and the level of the information security expected to be achieved.

(2) Establishment of provisions for use of terminal provided by entities other than the Institute

Head ISM shall establish procedures of granting approval and so on, when processing information for work on terminals provided by entities other than the Institute.

(3) Measures for the use of terminals provided by entities other than the Institute

(a) When processing information to execute work on terminals provided by entities other than the Institute, Users shall obtain an approval of the Terminal Managers in compliance requirements.

(b) Upon completion of information processing, Users shall delete the Confidential Information terminals outside the Institute.

9. Other matters

9.1. Mandate

Necessary matters concerning enforcement of the Policy shall be stipulated separately by the President/Chair of the Board of Directors.

9.2. Supplementary Provisions

The Policy became effective from 1 February 2021.

***

Annex

A.1 Examples of labelling for handling restrictions

Examples of labelling for restrictions in handling of Confidential Information

"No Distribution" or "Approval Required before Distribution" to information in case the information is not allowed or required approval for distribution. Similarly, no duplication, no printing, no transferring/forwarding, no transcribing, no reusing can be applied. Additional restrictions (recipient, date, etc.) can be added such as "Limited Distribution to (specific recipient)" or "No Distribution until (date)."
"Encryption Required for Stored or Transmitted"

Examples of labelling for handling restrictions of Critical Information

"Store until (date)," "Store at (location)," "No Editing," "No Deletion," "Disposed after Storing Period, " etc.

Examples of labelling for handling restrictions of Vital Information

"Must be Recovered within XX Days," "Store at (location)," etc.

A.2 Glossary

【A】

- “Areas requiring control measures” means areas under the control of the Institute where control measures for the facilities and environment are required to protect information.

【C】

- “Cloud service” means a capabilities which is offered via a paradigm for enabling network access to scalable and elastic pool of shareable physical or virtual resource with self-service provisioning and administration on-demand, by the provider-defined interface, and is flexible about setting of information security condition adequately.
- “Cloud service operator” means a provider offering the cloud service or a party which develops or operates the information system via the cloud service.
- “Common platform system” means information system shared by multiple agencies, excluding such information systems whose entire operations including hardware and software are controlled and managed by a single agency.
- “Communication line” means mechanisms for transmitting and receiving information among several information systems, and also among several equipment (including devices not purchased by the Institute), as well as between information systems and equipment, using prescribed communication protocol. Unless otherwise specified, it is a generic term referring to the communication lines used for information systems at the Institute. Communication line includes the one which is not directly managed by the Institute and also includes all connections regardless of their types (such as wire or wireless, physical or virtual).
- “Communication line equipment” means a device which connects communication lines, as well as communication lines and information systems, and controls information transmitted and received over these lines. Communication line equipment includes hubs, switches, routers, and firewalls.
- “Communication line outside the government agency” means a communication line other than “Communication line inside the government agency”.
- “CSIRT” means a system established at the Institute to respond to information security incidents which occur therein. An acronym for Computer Security Incident Response Team. “CYMAT” means a system established in the National center of Incident readiness and Strategy for Cybersecurity which provides proactive support for information security incidents which require unified actions with the government, in the event of, or fear of information security failure at the Institute due to cyber-attacks and so forth. An acronym for Cyber Incident Mobile Assistance Team (information security emergency supportteam).

【E】

- “Equipment, etc.” means a collective term for information systems components (such as servers, terminals, communication line equipment, multiple function devices and other apparatus for specified purposes, and software), as well as external storage media.
- “Equipment for specific purposes” means information system components for specific purposes as in the systems for TV conference, IP phones, and network cameras and so forth, which are connected to communication lines or equipped with external storage media.
- “External services on general terms and conditions” means information processing services by organisations other than the Institute such as private sectors, whose server equipment are used by the users to create, store, and transmit information. Those services which enable users to implement necessary and sufficient setting for information security shall not be in this category.

【I】

- “Information” means the information set forth in 1.1. (2) (b) of this Policy.
- “Information security incidents” means information security incidents set forth in JIS Q 27000:2014.
- “Information system” means systems consist of hardware and software (including those managed by outsourcing contractors), which are used for information processing or communications, and developed and procured by the Institute unless otherwise specified.

【L】

- “Labelling, etc.” means a measure to make information's classification clear to all who handle the information. This means to display the classification of information and any other actions to make the information classification a common knowledge. One of the examples of such measure is, to indicate the classifications of information recorded in a specific information system by describing them in regulations, and to make them known to all the users of said system.

【M】

- “Malware” (a short form for malicious programmes or software) means software in general which causes unsolicited results to information systems such as computer viruses, worms (not parasitic but self-replicating programmes), and spywares (programmes which collect various information against users’ will).
- “Mobile terminal” means, regardless of its type, a terminal designed to be carried around according to users’ business needs.

【O】

- “Outsourcing party” means an external contractor undertakes part of, or all of information processing tasks for the Institute.
- “Outsourcing” means contracting out part of, or all of information processing tasks of the Institute, including all types of contracts such as “mandate”, “quasi-mandate”, or “contract”.

【S】

- “Server equipment” means the components of information system which provide own services to terminals and other devices getting access to it via communication lines and other means (including components such as pre-loaded software, built-in mouse and keyboard), and unless otherwise specified those procured or developed by the Institute.
- “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 human- recognizable information such as characters or diagrams are written (hereinafter referred to as “hardcopies”), and those on which information unrecognizable by humans is recorded electronically or magnetically, and are processed by computers (hereinafter referred to as “electronic or magnetic data”, “external storage media”, respectively). The external storage media can be internal storage media built into server equipment, terminals, and communication equipment, or external storage media such as USB memories, external HDDs, and DVD-Rs.

【T】

- “Terminal” means the equipment of information system component which an employee directly operates (including the operating system and connected peripheral devices such as keyboard and mouse), and unless otherwise specified those procured or developed by the Institute. “Terminal” also means mobile terminals.