National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Information Security Countermeasures and Standards

September 23, 2016
Partial Revision: December 22, 2016
Partial Revision: March 1, 2018
Partial Revision: November 1, 2018
Partial Revision: March 27, 2019
Partial Revision: July 25, 2019
Partial Revision: September 10, 2019
Partial Revision: December 1, 2019
Partial Revision: July 9, 2020
Partial Revision: December 4, 2020
Partial Revision: June 24, 2021
Partial Revision: May 30, 2022
Decision by the Chief Information Security Officer

The following Countermeasures and Standards are established under Paragraph 3, Article 5 of the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Basic Rules on Information Security Countermeasures (NINS Rules No. 111 of 2016; hereinafter referred to as "Basic Rules").

Furthermore, for the terms of the Countermeasures and Standards, the same shall apply to the definitions specified in each item of Article 3 of the Basic Rules.

Table of Contents

1. Scope

Information assets subject to the Countermeasures and Standards shall be information assets provided for in Article 4 of the Basic Rules.

1.1. Those prescribed in the Countermeasures and Standards by the CISO provided for in the proviso of Paragraph 1, Article 4 of the Basic Rules

Those prescribed in the Countermeasures and Standards by the CISO provided for in the proviso of Paragraph 1, Article 4 of the Basic Rules shall be as follows.

(1) Visitors, guests in accommodation facilities, etc., use a configured LAN for the purpose of NINS providing internet access in such a way as to connect to the network and internet without using the global IP address managed by NINS and be physically or logically isolated from the network of NINS. Provided however, that the Information System Manager who installed the LAN must clearly indicate to the effect that NINS is not liable for any loss resulting from the use of the LAN on the users.

(2) Where a loan of networks, information systems, information facilities, equipment, or electromagnetic recording media is to be made based on the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Guidelines for the Loan of Fixed Assets, Etc. and where it falls under any of the following: Provided however, that, in principle, the information asset higher than confidentiality 2 shall be loaned after implementing “2) logical destruction (data destruction)” or “3) logical destruction (cryptographic key disposal)” in the “Information Asset Disposal Guidelines” when loaned, and at the time of return, lessee shall return after logical destruction pursuant to the form when lending. Considering the possibility of an information leakage arising from inadequate logical destruction by the lessee, the lessee's responsibility should be stipulated even if there is a leakage of information concerning the lessee from the relevant information asset after the return.

① Where the security policy to which the lessee is applied is indicated when the loan is to be made to a corporation.　Provided however, that in such case discord shall be avoided such as by indicating the applicable corporation’s security policy in the loan contract, etc.

(3) Provision of services, etc. to a person other than an executive officer or employee

Provision of services, etc. listed in any of the following items as recognized by the Institute CISO or Information System Manager and Information Security Officer to a person other than an executive officer or employee Provided however, that the application is limited to a person other than an executive officer or employee.

① Access to confidentiality 1 information

② Use of network that does not include information higher than confidentiality 2 (including logical isolation), information system, and electromagnetic recording media

③ Use of information system for the purpose of gathering information of a person other than an executive officer or employee (limited to those related to the input of information and upload of files)

1.2. Corresponding Rules

Corresponding requirements to the wording specified by these standards shall be as follows, in principle, unless otherwise provided for in additional notes in each item.

(1) Meaning of Necessity

The terms "must" and "shall" mean that the item is an absolute condition. On the other hand, the term "must not" means that the item is a prohibition.

(2) Meaning of Arbitrary

The term "may" mean that the item is an arbitrary requirement.

(3) Meaning of to Respond Immediately

The terms "immediately" and "instantly" mean as soon as possible from the time of grasping the event. The term "promptly" means as soon as possible within a few hours.

(4) Meaning of to Respond Without Delay

The term "without delay" means within a few days.

2. Organizational Structure, Duty, and Professional Responsibility

(1) Chief Information Security Officer (Article 5 of Basic Rules)

① The Chief Information Security Officer (hereinafter referred to as the "CISO") shall have the right of final decision and responsibility on the development, management, operation, and information security countermeasures of all information assets in the National Institutes of Natural Sciences (hereinafter referred to as "NINS").

② When the decision for determining the information security strategy has been made, the CISO shall properly notify the contents thereof to the relevant departments, agencies, etc. through the Institute Chief Information Security Officer.

③ In the event that an information security incident is recognized, the CISO must take into consideration the importance and extent of the impact and immediately make notification and public response to the Ministry of Education, Culture, Sports, Science and Technology, Ministry of Internal Affairs and Communications, and other responsible ministries and journalistic organizations in collaboration with each Executive Director in charge of general affairs, personal information protection, and public relations (in the event that the President designates the Vice President as the person in charge, this shall mean the Vice President; the same applies hereinafter.).

④ The CISO may appoint an expert who has expert knowledge and experience concerning information security, as needed, as the Information Security Advisor. (Article 10 of Basic Rules) The Information Security Advisor shall provide the CISO with technical advice concerning information security.

⑤ The CISO shall formulate a proposed basic plan on cyber security countermeasures (hereinafter referred to as “Basic Plan”) for a multi-year period composed of an overall objective, individual initiatives, and progress schedule and submit the matter to the Board of Directors.

⑥ In formulating the Basic Plan, threats against NINS, internal vulnerabilities, etc. must be brought to light and decisions must be made only after the analysis and assessment of the information security risk.

⑦ The CISO shall grasp the progress of the determined Basic Plan and share information with the Executive Director in charge of general affairs, Executive Director in charge of finance, and Manager in charge in the Administrative Bureau, and promote enhanced information security countermeasures in NINS.

⑧ The CISO may designate a deputy in the case where it is required. In this case, the CISO must notify the name, deputation period, and contact information of the deputy to the Institute Chief Information Security Officer.

(2) Institute Chief Information Security Officer (Article 6 of Basic Rules)

① The Institute Chief Information Security Officer (hereinafter referred to as the “Institute CISO”) must assist the CISO.

② The Institute CISO shall have the right of final decision and responsibility on the development, management, operation, and information security countermeasures of information assets in the institute, etc. under jurisdiction provided in Schedule 2 of the Basic Rules (hereinafter referred to as “Institute, etc. under Jurisdiction”.

③ The Institute CISO must promptly make a report to the CISO and General Information Security Officer (immediately in serious cases (including in cases where there is a possibility)) where an infringement of security over information assets has occurred or there is a risk of the infringement of security in the Institute, etc. under Jurisdiction.

④ The Institute CISO may designate a deputy in the case where it is required. In this case, the Institute CISO must notify the name, deputation period, and contact information of the deputy to the CISO, General Information Security Officer, and persons concerned in the Institute, etc. under Jurisdiction specified in 2.(3).

⑤ The Institute CISO shall designate based on the Information Security Policy with attention to taking the designated responsibility. In particular, the designation of the Information System Manager must give consideration for the expertise to be directly linked to the information security incident.

⑥ When the Information System Manager is designated based on Paragraph 1, Article 13 of the Basic Rules and when the Information System Manager intends to manage important servers (this shall mean an external public server and server dealing with important information including those storing information higher than confidentiality 3; the same applies hereinafter), after the confirmation of the expertise by the person designated by the Institute CISO or Institute CSIRT (hereinafter referred to as “Person to Confirm the Competency to Manage Important Servers”), the Institute CISO must respect the results and make designation. Furthermore, in the case the Person to Confirm the Competency to Manage Important Servers approves conditionally, the designation may be made conditionally.

⑦ Approval is included in the terms and conditions of the preceding paragraph by including the expertise of the Person in Charge of Information System under the control of Information System Manager; provided however, that in the case the terms and conditions changed due to retirement or transfer of the Person in Charge of Information System, after the Information System Manager contacts the Institute CISO the confirmation of expertise in the preceding paragraph must be obtained again.

⑧ With regard to the case where the Information System Manager other than the Information System Manager designated pursuant to ⑥ (hereinafter referred to as “Important Server Administrator”), the preceding paragraph is applied mutatis mutandis.

⑨ The Institute CISO may confirm the expertise of the Important Server Administrator to the Person to Confirm the Competency to Manage Important Servers at any time as deemed necessary and take measures including imparting conditions designation cancellations, etc. as needed.

⑩ When an application for a software to be installed in Important Servers is filed by the Important Server Administrator, the Institute CISO shall grant permission after examining the application. Furthermore, measures that should be taken as needed must be clearly indicated when permitted.

⑪ The Institute CISO may delegate the examination in the preceding paragraph as needed.

⑫ The Institute CISO must prepare a guideline about matters to implement in handing over Important Servers under jurisdiction of the Important Server Administrator to a successor (hereinafter referred to as the “Important Server Succession Guideline”).

(3) General Information Security Officer (Article 11 of Basic Rules)

① The Information Security Officer in the Administrative Bureau shall serve as the Information Security Officer directly attached to the CISO and be positioned to be the General Information Security Officer.

② The General Information Security Officer must assist the CISO.

③ The General Information Security Officer must prepare an emergency contact network including a contact system that will cover the CISO, Institute CISO, General Information Security Manager, and Information Security Officers in order to contribute to liaison in cases of emergency.

④ The General Information Security Officer must promptly report to the CISO in cases of emergency.

⑤ The General Information Security Officer may designate a deputy in the case where it is required. In this case, the General Information Security Officer must notify the name, deputation period, and contact information of the deputy to the CISO and Institute CISO.

(4) Information Security Officer (Article 11 of Basic Rules)

① The Information Security Officer must assist the Institute CISO.

② The Information Security Officer shall have the right and responsibility to provide instructions based on the Information Security Policy and Implementation Regulations and the Manual, etc. issued thereunder by the CISO and Institute CISO (hereinafter referred to as the "Information Security Policy, etc.") on the development, change in setting, operation, review, etc. in the network and information system of the Institute, etc. under Jurisdiction and on the management, etc. of other information assets.

③ The Information Security Officer shall have the right and responsibility to give instructions based on the Information Security Policy, etc. on Information Security Countermeasures of the Institute, etc. under Jurisdiction.

④ The Information Security Officer shall have the right to provide guidance and advice on information security to the Information Security Manager, Information System Manager, and Person in Charge of Information System of the Institute, etc. under Jurisdiction.

⑤ The Information Security Officer shall have the right and responsibility to engage in maintenance and management of the information security implementation procedures on information assets of the common network, information system, etc. of the Institute, etc. under Jurisdiction.

⑥ The Information Security Officer must prepare an emergency contact network including a contact system that will cover the Institute CISOs, Information Security Officer, Institute CSIRT, and Information Security Manager (hereinafter referred to as "Institute Emergency Contact Network") in order to contribute to liaison in cases of emergency.

⑦ For the Institute Emergency Contact Network, a review shall be carried out once or more times a year and if any change has occurred, this shall be submitted to the Institute CISO and General Information Security Officer.

⑧ The Information Security Officer shall provide the preparation of a contact system in cases of emergency, compilation of opinions related to compliance with Information Security Policy, and education, training, advice, and instructions to executive officers, employees, researchers involved in joint utilization or joint research, etc. on the information system held in the Institute, etc. under Jurisdiction.

⑨ The Information Security Officer may designate a deputy in the case where it is required. In this case, the Information Security Officer must notify the name, deputation period, and contact information of the deputy to the Institute CISO and persons concerned in the Institute, etc. under Jurisdiction.

⑩ The Information Security Officer shall have the right to conduct necessary inspections, etc. for monitoring the execution of rights of the Information System Manager.

⑪ The Information Security Officer must prepare an information asset ledger pertaining to network and information system in the Institute, etc. under jurisdiction and an external electromagnetic recording media management ledger in the Institute, etc. under jurisdiction. The preparation shall be made by March 31,2020.

⑫ The information asset ledger must include necessary items in terms of management such as the name, location, classification, specification, personal information preservation (applicable or not), specific personal information preservations (applicable or not), encryption of installed electromagnetic recording medium, and user, etc.

⑬ The external electromagnetic recording media management ledger must include necessary items in terms of management including the confidentiality classification and user, etc.

(5) Deputy Information Security Officer (Article 11 of Basic Rules)

① The Institute CISO may designate a Deputy Information Security Officer by designating the appointment period and scope of jurisdiction in cases where found to be necessary based on the request by the Information Security Officer.

② The appointment period of the Deputy Information Security Officer and scope of conduct in the Institute, etc. under Jurisdiction must be clearly indicated when the Information Security Officer intends to make a request to the Institute CISO provided in ①.

③ The appointment period provided for in ① shall be for a maximum of 2 years and the Deputy Information Security Officer may be reappointed. Furthermore, when the Deputy Information Security Officer loses eligibility as an employee of NINS, the appointment period shall expire on the day preceding that day.

④ The Deputy Information Security Officer shall have the authority and duty of the Information Security Officer within the designated scope of jurisdiction and appointment period and the Information Security Officer shall lose these.

⑤ The Institute CISO must notify the name and contact information of the Deputy Information Security Officer to the CISO, General Information Security Officer, and persons concerned promptly in case the Deputy Information Security Officer is appointed.

⑥ The Information Security Officer shall supervise the Deputy Information Security Officer.

⑦ The request in ① may not be issued by the Deputy Information Security Officer. Furthermore, the Institute CISO may not redundantly appoint the Deputy Information Security Officer in the scope of jurisdiction.

(6) CSIRT (Article 12 Basic Rules)

① The CSIRT is an organization in charge of the core of incident management in NINS and shall correspond to computer security incidents (defined as events considered as security issues in the operation of the information system and same as the definition of NIST (National Institute of Standards and Technology)).

② The Institute CSIRT shall prepare for the prevention, countermeasures, and supervision of incident outbreaks and deal, etc. with such incidents during and after the occurrence thereof in each institute.

③ The Institute CSIRT may give advice about computer security incident countermeasures to the Institute CISO, Information Security Officer, and Information System Manager. Furthermore, the Institute CSIRT shall respond to any request for advice made by the Information Security Officer and Information System Manager.

④ The Institute CSIRT may exercise the authority of the Institute CISO to which he/she belongs in regard to incidents and take measures or order for urgent temporary suspension and network cut off immediately notwithstanding the instructions of the Institute CISO and Information Security Officer when prompt response is deemed necessary for the purpose of preventing damage or attack in case of the occurrence of incidents (including the case of possible occurrence).

⑤ The Institute CSIRT has a Team Leader who is appointed by the Institute CISO.

⑥ The Team Leader is to conduct the review, coordination, etc. in relation to the handling of the Institute CSIRT.

⑦ The CSIRT has a General CSIRT Leader who shall serve as the Team Leader of the Administrative Bureau, etc. provided in Schedule 2 of the Basic Rules.

⑧ The Team Leader can offer opinions to Executive Officers, Director General provided for in Item (i), Paragraph 1, Article 6 of the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, General Rules for Organization and Operation(General Rules No.1, 2004) under jurisdiction, Secretary General provided for in Paragraph 3, Article 17, and Director of NINS-run research facilities provided for in Paragraph 1, Article 2-2 deemed necessary from the perspective of information security as Institute CSIRT; provided however, that when opinions are offered to Executive Officers, the Team Leader must coordinate with the General CSIRT Leader.

⑨ The Institute CSIRT must set forth all Important Servers that are considered especially important and other Important Servers subject for inspection by random extraction, etc., confirm the installation, etc. of the servers periodically, and where a problem is seen, instructions to rectify, etc. must be issued to the Important Server Administrator of the server and reported to the Institute CISO.

⑩ If the Team Leader judged that is it is necessary to confirm the expertise of the Important Server Administrator in the Institute, etc. under Jurisdiction, the Institute CISO may clearly indicate said reason and request reconfirmation to the Institute CISO.

⑪ The General CSIRT Leader is to take into consideration the content of the computer security incident and if contacting the external CSIRT, JPCERT Coordination Center (JPCERT/CC), Information-technology Promotion Agency, Japan (IPA), etc. (hereinafter referred to as “CSIRT, etc. Outside the Organization”) is generally accepted, have approval from the CISO and Institute CISO where the computer security incident happened and contact CSIRT, etc. Outside the Organization

⑫ The General CSIRT Leader may request the Team Leader of the Institute CSIRT where the computer security incident happened to contact the CSIRT, etc. Outside the Organization set forth in ⑧ as needed.

⑬ The General CSIRT Leader must compile the incidents that occurred in NINS each fiscal year and report them to the CISO in addition to working to coordinate the Institute CSIRT, coordinate and share information with CSIRT, etc. Outside the Organization.

(7) Information Security Manager (Article 16 of Basic Rules)

① The Information Security Manager shall have authority and responsibility in relation to classification and specification of information handled in the network and information system and Information Security Countermeasures of divisions, etc. under jurisdiction (Item (v), Article 3 of the Basic Rules; hereinafter referred to as “Information Handled under Jurisdiction”).

② The Information Security Manager must promptly make a report to the Incident Report Desk of Each Institute provided in 2.(13)② where an infringement of security over Information Handled under Jurisdiction has occurred or there is a risk of the infringement of security and seek the instructions of the Information Security Officer.

③ The Information Security Manager must prepare the “Handling Procedures” that compiles the information handling precautions, etc. in the handling department where information higher than confidentiality 3 is handled.

(8) Information System Manager (Article 13 of Basic Rules)

① The Information Security Manager shall have the right and responsibility to engage in management, development, change in setting, operation, review, etc. of the network under jurisdiction (Item (i), Article 3 of the Basic Rules), information system (Item (ii), Article 3 of the Basic Rules), information facilities and equipment (Item (iii), Article 3 of the Basic Rules), and electromagnetic recording media (Item (iv), Article 3 of the Basic Rules), and system related documents (Item (vi), Article 3 of the Basic Rules) (hereinafter referred to as “Information System, etc. under Jurisdiction”).

② The Information System Manager shall have authority and responsibility concerning information security of the Information System, etc. under Jurisdiction.

③ The Information System Manager shall have responsibility for the maintenance and management of the information security implementation procedures of the Information System, etc. under Jurisdiction.

④ The Information System Manager must prepare the information asset ledger pertaining to network and information system under jurisdiction.

⑤ The Information System Manager must prepare the external electromagnetic recording media management ledger pertaining to external electromagnetic recording media under jurisdiction.

⑥ The Information System Manager must not manage Important Servers or where the Information System Manager has not received the designation as an Important Server Administrator from the Institute CISO.

⑦ The Information System Manager designated as the Important Server Administrator must prepare a system configuration catalog, etc. for Important Servers and submit it to the Institute CISO. The Institute CISO must make matters available for inspection by the Institute CSIRT.

⑧ In cases where the Important Server Administrator seeks to install software to Important Servers (including when an outsourced party, etc. carries out the installation), the Important Server Administrator must present the necessity, the system configuration catalog, etc. and obtain permission after applying to the Institute CISO.

⑨ The permission of the Institute CISO of the preceding paragraph shall apply mutatis mutandis when Important Servers are newly installed (including when installed servers are newly treated as Important Servers).

⑩ For the Important Server Administrator, the handing over Important Servers under jurisdiction must be made in accordance with the Important Server Succession Guideline.

⑪ For the Information System Manager, action must be taken to address request for cooperation and consultation within the range possible from other Information System Managers.

(9) Person in Charge of Information System (Article 14 of Basic Rules)

① The Person in Charge of Information System shall engage in work including the management, development, change in settings, operation, and update of the information system, etc. under jurisdiction in accordance with the instructions, etc. of the Information System Manager.

② The Person in Charge of Information System shall manage external electromagnetic recording media in accordance with the instructions, etc. of the Information System Manager.

③ The Person in Charge of Information System shall make entries to the information asset ledger and external electromagnetic recording media management ledger in accordance with the instructions, etc. of the Information System Manager.

(10) Information Security Committee (Article 17 of Basic Rules)

① The Information Security Committee must confirm the implementation state of the Basic Plan, results of the audit provided for in Article 25 of the Basic Rules (hereinafter referred to as “audit”) and results of the self-inspection provided for in Article 26 of the Basic Rules (hereinafter referred to as “self-inspection”) each fiscal year.

② The Information Security Committee may suggest improvement measures to the CISO as needed based on the implementation state of the Basic Plan, audit and self-inspection results, etc.

③ The CISO may seek the opinion of the Information Security Committee concerning the Basic Plan, etc.

(11) Institute Information Security Committee (Article 18 of Basic Rules)

An Institute Information Security Committee led by the Institute CISO in the institute, etc. as the chairperson shall be established to carry out Information Security Countermeasures to be treated individually in each institute, etc. and make decisions on important matters concerning Information

Security in institutes, etc.

(12) Prohibition of Concurrent Service (Article 19 Basic Rules)

① In the implementation of the Information Security Countermeasures, except in cases of urgent necessity, the person who applies for the approval or permission and the person who makes the approval or person who grants the permission must not be the same person.

② In the information security audit, the person who is audited and person who conducts the audit must not be the same person.

③ The Person to Confirm the Competency to Manage Important Servers provided for in 2.(2)⑥ and the Information System Manager who will receive the confirmation of competency, except in cases of urgent necessity, must not be the same person.

(13) Unified Support Desk Concerning Information Security and Support for Receiving External Reports

① The unified support desk concerning information security of NINS shall be Planning Coordination Section, Liaison and Planning Division, Administrative Bureau.

② In regard to the unified support desk concerning information security incidents in NINS (hereinafter referred to as "Incident Report Desk of Each Institute") and information security incident on information assets of the information system, etc. in NINS, the following shall be established as a support desk for receiving external reports (hereinafter referred to as "External Reporting Desk").

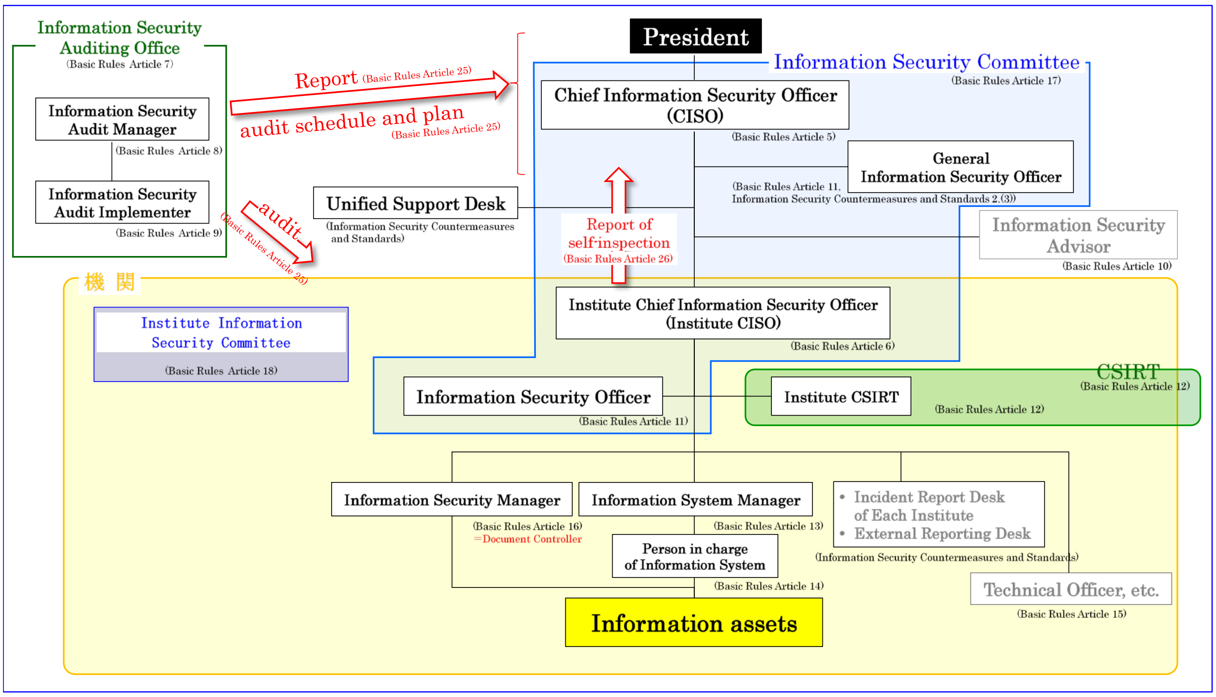
Category Including Institutes (Schedule II of the Basic Rules)	Incident Report Desk of Each Institute	External Reporting Desk
National Astronomical Observatory of Japan	Information Security Office	General Affairs Section, General Affairs Division
National Institute for Fusion Science	Information Network Group, Division of Information and Communication Systems	Planning and Evaluation Section, General Affairs Division, Department of Administration
Three Okazaki Institutes	Incident Report Desk of Each Institute of three Okazaki Institutes	Information Service Section, General Affairs Division, General Affairs Department, Okazaki Administration Center
Administrative Bureau, etc.	Planning Coordination Section Liaison and Planning Division Administrative Bureau	Planning Coordination Section Liaison and Planning Division Administrative Bureau

Note: In regard to the Center for Novel Science Initiatives specified in Item (i), Article 2-2 of the General Rules for Organization and Operation, Astrobiology Center specified in Item (ii) of the same article, and International Research Collaboration Center specified in Item (iv) of the same article, research laboratories belong to them shall contact with the Incident Report Desk where the laboratory is located.

③ The Institute CISO shall establish the Incident Report Desk of Each Institute and External Reporting Desk and when these desks have received reports of information security incidents from departments, etc., they shall confirm the status and establish a system for reporting to them.

④ The Institute CISO must announce the line of communication to the External Reporting Desk publicly.

Control Diagram (Basic Rules on Information Security Countermeasures)


Information Security Auditing Office
(Basic Rules Article 7)
Information Security Audit Manager
(Basic Rules Article 8)
Information Security Audit Implementer
(Basic Rules Article 9)
Report (Basic Rules Article 25)
audit schedule and plan (Basic Rules Article 25)
audit
(Basic Rules Article 25)
Unified Support Desk
(Information Security Countermeasures and Standards)
President
Information Security Committee
(Basic Rules Article 17)
Chief Information Security Officer (CISO)
(Basic Rules Article 5)
General Information Security Officer
(Basic Rules Article 11, Information Security Countermeasures and Standards 2.(3))
Report of self-inspection
(Basic Rules Article 26)
Information Security Advisor
(Basic Rules Article 10)
機 関
Institute Information Security Committee
(Basic Rules Article 18)
Institute Chief Information Security Officer (Institute CISO)
(Basic Rules Article 6)
Information Security Officer
(Basic Rules Article 11)
CSIRT
(Basic Rules Article 12)
Institute CSIRT
(Basic Rules Article 12)
Information Security Manager
(Basic Rules Article 16)
=Document Controller
Information System Manager
(Basic Rules Article 13)
Person in charge of Information System
(Basic Rules Article 14)
• Incident Report Desk of Each Institute
• External Reporting Desk
(Information Security Countermeasures and Standards)
Technical Officer, etc.
(Basic Rules Article 15)
Information assets

(14) Information System Manager Support Desk

The Institute CISO must establish a tech support desk intended to support Information System Managers and inform them.

3. Classification and Management Approach of Information Assets

(1) Classification of Information Assets

The information assets in NINS shall be subjected to classification and rating of confidentiality, integrity, and availability based on Article 20 of the Basic Rules and handling restrictions specified in Schedule 1 of the Basic Rules.

① Subdivision of Classification and Rating

The Institute CISO may subdivide the classification and rating of information assets provided for in Schedule 1 of the Basic Rules by providing separately and apply the handling restrictions, etc. within a range that satisfies the Basic Rules and Countermeasures and Standards.

Subdivision shall be created by means of providing a branch number to the classification in Schedule 1 of the Basic Rules.

(2) Management of Information Assets

① Responsibility for Management

(i) The Information Security Manager shall have the responsibility for management regarding information assets under jurisdiction.

(ii) If information assets (limited to those falling under the category of Items (v) and (vi), Article 3 of the Basic Rules; hereinafter referred to as "information data assets") were reproduced or transmitted, reproduced, etc. information assets must also be managed based on the classification in (1).

② Indication of the Classification of Information Assets

Employees, etc. (means all persons who are employed based on the Employee Regulations provided by NINS; the same applies hereinafter) must indicate the classification and rating of information assets in accordance with the instruction of the Information Security Manager in relation to the information assets set forth in (i) below and properly manage such as clearly indicating the handling restrictions as needed; provided however, that when the rating of information assets is 1 (confidentiality 1, integrity 1, and availability 1), the indication may be omitted.

The Information System Manager must indicate the classification and rating of information assets for the information assets set forth in (ii) and (iii) below; provided however, that the indication may be omitted for those lower than confidentiality 2, integrity 1, and availability 1. (Note that the omission of those lower than confidentiality 2 is on the premise of proper disposal according to the Guidelines for Data Disposal.)

(i) Item (v), Article 3 of the Basic Rules (information handled in networks and information systems) and Item (vi) of the same article (system related documents)

For files (data), indicate in file names, etc. For printed documents, indicate in the top margin, etc. of the document.

(ii) Item (ii), Article 3 of the Basic Rules (Information system)

Without an impact on the performance, conditions for use, etc., indicate in a label, etc. in an easy-to-find and hard to peel away place.

(iii) Item (iv), Article 3 of the Basic Rules (electromagnetic recording media)

Indicate in a label, etc. anywhere on the case or exterior of the electromagnetic recording media; provided however, that for internal electromagnetic recording media, when it is indicated in the case to which the electromagnetic recording media is contained, it is not necessary to indicate in the electromagnetic recording media

③ Preparation of Information

(i) The person who prepares the information must specify the classification and handling restrictions of the information based on the classification in (1) when preparing information in accordance with instructions from the Information Security Manager.

(ii) The person who prepares the information must also prevent the loss, leak, etc. of information in the course of preparation. Furthermore, when the information becomes unnecessary in the course of its preparation, it must be deleted.

(iii) The Information Security Manager or Information System Manager must give due consideration to handling restrictions based on the confidentiality classification, management of access authority, service continuity, etc. and take countermeasures against alteration or deletion when the information is stored for a long period of time to information assets that falls under item (iv), Article 3 of the Basic Rules.

④ Obtaining Information Assets

(i) A person who obtains information assets prepared by executive officers, employees, etc. of NINS must handle them based on the classification of the source information assets.

(ii) A person who obtains information assets prepared by a person other than executive officers, employees, etc. of NINS must specify the classification and handling restrictions of the information based on the classification of the information assets.

(iii) A person who obtains information assets must ask the Information Security Manager for his/her decision when the classification of the information assets is uncertain.

⑤ Use of Information Assets

(i) A person who uses information assets must not use information assets for purposes other than for operations unless permitted by the Institute CISO.

(ii) A person who uses information assets must properly handle them depending on the classification of the information assets.

(iii) A person who uses information assets must handle electromagnetic recording media in accordance with the optimal classification when multiple information of different classifications of information assets is recorded in the same electromagnetic recording media.

⑥ Storage of Information Assets

(i) The Information Security Manager or Information System Manager must properly store information assets in accordance with classification.

(ii) The Information Security Manager or Information System Manager must take measures of write-protect (including taking countermeasures against alteration or deletion by WORM (Write Once Read Many) media including DVD-R) when electromagnetic recording media of information data assets is stored for a long period of time.

(iii) The Information Security Manager or Information System Manager must give due consideration for the possibility of suffering from natural disasters and take necessary measures such as storing in an area having a very low possibility and multiple storage in a different location when electromagnetic recording media of data acquired as backup of electromagnetic recording media or information system with low frequency of use are stored for a long period of time.

(iv) The Information Security Manager or Information System Manager must store electromagnetic recording media in a fire resistant, heat resistant, water resistant, humidity resistant, and lockable location when electromagnetic recording media of information higher than confidentiality 3, higher than integrity 2, and availability higher than 2 are stored.

⑦ Transmission of Information

A person who transmits information higher than confidentiality 2 by email, cloud service, etc. (including external services provided for in Standards 8) must encrypt the information based on appended form 2 “Encryption Guidelines”.

For information higher than confidentiality 3, the transmission of information is prohibited by email in principle.

⑧ Transport of Information Data Assets, Etc.

(i) A person who transports information data assets higher than confidentiality 2 (including cases when entrusting transport) by a vehicle, etc. and information assets in which information data assets are recorded (hereinafter referred to as “information data assets, etc.”) must always take measures to prevent the illegal use of information data assets, etc. (store it in a lockable case, etc., encrypt the information data asset, establish a storage password, etc.) with regard to information data assets higher than confidentiality 3, etc. as needed in regard to information data assets higher than confidentiality 2, etc.

(ii) A person who transports information data assets higher than confidentiality 3 (including cases when entrusting transport) must clearly indicate the conservation measures to be taken in transport, impact in the event of a data breach, and other necessary matters to the Information Security Manager and obtain his/her permission.

⑨ Provision and Publication of Information Data Assets

(i) A person who provides information data assets higher than confidentiality 2 outside must encrypt based on the “Encryption Guidelines” listed in appended form 2 as needed.

(ii) A person who provides information data assets higher than confidentiality 2 must obtain the permission of the Information Security Manager unless otherwise provided for in the separate handling pursuant to the rules, regulations, and other contracts of information assets designated by the Institute CISO and NINS.

⑩ Disposal of Information Assets

(i) A person who disposes information assets higher than confidentiality 2 must dispose electromagnetic recording media in accordance with the "Guidelines for Data Disposal" in appended form 1 when the electromagnetic recording media of information become unnecessary.

(ii) The Information System Manager shall prepare a record in regard to the disposal of information assets (date and time, person in charge, and disposal details (disposal method, outsourcing company when outsourced, etc., and evidence based on the Guidelines for Data Disposal)) when having disposed of information assets that fall under information systems prescribed in Item 2, Article 3 of the Basic Rules rated as higher than confidentiality 3 or electromagnetic recording media prescribed in Item 4 and submit it to the affiliated Information Security Manager after attaching a copy of said information asset ledger or external electromagnetic recording media management ledger. The Information Security Manager shall store the record for 30 years (same as “books recording the status of transfer or disposal of corporate document files, etc.” in the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Corporate Document Management Rules).

4. Physical Security

4.1. Management of Servers, Etc.

(1) Installation of Devices

The Information System Manager shall take appropriate measures as needed such as installing in locations in which the impact of fire, flood, dirt, vibration, temperature, humidity, etc. are eliminated as far as possible, and fixing appropriately so as not to be easily removed when servers and other devices are attached.

(2) Redundancy of Servers

In consideration of the availability, etc., of networks, information systems, information facilities and equipment, the Information System Manager must make efforts so that they have a reasonable redundant configuration.

(3) Power Supply of Devices

① The Information System Manager shall coordinate with the Information Security Officer and Facility Administration Section, confirm the power supply system in regard to the power supply of servers and other devices, and install a reserve power source with the capacity of adequately supplying sufficient power until the time that the device is disconnected as needed in cases where power cuts are likely in the system.

② The Information System Manager shall coordinate with the Information Security Officer and Facility Administration Section and take measures to protect servers and other devices in cases where the impact of overcurrent from lightning, etc.

(4) Communication Cables and Other Wirings

① The Information Security Officer and Information System Manager must coordinate with the Facility Administration Section and take measures as needed to prevent damage, etc. of communication cables and power supply cables.

② The Information Security Officer and Information System Manager must take protective measures for accessible locations to communication cables including public spaces.

③ The Information Security Officer and Information System Manager must manage appropriately such as installing in a location where network connecting ports (hub ports, etc.) will not be easily accessed by others, locking of connecting ports, or preventing devices to get through the network even when connected unless in the case of connection by the method prescribed by the Information Security Officer in advance.

④ The Information Security Officer and Information System Manager must provide measures which prevents any person who is not an outsourced company who is allowed to operate by the Information Security Officer and Information System Manager, Person in Charge of Information System, or by contract to change and add the wiring as needed.

(5) Periodic Maintenance and Repair of Devices

① The Information System Manager must implement periodic maintenance and inspection of servers higher than availability 2 and other devices as needed.

② When devices with built-in electromagnetic recording media that store data that fall under the classification higher than confidentiality 3 are to be repaired by external companies, the Information System Manager must have the devices in a state where the content is deleted or in a state where the electromagnetic recording media are removed. When this measure may not be taken, the Information System Manager must maintain security by confirming the system of maintenance of confidentiality, etc. in addition to concluding a non-disclosure agreement with companies who are outsourced the repair when having external companies repair malfunctions.

(6) Installation of Servers Outside NINS

The Information Security Officer and Information System Manager must obtain the approval of the Institute CISO when servers other than in real property owned or rented by NINS are installed. Furthermore, the information security countermeasure situation of devices must be checked periodically.

(7) Disposal, Transfer, etc. of Devices

After deleting all information in accordance with the "Guidelines for Data Disposal" in appended form 1, when devices that store data that fall under the classification higher than confidentiality 2 are disposed, returned at the end of the lease, transferred, etc. the Information System Manager must take measures to make it impossible to restore; provided however, that when transferred to other national university corporations, etc. it is certain that the appropriate information security policy is applicable at the transferee and this does not apply when the approval of the Institute CISO was obtained without violating various rules of NINS.

4.2. Management of Information Management Areas (Information System Office, etc.)

(1) Structure, etc. of the Information Management Areas

① The Information Management Areas are rooms where network backbones and important information systems are installed and the management and operation of devices, etc. are conducted (hereinafter referred to as “Information System Rooms”) and storerooms of electromagnetic recording media.

② The Information Security Officer and Information System Manager shall establish Information Management Areas in the 2nd floor or higher in principle and must give due consideration so that it is not easily intruded from outside when compelled to establish Information Management Areas in the basement or 1st floor.

③ Doors connected to the outside from Information Management Areas shall be the minimum necessary and the Information Security Officer and Information System Manager must make efforts to prevent unauthorized entry with locks, monitoring functions, warning devices, etc. in collaboration with the Facility Administration Section.

④ The Information Security Officer and Information System Manager must take earthquake-resistant measures including toppling and fall prevention, fire prevention measures (installation of clean agent fire extinguishers, etc.), waterproofing, and other measures as needed for devices, etc. within Information System Rooms.

⑤ The Information Security Officer and Information System Manager shall make efforts to fully block off openings under the floor including outer walls enclosing the Information System Rooms in collaboration with the Facility Administration Section.

⑥ The Information Security Officer and Information System Manager must give due consideration so that fire-extinguishing agents, fire defense equipment, etc. installed in Information Management Areas do not have an impact on the devices, etc. and electromagnetic recording media.

⑦ The Information Security Officer and Information System Manager must give due consideration in the operation and maintenance of air-conditioning (exhaust heat) facilities and information systems in regard to the power supply in Information Management Areas in collaboration with the Facility Administration Section.

(2) Access Control, etc. of the Information Management Areas

① The Information System Manager shall restrict access to Information Management Areas only to those who have been granted permission in principle using IC cards, biometrics, etc. including fingerprint authentication and record an access log.

② Executive officers, employees, and outsourced companies must carry an identification card and present it upon request.

③ The Information System Manager shall take the following countermeasures as needed when visitors from outside enter Information Management Areas.

(i) Restrict Entry Areas

(ii) Attendance of executive officers, employees, etc. who have been granted permission to access Information Management Areas

(iii) Measures that can distinguish external visitors from executive officers, employees, etc.

④ The Information System Manager must ensure that computers, mobile terminals, telecommunications line devices, electromagnetic recording media, etc. are not brought into Information Management Areas that have system handling information assets higher than confidentiality 3 installed without permission.

(3) Carrying In and Out of Devices, Etc.

① The Information System Manager must have employees or outsourced companies confirm the effects of moved devices, etc. on existing information systems.

② The Information System Manager must have employees present at the move of devices, etc. of the Information System Rooms.

4.3. Management of Telecommunications Lines and Telecommunication Line Devices

① The Information Security Officer and Information System Manager must coordinate with the Facility Administration Section and manage telecommunications lines and telecommunications line devices of networks, information facilities, and equipment under jurisdiction appropriately. Furthermore, documents concerning telecommunications lines and telecommunications line devices must be properly stored.

② The Information Security Officer must limit network connections to the outside to the minimum necessary and decrease the connection points as much as possible.

③ The Information Security Officer and Information System Manager must choose the appropriate lines after reviewing the necessary security standards when telecommunications lines are connected to information systems handling information assets higher than confidentiality 2 under jurisdiction. Furthermore, encryption must be conducted based on appended form 2 “Encryption Guidelines” of the information to be transmitted as needed.

④ The Information Security Officer and Information System Manager must implement adequate security countermeasures for lines used in networks, information facilities, and equipment (including LAN ports) under jurisdiction. so as not to cause destruction, wiretapping, alteration, deletion, etc. of information on transmission as needed.

⑤ The Information Security Officer must choose lines that allow the continuous operation of telecommunications lines connected by the information systems that handle information higher than availability 2. Furthermore, measures must be taken such as giving the lines a redundant configuration as needed.

4.4. Management of PC, Etc. of Employees, Etc.

(1) Management of PCs, Etc. by the Information System Manager

① The Information System Manager must take physical measures including the management of locks, etc. of offices, etc. (including fixing PCs, etc. by a security wire, etc.) as needed as a protection against theft. In regard to electromagnetic recording media where information assets higher than confidentiality 2 has been recorded once, recorded information must be promptly deleted or media must be physically destroyed, etc. when it is no longer necessary to save the information.

② The Information System Manager must set to ensure security by inputting a password or biometrics when logging in to information systems.

③ The Information System Manager must combine passwords (BIOS/UEFI password, storage password, etc.) at startup of terminals as needed.

④ The Information System Manager shall put two-factor authentication to use in user authentication as needed in view of the importance of the information handled.

⑤ The Information System Manager must validate the encryption function (including the encryption function of a file systems) of PCs, mobile terminals, etc. with built-in electromagnetic recording media and use this. If a security chip is installed in a terminal, consideration must be given so as to effectively utilize its function. Furthermore, when using an electromagnetic recording medium that connects externally including a USB memory, etc., data of confidentiality 2 in principle shall be encrypted and if recording data higher than confidentiality 3, the entire medium, which is encrypted, must be used.

⑥ The Information System Manager shall encrypt electromagnetic recording media in principle in the use of laptop computers and tablet PCs which are assets of NINS for business outside of NINS; provided however, that after FY 2021, use without encryption is prohibited.

⑦ When encrypting as provided in ⑤ and ⑥, appended form 2 “Encryption Guidelines” shall be observed in principle.

(2) Management of PC, Etc. by Employees, Etc.

Employees, etc. may become a self-manager (hereinafter referred to as “Self-Manager”) in regard to mobile terminals including laptop PCs and smart devices and electromagnetic recording media which are assets of NINS used by oneself with the permission of the Information System Manager. In this case, employees are under obligation and liable for such devices as Information System Manager. Furthermore, in regard to management of such devices, 4.4.(1) “Management of PCs, Etc. by Information System Manager” is applied mutatis mutandis and if disposing them and transferring assets, 4.1.(7) is applied mutatis mutandis.

5. Personnel Security

5.1. Matters to be Observed by Employees, Etc.

(1) Matters to be Observed by Employees, Etc.

① Observance of Information Security Policy, etc.

Employees, etc. must observe the Information Security Policy, etc. Furthermore, if there is anything unclear about the information security or observance is a difficult point, etc., promptly consult with the Information Security Manager and ask for instructions.

② Prohibition of Use for Purpose Other Than Duty

Employees, etc. shall not carry out information assets, access information systems, transfer information systems that do not fall under Item (i) and Item (iii), Paragraph 1, Article 4 of Basic Rules, use e-mail addresses, and use the Internet for the purpose other than duty without the permission of the Institute CISO based on Item (ii), Article 15 of the Employment Regulations.

③ Carrying Out Mobile Terminals, Electromagnetic Recording Media, Etc. and Restrictions on Information Processing Work Outside

Employees, etc. shall observe the Information Security Policy and exercise due care to the transport of information assets listed in the Handling Restrictions and 3.(2)⑧ of the Countermeasures and Standards by classification in Appended Form 1 of Basic Rules in particular if carrying out mobile terminals, electromagnetic recording media, etc. which are assets of NINS.

④ Use of PCs, Mobile terminals, Electromagnetic Recording Media, Etc. (hereinafter referred to as “Terminals, Etc. Other Than Those Provided”) Other Than Information System which are Assets of NINS (including personal effects) for Business

(i) Employees, etc. shall not use Terminals, Etc. Other Than Those Provided in duties that deals with information assets higher than confidentiality 2 in principle; provided however, that they may be used with the permission of the Information Security Manager in a necessary case in the course of duties. In this case, employees, etc. are deemed to have agreed that the Information Security Policy would be applied to terminals, etc. other than those provided.

(ii) Employees, etc. shall not process information and store information assets higher than confidentiality 3 by PCs, mobile terminals, electromagnetic recording media, etc. for personal use unless permitted by the Institute CISO as provided in the handling restrictions of Appended Form 1 “Classification of Information Assets by Confidentiality” of the Basic Rules.

(iii) Employees, etc. shall observe the procedures provided by the Information System Manager who has jurisdiction of the connected networks and information systems and follow instructions of the Information System Manager if Terminals, Etc. Other Than Those Provided are connected to networks and information systems. Furthermore, there must be cooperation with the Information System Manager in regard to the careful examination of Terminals, Etc. Other

Than Those Provided if the Terminals, Etc. Other Than Those Provided are suspected to be the cause when an information security incident has arisen.

⑤ Prohibition of Changing Security Settings in PCs and Mobile Terminals

Employees, etc. must not intentionally change the settings of the security functions in the software of PCs and mobile terminals without permission of the Information Security Manager except when changing the settings to obviously strengthen security.

⑥ Management of Desk-Top Terminals, Etc.

Employees, etc. must take appropriate measures including locking of PCs and mobile terminals when leaving one's seat and storage in a place where electromagnetic recording media, documents, etc. are not easily accessed to prevent use by a third party and information from being accessed without permission of the Information Security Manager in regard to PCs, mobile terminals, electromagnetic recording media, documents on which information is printed, etc.

⑦ Matters to be Observed on the Occasion of Retirement, Etc.

Employees, etc. must return utilized information assets of NINS when leaving business operations due to transfer, retirement, etc. Furthermore, information higher than confidentiality 2 which may come to knowledge in the course of business must not be divulged thereafter.

⑧ Use of Networks Other Than the Network Provided by NINS

Employees, etc. must institute security information countermeasures (such as restricting services, ports, etc. available to the information system from outside) appropriate for the information system (Terminals, Etc. Other Than Those Provided) to be connected when using networks other than the network provided by NINS to operations, as well as use them with attention to the encryption status of the communication, while taking into consideration the possible surreptitious intrusion of communication.

(2) Handling of Part-Time Employees and Temporary Employees

① Observance of Information Security Policy, etc.

The Information Security Manager must make part-time employees and temporary employees understand, implement, and observe contents of the Information Security Policy, etc. for part-time employees and temporary employees to be complied by when appointed.

② Consent for the Observance of the Information Security Policy, etc.

The Information Security Manager shall request the signature to the consent form to the effect that the Information Security Policy, etc. shall be observed upon the appointment of part-time employees and temporary employees.

(3) Posting of the Information Security Policy, etc.

The CISO and Institute CISO must always post the Information Security Policy, etc. to enable Employees, etc. to access them.

(4) Explanation to the Outsourced Companies

The Information Security Manager and Information System Manager must explain the observance of the contents to be complied by outsourced companies and classified materials of the Information Security Policy, etc. including entrepreneurs who received a subcontract from outsourced companies in cases where orders for the development, maintenance, etc. of networks and information systems under jurisdiction are to be placed.

5.2. Education, Training, and Drills

(1) Education, Training, and Drills Pertaining to Information Security

① The CISO and Institute CISO must implement education, training, and drills pertaining to Information Security periodically.

② The CISO and Institute CISO must implement education, training, and drills with due consideration to the CSIRT and Important Server Administrator.

(2) Formulation and Implementation of Education and Training Programs

① The CISO must formulate education and training programs pertaining to information security for executive officers, employees, etc. to be implemented as NINS as a whole and report to the Information Security Committee.

② The CISO must formulate education and training programs pertaining to information security for executive officers, employees, etc. to be implemented as each institute and report to the Information Security Committee.

③ Executive officers, employees, etc. must make maximum effort to participate in education and training programs designated by the CISO and Institute CISO.

④ The CISO and Institute CISO shall take measures such as prohibiting from use the whole or part of information assets to persons who didn’t participate in education and training as needed.

⑤ The Institute CISO must implement training pertaining to Information Security targeted to new Employees, etc.

⑥ The education and training programs designated by the CISO and Institute CISO must show consideration to the General Information Security Officer, Information Security Officer, CSIRT, Information Security Manager, Information System Manager, Person in Charge of Information System, and other Employees, etc., of their roles, comprehension pertaining to information security, etc.

⑦ The CISO and Institute CISO must report the implementation state of education and training programs and participation state of education and training of executive officers, employees, etc. to the Information Security Committee at least annually.

(3) Emergency Response Drills

① The CISO and Institute CISO must regularly implement drills while envisaging emergencies. For the drill program, the system, range, etc. of the drill implementation must be determined and made to be implemented effectively while taking into consideration the network, scale, etc. of each information system.

② The Institute CSIRT must regularly implement the Incident Response Drill and endeavor to improve response capacity.

(4) Participation in Education, Training, and Drills

All executive officers, employees, etc. must participate in prescribed education, training, and drills.

5.3. Report of Information Security Incidents

For the reporting route of information security incidents, a deputy in the absence of the applicable person due to an official trip, etc., or when the deputy has not been appointed, the immediate superior in the shall be in charge of the response.

(1) Report of Information Security Incidents of Employees, Etc. (Incident Report Desk of Each Institute)

In this paragraph, security incidents arising from outside including the leakage of information to the outside and unauthorized access from outside shall be handled as important.

① Employees, etc. must report immediately to the Incident Report Desk of Each Institute in the case an information security incident is confirmed or in the case a potential incident is found.

② The Incident Report Desk of Each Institute that received the report must report to the Institute CSIRT and Information Security Officer immediately.

③ The Institute CSIRT who received the report from the Incident Report Desk of Each Institute must cooperate with the Information System Manager and respond immediately.

④ The Information Security Officer who received the report from the Incident Report Desk of Each Institute must report to the Institute CISO immediately.

⑤ The Institute CISO who received the report from the Information Security Officer must determine the importance of the incident and he/she must instruct the response to the Information Security Officer and Institute CSIRT immediately for those determined to be important (hereinafter referred to as “important items”) and promptly for those determined to be not important (hereinafter referred to as “unimportant items”).

⑥ The Information Security Officer who received instructions from the Institute CISO must instruct the necessary response to the Information Security Manager immediately for important items (promptly for unimportant items).

⑦ The Information Security Manager who received instructions from the Information Security Officer must respond immediately for important items (promptly for unimportant items).

⑧ The Institute CSIRT must confirm the status immediately and make a status report to the Institute

CISO and Information Security Officer immediately for important items (promptly for unimportant items).

⑨ The Information Security Manager must report the status on the leakage of information arising from the incident to the Information Security Officer immediately for important items (promptly for unimportant items).

⑩ The Information Security Officer who received the report from the Information Security Manager shall report the status to the Institute CISO immediately for important items and promptly for unimportant items.

⑪ The Institute CISO must receive the status report of the Institute CSIRT and Information Security Officer, re-evaluate the importance of the incident, and report to the President, CISO, and General Information Security Officer immediately for important items (promptly for unimportant items).

(2) Report of External Information Security Incidents (External Reporting Desk)

① The External Reporting Desk must report to the Institute CSIRT and Information Security Officer immediately where external notice has been received in regard to the information security incident on networks, information systems, and other information assets managed by NINS.

② The Institute CSIRT who received the report from the External Reporting Desk must cooperate with the Information System Manager and respond immediately.

③ The Information Security Officer who received the report from the External Reporting Desk must report to the Institute CISO immediately.

④ The Institute CISO who received the report from the Information Security Officer must instruct the response to the Information Security Officer and Institute CSIRT immediately.

⑤ The Information Security Officer who received instructions from the Institute CISO must instruct the necessary response to the Information Security Manager immediately

⑥ The Information Security Manager who received instructions from the Information Security Officer must respond immediately.

⑦ The Institute CSIRT must confirm the status and make a status report to the Institute CISO and Information Security Officer immediately.

⑧ The Information Security Manager must report the status on the leakage of information arising from the incident to the Information Security Officer immediately.

⑨ The Information Security Officer who received the report from the Information Security Manager must report the status to the Institute CISO immediately.

⑩ The Institute CISO must receive the status report of the Institute CSIRT and Information Security Officer, re-evaluate the importance of the incident, and report to the President, CISO, and General Information Security Officer immediately for important items (promptly for unimportant items).

(3) Investigation to Determine the Cause, Record, Prevention of Reoccurrence, etc. of the Information

Security Incident

① The Institute CSIRT must investigate to determine the cause of this information security incident and store a record in collaboration with Information Security Manager, Information System Manager, etc. of the department where the information security incident has been caused. Furthermore, a draft of the investigation to determine the cause and reoccurrence prevention plan must be formulated and submitted to the Institute CISO and Information Security Officer as promptly as possible.

② The Institute CISO must receive the submission of the draft of the investigation to determine the cause and reoccurrence prevention plan from the Institute CSIRT, formulate the investigation to determine the cause and reoccurrence prevention plan of NINS, report to the President, CISO, and General Information Security Officer, and instruct reoccurrence prevention measures to the Information Security Officer.

(4) Report of the CISO

The CISO who received the report from the Institute CISO shall report the information security incident that has been determined as an important item, background thereof, and investigation result to determine the cause and reoccurrence prevention plan to the Board of Directors.

(5) Information Sharing of Information Security Incidents

The CISO and Institute CISO must disclose information on information security incidents that occurred within NINS as detailed as possible to executive officers, employees, etc. using the website, etc. and allow sharing of information.

5.4. Management of IDs, Passwords, Etc.

(1) Handling of IC Cards, Etc.

① Employees, etc. must strictly observe the following matters, as regards self-managed IC cards.

(i) IC cards, etc. used for authentication shall not be shared between Employees, etc. without the permission of the Information System Manager.

(ii) When not needed for work, the IC card, etc. has to be pulled out of the card reader device, slot of terminals including PCs, etc.

(iii) In the event that the IC card, etc. was lost, promptly report to the Information System Manager must be made and follow his/her instruction.

② The Information System Manager must promptly suspend access, etc. using the IC card, etc. upon the report of the loss, etc. of the IC card, etc.

③ In the event of switching IC cards, etc., the Information System Manager must collect and dispose the card before the switch after making it impossible to restore such as crushing it.

(2) Handling of IDs

Employees, etc. must strictly observe the following matters, as regards self-managed IDs.

① IDs which are utilized by a person shall not be used by another person.

② In the event of utilizing a shared ID, it shall not be utilized by other than the users of the shared ID except for cases where the Information System Manager approves.

(3) Handling of Passwords

Employees, etc. must strictly observe the following matters, as regards self-managed passwords (including passphrases to derive secret keys) and secret keys in public key cryptography (hereinafter referred to as "public keys").

① The password must be managed in such a way that another person does not learn of it. Furthermore, in places where the entry process of passwords is highly likely to be leaked to others including public transportation and public space, one must take due care not to leak the password.

② The password shall be a combination of 2 types or more of symbols, English lowercase letters, English uppercase letters, and numbers as a general rule and it shall be of length of 12 characters or more, or of having complexity either equaling or surpassing this. (The length of the password should be as long as possible.) Furthermore, don't create a password which is easy to search or presume including combinations of presumable character string and character strings appearing in dictionaries, etc., letter and number substitutes, etc.

③ In the event of passwords or secret keys are or likely to be leaked, they must be changed immediately and promptly reported to the Information Security Manager; provided however, that for those that are session managed including web applications, due care shall be exercised to carry out changes in password after destroying the session.

④ Employees, etc. handling multiple information systems shall not use the same password and secret keys between systems with regard to information systems higher than confidentiality 3 in principle.

⑤ Tentative passwords in principle must be changed at the time of initial login.

⑥ Passwords and secret keys shall not be shared between Employees, etc. except for cases where the Information System Manager approves.

5.5. Handling of Researchers Involved in Joint Utilization and Joint Research

(1) Scope of Application

Those specified under the items of Paragraph 1, Article 4 of the Basic Rules

(2) Application in these Countermeasures and Standards

Apply by replacing Employees, etc. with researchers involved in joint utilization and joint research; Provided however, except when prescribed by particulars falling under the Employment Regulations of NINS and the Institute CISO.

(3) Consent Form

The Institute CISO shall request researchers involved in joint utilization and joint research their signature to the consent form as needed to the effect that the Information Security Policy, etc. shall be observed.

6. Technical Security

6.1. Computer and Network Management

(1) Installation, Etc. of Document Server

① The Information System Manager must install the capacity of a file server (including the network attached storage; the same applies hereinafter) that Employees, etc. can use as needed such as considering the failure of availability due to overcapacity and inform Employees, etc.

② The Information System Manager must configure the file server in groups corresponding with the assumed usage conditions and set the access authority properly such as making it impossible for Employees, etc. to access and use the folder and file of other groups.

③ The Information System Manager must take measures such as preparing a separate folder with respect to data handled only by particular Employees, etc. including personal information and personnel records and make it impossible for employees, etc. other than the employees in charge to access or use.

(2) Implementation of Backup

The Information System Manager must implement a regular back-up as needed irrespective of the redundancy measures of the server with respect to information recorded in the file server, etc.

(3) Exchange of Information, Etc. on Information Systems with Other Groups

When exchanging information higher than confidentiality 2 including authentication information on information systems and information by a software handling information higher than confidentiality 2 with other groups, the Information System Manager must determine matters related to their handling in advance and obtain the permission of the Institute CISO.

(4) System Management Record and Operational Check

① The Information System Manager must prepare the operation record on operations implemented in the operation of the information system under jurisdiction.

② The Information System Manager must prepare the record on operational contents as needed and manage it appropriately to prevent fraud, falsification, etc. in cases where any work has been taken including system changes in important servers, other information systems and networks under jurisdiction considered to be important.

③ The Information Security Officer, Information System Manager or Person in Charge of Information System, and an outsourced company who is allowed to operate based on a contract must engage in work by two or more persons as needed and check each other’s work in cases of any work to be taken including important or high impact system changes, etc. pertaining to information systems.

(5) Management of Information System Specifications, Etc.

The Information Security Officer and Information System Manager must manage the network configuration diagrams and information system specifications appropriately in order to avoid access, loss, etc. by persons other than those as may be necessary in the course of work irrespective of the recording media.

(6) Collection of the Utilization Log of Information Systems, Etc. (Log Acquisition)

① The Information System Manager must acquire records necessary to ensure information security and retain for the following time period. Provided however, the Institute CISO can determine separately the matters related to (i) to (iii) until March 31, 2020.

(i) For the gateway log which is the external connection (internet), all logs shall be retained for 2 years or more in principle.

(ii) The important server log (including those related) shall be retained for 1 year or more in principle.

(iii) Excluding those set forth in (i) and (ii) above, for PCs and mobile terminals that retain information higher than confidentiality 3, access logs, etc. shall be retained for 1 year or more in principle.

(iv) For other devices, it shall be 30 days or more in principle; provided however, that the Institute CISO may specify separately as needed.

② For logs in the preceding paragraph that exceed 30 days may be retained in external electromagnetic recording media while securing their integrity; provided however, that where another means is specified by the Institute CISO, it shall be based on this.

③ Entries acquired as logs set forth in ① must be appropriate items in preparation for unauthorized access, etc. including when and which information assets were accessed by whom (or terminal); provided however, that where another acquired entry is specified by the Institute CISO, it shall be based on this.

④ The Information System Manager must inspect or analyze hacks, fraudulent manipulation, etc.by third parties with harmful intent as needed such as the setting up regular inspections or analyses of acquired logs.

⑤ The Institute CISO must set forth other necessary matters including the handling of the cases where it becomes impossible to acquire logs as needed and measures must be taken to order the proper management of logs to the Information System Manager.

(7) Error Log

① The Information System Manager must prepare an error log on reports of system failures from Employees, etc., and processing results, problems, etc. of system failures.

② The Information System Manager shall report to the Incident Report Desk of Each Institute immediately if he/she judges that the system failure arises from an information security incident.

(8) Connection Control, Path Control, Etc. of Networks

① The Information Security Officer and Information System Manager must set the firewall, router, and other communications software to eliminate inconsistencies in the setting with respect to filtering and routing of networks in the Institute, etc. under Jurisdiction.

② The Information Security Officer and Information System Manager must appropriately provide access control to the network to prevent unauthorized access with respect to networks in the Institute, etc. under Jurisdiction.

(9) Separation, Etc. of Systems Available to Outsiders

The Information System Manager must take measures such as physically or logically separating other networks and information systems as needed with respect to systems available to visitors (excluding those set forth in 1.1.(1)).

(10) Connection Restrictions, Etc. with External Networks

① The Information System Manager must obtain permission from the Institute CISO and Information Security Officer when connecting networks under jurisdiction with external networks.

② The Information System Manager must investigate the network configuration, equipment configuration, security technology, etc. for external networks seeking connection in detail and confirm that they cause no adverse effect on all information assets of all NINS networks and information systems, etc.

③ The Information Security Officer and Information System Manager must set the server, etc.to the appropriate segment including external networks or DMZ (demilitarized zone, etc.) to defend from intrusion into NINS network (meaning networks falling under Item (i), Article 3 and Article 4 of the Basic Rules; the same applies hereinafter) where publishing a web server, etc. to the web.

④ The Information System Manager must physically and logically cut off the external network promptly in accordance with the judgment of the Information Security Officer if there are problems to the security of the connected external network and threats to information assets are anticipated.

(11) Security Management of Multi-function Printer

① In the cases where combined machines connected to networks are procured, unless otherwise provided for by the Institute CISO, the functions, management methods, etc. held by the combined machines shall be equivalent to the security requirements necessary for the server connected to the network (including the requirement, etc. of data deletion implemented at the end of the operation).

② The Information System Manager must take measures for information security incidents involving combined machines in operation by conducting the appropriate setting, etc. of the functions of combined machines.

③ The Information System Manager must take necessary measures for the handling of information leaks such as not deleting or reusing all information in the electromagnetic recording media of combined machines in accordance with the security requirements stipulated in ① when the operation of combined machines is concluded.

(12) Security Management of Machines with Specific Uses

The Information System Manager must implement measures suited to the characteristics of such devices when some form of threat is assumed using connection configuration, etc. to handled information, use method, and telecommunications lines with respect to machines with specific uses (meaning those with components specific to information systems with specific uses including teleconference system, IP phone system, and network camera system that are connected to telecommunication lines or have electromagnetic recording media built into them, and other IOT devices).

(13) Installation and Anti-Wiretapping Measures of Wireless LAN (Wi-Fi; hereinafter referred to as the “Wireless LAN”)

① In the case where wireless LAN is installed, the Information System Manager must obtain the permission of the Information Security Officer (if provisions have been made separately by the Institute CISO, that person) and apply encryption and the authentic method which make decoding virtually difficult such as encryption based on Appended Form 2 on “Encryption Guidelines” for wireless channels in layer 2 except in the case of installation using the means designated by the Institute CISO).

② The operation of the Wireless LAN must give consideration to conform to the guidelines, etc. provided by the Ministry of Internal Affairs and Communications and take necessary security measures in accordance with the instruction of the Information Security Officer.

(14) Security Management of E-Mails

① The Information System Manager (hereinafter referred to as the “E-mail System Manager”) operating the e-mail server (including the e-mail service; must conduct the setting of the e-mail server, etc. so that e-mail forwarding from outside to outside (relay and processing of e-mails) is to be made impossible by unauthorized users. Furthermore, internal measures must be taken for the purpose of preventing the spread of the breach and beefing up surveillance.

② The E-mail System Manager shall build a system that allows the detection of reception or transmission of unusual e-mail thought to be phishing e-mail, spam e-mail, etc.

③ The E-Mail System Manager must take necessary measures such as e-mail filtering and suspending the operation of the e-mail server where the transmission and reception of unusual e-mail was detected. Furthermore, measures for disposal, quarantine, etc. of such e-mails must be taken and information must be shared within NINS through reporting to the Incident Report Desk of Each

Institute as needed.

④ The E-Mail System Manager must set the upper limit of the transmission and reception capacity of e-mails according to the utilization and application of e-mails (upper limit, total amount, etc. of the number of transmission and reception per day of each person) and take measures to prevent the transmission of bulk e-mail, etc. such as limiting the transmission and reception of e-mails over the maximum limit.

⑤ The E-Mail System Manager must agree with the method of utilization between outsourced companies with respect to e-mail address use such as observing the Information Security Policy in the case where the e-mail address is granted based on contract, etc. to operators, etc. of outsourced companies permanently stationed at NINS for system development, operation, maintenance, etc.

(15) Restriction on Use of E-mails

① Employees, etc. shall not forward e-mails using the automatic forwarding function in principle except in cases specified by the Institute CISO and in which the permission of the Information Security Officer is obtained.

② Employees, etc. shall not send e-mails to destinations not necessary in the course of business.

③ Employees, etc. shall pay particular attention to points that fall under private personal information of the e-mail and take measures such as making e-mail addresses of other destinations unknown as needed to case where e-mails are sent to multiple people.

④ Employees, etc. must report to the Information Security Manager when wrongly sending e-mails higher than confidentiality 2; provided however, that this does not apply when persons who were wrongly sent e-mails of confidentiality 2 are executive officers, employees, joint users and joint researchers, etc.

⑤ Employees, etc. shall not use free mail, network storage service, etc. outside the range of application of the Information Security Policy provided for int Paragraph 1, Article 4 of the Basic Rules (hereinafter referred to as “Services, Etc. Outside the Policy”) in the course of business except with regard to the information of confidentiality 1; provided however, that they may use this in the course of business only if this is information of confidentiality 2 and is permitted to use services, etc. outside the policy by the Institute CISO and the use of this is unavoidable.

(16) Electronic Signature, Hash Value, Time Authentication and Encryption

① Employees, etc. must encrypt, or set up password, etc. in accordance with Appended Form 2 on “Encryption Guidelines” in cases where it is necessary to ensure the confidentiality and integrity of data sent outside in accordance with the handling restrictions specified under classifications of information assets and must transmit taking into consideration of the handling restrictions provided in Appended Table 1 of the Basic Rules “Classification of information assets by integrity”

② Employees, etc. must observe the Schedule 2 “Encryption Guidelines” in principle where encryption is conducted. Furthermore, the key for decoding must be managed appropriately such as storing and transmitting separately with the encrypted information; provided however, that this must be complied if the Institute CISO has separately set the method of management.

③ When an electronic signature is to be used, the information and means to verify the propriety of the electronic signature must be provided safely to the signature verifier; provided however, that this must be complied if the Institute CISO has separately set the means of provision.

(17) Prohibition of Installment, Etc. of Software Without Permission

① Employees, etc. may install software only in cases where designated by the Institute CISO and permission of the Information System Manager who has jurisdiction for such devices (including Self-managers; the same shall apply hereinafter in this paragraph) was obtained based on the operational necessity. Furthermore, the Information System Manager must manage the license of the software as needed when installing.

② Employees, etc. shall not use unauthorized copies of software.

③ Employees, etc. must understand the risk of malware incorporation, conduct investigations, etc. of assessment of such software by a third party, and do preliminary consultations with the Information System Manager who has jurisdiction for such devices as needed with the installation of a software of ambiguous sources in the case where software is installed based on ①.

(18) Restrictions on Change in Device Configuration

Employees, etc. must obtain the permission of the Information System Manager who has jurisdiction for such devices where it is necessary to conduct the alteration, addition, and exchange of devices for PCs and mobile terminals in the course of business.

(19) Prohibition of Network Connection Without Permission

Employees, etc. shall not connect PCs and mobile terminals to the network within NINS without permission of the Information Security Officer and Information System Manager except where the method is specified by the Institute CISO.

(20) Prohibition of Internet Use for Purpose Other Than Duty

Employees, etc. shall not use the internet (including browsing of website and utilizing the services on the internet) for purpose other than duty by using the information assets of NINS except where specified by the Institute CISO.

6.2. Access Control

(1) Access Control

① Access Control, Etc.

The Information System Manager must restrict the use of systems to make it impossible to access for employees, etc. without authority to access for each network or information system under jurisdiction.

② Handling of User ID

The Information System Manager must manage user IDs appropriately.

The Information System Manager shall delete or suspend the user ID of Executive officers and employees, etc. or joint use or collaboration researchers within one month in principal when they lose the status due to the transfer or resignation; provided however, the Institute CISO can set other handling method separately. In this case, the Institute CISO must specify the method appropriately with taking consideration in the case where the user causes the incident and the damage given to NINS and take countermeasures such as obtaining the signature for insuring obedience from the user.

(i) The Information System Manager must specify how to manage information including registration, change, and deletion of users, and handling, etc. of user ID associated with transfer and temporary assignment of employees, etc., or retired persons.

(ii) Employees, etc. must notify the Information System Manager to delete the user registration in cases where the need in the course of business ceases to exist.

(iii) The Information System Manager must inspect regularly and as needed to prevent unused IDs from being left unattended except where specified by the Institute CISO.

③ Management, Etc. of IDs with Privilege

(i) The Information System Manager must make users of IDs with privilege including administrative rights to the minimum necessary.

(ii) The Information System Manager shall not allow outsourced companies to change IDs with privilege and password except ID and password used by outsourced companies in networks and information systems with entrusted management based on contracts.

(iii) The Information System Manager must disable default IDs with privilege (examples: Administrator, root, etc.) in principle except where specified by the Institute CISO. In case IDs may not disabled, the password based on 5.4.(3) must be changed to other than the default password.

(2) Restrictions on Access, Etc. from Outside by Employees, Etc.

① When accessing internal networks or information systems from outside, employees, etc. must obtain permission of the Information Security Officer (with respect to matters concerning the Information System Manager' LAN which is built independently, such Information System Manager. The same shall apply hereinafter in this section.) except where the method is specified by the Institute CISO.

② The Information Security Officer must restrict access to internal networks and information systems from outside to the minimum necessary of those who has reasonable grounds necessary for access except where specified by the Institute CISO.

③ The Information Security Officer must secure the function to confirm the identification of the system user if access from outside is approved.

④ The Information Security Officer must take measures of encryption, etc. based on Appended Form 2 on “Encryption Guidelines” for protecting from wiretapping in the middle of communication if access from outside is approved.

⑤ The Information Security Officer and Information System Manager must take necessary measures for maintaining security when leasing mobile terminals to employees, etc.to access from outside.

⑥ Employees, etc. must confirm that the mobile terminal brought into or taken back from outside is not infected with malware and virus before connecting to the NINS network by antivirus software and also confirm the status of the application of the security patch.

⑦ The Information Security Officer must prohibit the connection of a public communication channel (mobile communication network, public wireless LAN, internet connection service, etc.), tunnel communication, etc. to the NINS network in principle; provided however, that in the case where connection is unavoidably permitted, necessary measures must be taken for maintaining information security including encryption of the communicated content in addition to authentication using the ID and password, authentication information including biometric information of the user, and media (IC card, etc.) to record this.

⑧ Employees, etc. shall not connect to the NINS network from outside NINS unless it is a connection pursuant to the provisions of ①.

(3) Setting of the Automatic Identification

The Information System Manager must set the system to automatically identify the propriety of connection between the terminal and network by equipment dependent information, etc. on devices used in networks in principle.

(4) Display, Etc. at Login

The Information System Manager must set the system insofar as possible so as to enable Employees, etc. with legitimate access privileges to confirm that their own accounts are not used improperly by messages at login, restrictions on the number of login attempts, setting of access time out, displays of the login time and logout time, etc.

(5) Management of Password Information

① The Information System Manager must tightly control the information on passwords of employees, etc. To protect from unauthorized use of the password file, an enhanced function of the password security setting in the operating system, etc., must be effectively utilized.

② In cases of issuing passwords for Employees, etc. in principle, except where specified by the Institute CISO, the Information System Manager must issue a temporary password and have the temporary password to be changed immediately after login.

(6) Restrictions of Connection Time by Privilege

The Information System Manager must restrict the connection time to the minimum necessary to networks and information systems by privilege.

6.3. System Development, Installation, Maintenance, Etc.

(1) Procurement of Information Systems

① The Information System Manager must clearly indicate the technical security functions necessary in procurement specifications in procuring information system development, installation, maintenance, etc.

② In procuring devices and software, the Information System Manager must investigate the security functions of the products and confirm that there is no information security problem.

(2) Information System Development

① Specification of the Officer and Operator in System Development

The Information System Manager must specify the officer and operator in system development. Furthermore, the bylaws for system development must be formulated as needed and shared between relevant persons.

② Management of ID of the Officer and Operator in System Development

(i) The Information System Manager must manage the ID used by the officer and operator in system development and delete the ID for development following the completion of development.

(ii) The Information System Manager must set the access authority of the officer and operator in system development.

③ Management of Hardware and Software Used for System Development

(i) The Information System Manager must specify the hardware and software used by the officer and operator in system development.

(ii) In cases of installing software other than software recognized to be used, the Information System Manager must remove such software from the system with uninstallation or roll back of the operating system, etc.

(3) Installation of Information Systems

① Separation of the Development Environment and Operational Environment and Clarification of the Migration Procedures

(i) The Information System Manager must separate the system operational environment from system development and maintenance and test environment in principle.

(ii) The Information System Manager must clarify the procedures at the time of formulation of the plan for system development and maintenance in the migration to the system operational environment from system development maintenance and test environment.

(iii) The Information System Manager must ensure the storage of information assets recorded in information systems at the time of migration and endeavor to minimize influence including the suspension of information systems upon migration.

(iv) The Information System Manager must implement installation after confirming that the availability of system and service to be installed is secured.

② Test

(i) The Information System Manager must conduct a sufficient test including conducting an independent hosting test for the structure developed and the structure to be developed prior to connection to information systems already in operation.

(ii) The Information System Manager must confirm the operation with a pseudo-environment beforehand in principle when conducting the test.

(iii) The Information System Manager must not use personal information and highly confidential information in test data.

(4) Maintenance and Storage of Materials, Etc. Related to System Development and Maintenance

① The Information System Manager must properly maintain and store materials relating to system development and maintenance and system-related documentation.

② The Information System Manager must store the test result throughout a period of time.

③ The Information System Manager must store the source code for information systems in a suitable manner.

(5) Ensuring Accuracy of Input-Output Data of Information Systems

① The Information System Manager must design an information system that incorporates coverage and validation check function and the function to remove the input of fraudulent character strings, etc. in regard to data entered into information systems.

② In the event that information could be altered or leaked intentionally or by negligence, the Information System Manager must design an information system that incorporates a check function to detect this.

③ The Information System Manager must design the information system for the processing of information to be accurately reflected and generated in regard to data generated from information systems.

(6) Management of Change in Information Systems

The Information System Manager must prepare the change log of program specification, etc. as needed if information systems are changed.

(7) Development and Maintenance Software Update

The Information System Manager must check the compatibility with other information systems if development and maintenance software, etc. is updated or a patch is applied.

(8) System Update or Validation, Etc. When Integrating

The Information System Manager must build a risk management structure with system update and integration, clarification of the transfer basis, and conduct the validation of the operation system after update and integration.

6.4. Countermeasures Against Unauthorized Programs

(1) Measures to be Taken by the Information Security Officer

The Information Security Officer must take the following measures as countermeasures against unauthorized programs in the backbone and common networks.

① For files received from external networks, unauthorized programs including computer virus must be checked in the gateway into the Internet and intrusion into the system of unauthorized programs must be prevented.

② For files sent to external networks, unauthorized programs including computer virus must be checked in the gateway into the Internet and the spread of unauthorized programs outside must be prevented.

③ Information about C&C server used for attacks must be collected and exit countermeasures including imposing a limitation on external communications (including the connection refusal to C&C server) using FW, IPS, Proxy, and GW, etc. must be undertaken.

④ Unauthorized program information including computer virus must be collected and employees, etc. must be alerted as needed.

⑤ A countermeasure software for computer virus and other unauthorized programs must be installed in servers, PCs, and other terminals of jurisdiction. Furthermore, the pattern file of countermeasure software for unauthorized programs must be kept up-to-date at all times.

⑥ For the software used for the duty, those no longer supported by the developer including patches, version upgrades, etc. must not be used except in the case of using them in a standalone or completely isolated network; provided however, that except in the case of undertaking measures by the order of Information Security Officer or Information System Manager and obtaining approval. In this case that is determined to be necessary, the Information Security Officer or Information System Manager may request the decision of the Institute CISO.

⑦ With regard to information system accepted with the above, the Information Security Officer must gain an understanding of this and confirm the operation status regularly.

(2) Measures to be Taken by the Information System Manager

The Information System Manager must take the following measures as countermeasures against unauthorized programs.

① The Information System Manager must install the countermeasure software for unauthorized programs in servers, PCs, and other terminals of jurisdiction.

② The countermeasure software for unauthorized programs shall not reach the end of the support lifecycle and the pattern file must be kept up-to-date at all times.

③ The Information System Manager must take necessary measures including preventing employees, etc. from the use of electromagnetic recording media other than media that is managed by oneself to prevent computer virus and other infections in the case where electromagnetic recording media were used in systems not connected to the Internet. Furthermore, unless in the case the possibility of infection and intrusion of unauthorized programs is extremely low, countermeasure software for unauthorized programs must be installed and the update of the software and pattern file must be regularly implemented.

(3) Matters to be Observed by Employees, Etc.

Employees, etc. must observe the following matters related to countermeasures against unauthorized programs.

① In the case where the countermeasure software for unauthorized programs was installed into PCs and mobile terminals, unless in the case where the permission of the Information System Manager has been obtained, the setting of the software shall not be changed.

② If importing data or software from outside, it must be checked with a countermeasure software for unauthorized programs in principle; provided however, that in the case where this is difficult, excluding the case where it can be explained reasonably that problems due to unauthorized programs will not occur. Furthermore, if importing software, the rules of 6.1.(17) must be observed.

③ If a suspicious e-mail has been received, report to the Incident Report Desk of Each Institute immediately and comply with instructions.

④ For terminals, a full check must be periodically performed with a countermeasure software for unauthorized programs.

⑤ If an email with an attached file is sent or received, a check must be performed with a countermeasure software for unauthorized programs. Furthermore, if it's an encrypted file, due consideration shall be given to unchecked points if not encoded and they must be checked based on ② above.

⑥ Information on unauthorized programs provided by the Information Security Officer, Institute CSIRT, etc. must be checked at all times.

⑦ If infected or suspected to be infected with an unauthorized program including a computer virus, a report must be made to the Incident Report Desk of Each Institute promptly and the retention of the condition and following measures must be taken as needed in accordance with instructions.

(i) In case of a device connected to the wired LAN

The LAN cable must be removed immediately.

(ii) In the case of a device transmitting by a wireless LAN

The use must be stopped immediately, and the setting must be made to cease transmission.

(4) Support System by Experts

The Information Security Officer must keep the lines of support of outside experts open to prepare for inadequacies in the implemented countermeasures for unauthorized programs.

6.5. Countermeasures Against Unauthorized Access

(1) Measures to be Taken by the Information Security Officer and Information System Manager

The Information Security Officer and Information System Manager must take the following measures as needed as countermeasures against unauthorized access.

① For a port not used in information systems, this must be closed or rendered unavailable in principle.

② For unnecessary service, the function must be deleted or suspended.

③ For web servers, to prevent falsification of web pages by unauthorized access, proper measures must be taken including the setting for unauthorized access detection tool and to detect the replacement of data and report to the Information Security Officer and Information System Manager.

④ For important system files, etc., an inspection for the replacement of relevant files must be conducted regularly.

⑤ The Information Security Officer must establish a system and communications that coordinate with the Incident Report Desk of Each Institute and can implement the monitoring, notification, external reporting desk, proper response, etc.

(2) Warning of Attack

The Institute CISO and Information Security Officer must take necessary measures, including the suspension of the system, when it has become clear that the server, etc. will be attacked. In addition, they must strive to collect information in close contact with relevant organizations.

(3) Retention of Records

If an attack has a possibility of crime such as a violation of the Unauthorized Computer Access Control Act (including those by social engineering) such as a server, etc. receiving an attack, the Institute CISO and Information Security Officer must preserve records of the attack as needed and endeavor to cooperate closely with the police and relevant organizations.

(4) Attack from the Inside

The Information System Manager who manages a backbone network must monitor attacks on LAN servers, etc. from information system terminals connected to the LAN and attacks on external sites.

(5) Unauthorized Access by the Employees, Etc.

The Information Security Officer and Information System Manager must notify the Information Security Manager of the office, division, etc. to which the employee belongs and request appropriate measures when they detect unauthorized access by the employee, etc.

(6) Denial of Service Attack

The Information Security Officer and Information System Manager must, as far as possible, take measures to ensure the availability of information systems in order to prevent the loss of access to services by users due to denial of service attacks by third parties against information systems that can be accessed from outside.

(7) Targeted Attack

In order to prevent intrusion into information systems by targeted attacks, Information Security Officers and Information System Managers must take personnel measures and entry measures, such as education and alerting of executive officers, employees, etc. auto play invalidation by setting policies for the OS, etc. Furthermore, internal countermeasures such as checking the communication must be taken for early detection and handling of intruding attacks.

6.6. Collecting Security Information

(1) Collecting and Sharing Vulnerability Information, Updating Software, Etc.

Information Security Officers and Information System Managers must collect information on vulnerabilities in computer software, etc., and share it among relevant parties as needed. In addition, countermeasures such as software update, etc. must be implemented according to the urgency of the vulnerability.

(2) Collection and Dissemination of Security Information on Unauthorized Programs, Etc.

The Information Security Officer must collect security information such as unauthorized programs and shall inform employees, etc. of the response methods as needed.

(3) Collection and Sharing of Information on Information Security

The Information Security Officer and Information System Manager must collect information on information security and share it among relevant persons as needed. Furthermore, when a new threat to information assets under the jurisdiction is recognized by the change of social environment, technical environment, etc. on information security, the countermeasures to preemptively prevent infringement of security must be taken promptly.

(4) Collection and Sharing of Information by the Institute CSIRT

The Institute CSIRT shall collect and analyze computer software vulnerabilities, security information such as unauthorized programs, and a wide range of information related to information security and shall alert and provide information to organizations under jurisdiction as needed. Furthermore, information should be shared among Institute CSIRTs as needed.

7. Operations

7.1. Monitoring Information Systems

① In order to detect security-related incidents, the Information Security Officers and Information System Managers must cooperate and continuously monitor information systems with confidentiality level 3 or higher.

② The Information Security Officer and Information System Manager must take measures to enable accurate time setting of servers that jointly acquire logs, etc. and time synchronization between servers.

③ The Information Security Manager and Information System Manager must continuously monitor the system which jointly gets a permanent connection with the external WAN.

7.2. Monitoring the Network

① Executive officers, employees, etc. shall not intercept and monitor network communication data except for Network Supervisors provided for in Paragraph 1, Article 23 of the Basic Rules (hereinafter referred to as "Network Supervisor”); provided however, that the network supervisor may make the subordinate person in charge of the information system intercept and monitor the communication data of the network based on his authority.

② The cases specified in the Countermeasures and Standards provided for in Paragraph 2, Article 23 of the Basic Rules shall be those the CISO or Institute CISO permits to prevent serious security breaches inside or outside NINS. The extent to which communication can be made shall be limited to the minimum necessary and the Network Supervisor must prohibit information recipients from transmitting to others and must also record contents and destination of the transmission. The person in charge who was conveyed the information must not transmitting this information to others. In this case, The Network Supervisors must record the person in charge and the contents of conveyed the information.

③ Notwithstanding the foregoing provisions, Network Supervisors may, at their own discretion, respond in cases of urgency to prevent serious security breaches against or outside NINS; provided however, that the approval of the CISO or Institute CISO shall be obtained subsequently.

7.3. Check Compliance with the Information Security Policy

(1) Confirmation of and Dealing with the Status of Compliance

① The Information Security Officer and Information Security Manager must confirm the status of compliance with the Information Security Policy and report any problems to the Institute CISO promptly.

② The Institute CISO shall respond appropriately and promptly to the problems that have arisen.

③ The Information System Manager shall periodically check the status of compliance with the Information Security Policy in the system settings, etc. of networks and servers, etc., and shall take appropriate and prompt action if any problems occur.

(2) Survey on the Usage of PCs, Mobile Terminals, Electromagnetic Recording Media, etc.

The Information Security Officer (including those designated by the Information Security Officer as persons who perform inspections)　and Institute CSIRT may investigate the usage conditions of the logs of personal computers, mobile terminals, and electromagnetic recording media, etc. and records of transmission and reception of electronic mails, etc., used by employees, etc., for the purpose of investigating unauthorized access, unauthorized programs, etc.

(3) Obligation of Employees, Etc. to Report and Cooperate

① Employees, etc. must immediately report to the Incident Report Desk of Each Institute in the case when any violation of the Information Security Policy has been discovered.

② If the Information Security Officer determines that a violation may have a significant immediate impact on information security, appropriate action must be taken in accordance with the emergency response plan.

③ Employees, etc. have an obligation to immediately cooperate with and respond to investigations conducted based on the Information Security Policy by the Information Security Audit Officer, Information Security Audit Implementer, Information Security Officer, Institute CSIRT, Information Security Manager, and Information System Manager.

④ Employees, etc. are obliged to cooperate with the Information Security Officer and Institution CSIRT when requested to cooperate with them on technical expertise, etc., possessed by them.

⑤ For audits conducted by the Information Security Auditing Office (includes vulnerability testing performed by outsourcing) Executive officers, employees, etc. shall be obliged to cooperate in this regard.

7.4. Measures, Etc. in Case of Emergency

(1) Formulation of an Emergency Response Plan

The Institute CISO shall establish an emergency response plan in order to promptly and appropriately implement measures such as communication, preservation of evidence, prevention of damage expansion, recovery, and prevention of recurrence in the event of or likely to occur the security breaches against information assets by an information security incident, violation of the Information Security Policy, etc. and shall appropriately deal with an information security violation according to the plan.

(2) Items to be Included in the Emergency Response Plan

The emergency response plan must provide for the following contents:

① Contact Persons

② Matters to Be Reported Concerning Cases That Have Occurred

③ Responsive Measures to Cases That Have Occurred

④ Formulation of Measures to Prevent Recurrence

(3) Ensuring Consistency with Business Continuity Plans

The CISO must ensure the consistency of the Information Security Policy with the established business continuity plan of the National Institutes of Natural Sciences in preparation for natural disasters, large-scale and wide-ranging diseases, etc.

(4) Review of the Emergency Response Plan

The Institute CISO must review the emergency response plan according to the change of the situation surrounding information security and the change of the organization system, etc. as needed.

7.5. Exceptional Measures

(1) Permission for Exceptional Measures

The Information Security Manager and Information System Manager may, with the permission of the Institution CISO, take exceptional measures in cases where it is difficult to comply with information security related rules and there are reasonable grounds for adopting a method different from the compliance rules or for not implementing the compliance rules in order to continue the proper execution of the business such as the operation of NINS.

(2) Emergency Exceptional Measures

The Information Security Manager and Information System Manager must report to the Institute CISO promptly after the implementation of the exceptional measures in cases where the implementation of the exceptional measures is unavoidable, such as in cases where the performance of NINS business requires urgency.

(3) Management of Applications for Exceptional Measures

The Institute CISO must appropriately store applications for exceptional measures and examination results and periodically check the status of applications.

7.6. Compliance with Laws and Regulations

Employees, etc. must comply with relevant laws and regulations as well as various rules established by NINS in order to protect information assets used in the performance of their duties and observe them.

Particular attention should be paid to the following laws and regulations and rules established by NINS.

① Copyright Act (Act No. 48 of 1970)

② Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999)

③ Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, Etc.

(Act No. 59 of 2003)

④ Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures (Act No. 27 of 2013)

⑤ Computer Crime Prevention Act of the Penal Code (Act No. 45 of 1907)

⑥ Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Act No. 137 of 2001)

⑦ Act on Regulation of Transmission of Specified Electronic Mail (Act No. 26 of 2002)

⑧ National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Personal Information Protection Rules (NINS Rules No. 54 of 2005).

⑨ National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Rules for the Handling of Specific Personal Information (NINS Rules No. 106 of 2015).

In addition, the following points must be observed when collecting and managing personal information electronically.

- When collecting personal information, the purpose of use must be clearly stated based on “The Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc.” and “National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Personal Information Protection Rules”
- The purpose of use must be described so that the handling of personal information can be understood, and the consent of the person must be obtained.
- Personal information collected by means other than electronic means can be digitized only to the extent that the purpose of use is achieved.

7.7. Disciplinary Action, Etc.

(1) Disciplinary Action, Etc.

① Employees, etc. who violate the Information Security Policy and their supervisors shall be subject to disciplinary action according to the Employment Regulations of NINS, depending on the seriousness and the circumstances, etc. of the incident that has occurred.

② If Joint Use or Joint Collaboration Researchers etc. has violated Information Security Policy and then has caused damage to NINS, intentionally or by gross negligence, the employee etc. may be forced to compensate for the amount of damage to NINS based on the labor contract. In addition, the supervisor of the Joint Use or Joint Collaboration Researcher is subject to disciplinary action based on NINS Employee Regulation, depending on severities, incident circumstances and other factors.

③ Employees, etc. who committed any act of interference, harassment, and compulsion to the performance of duties of the Information Security Audit Manager, Information Security Audit

Implementer, or CSIRT, taking advantage of his/her position, is subject to a disciplinary action depending on his/her action's severity according to the Employment Regulations of NINS; provided however, that the Information Security Audit Manager, Information Security Audit Implementer, or CSIRT, shall take reasonable accountability and therefore, if they consider as urgent, they may give detailed account to those concerned after the disciplinary action.

④ Joint users, joint researchers, etc. who committed any act of interference, harassment, and compulsion to the performance of duties of the Institute CISO and Information Security Officer, based on one's position while in office and social position, must stop using information assets of the National Institutes of Natural Sciences and delete or return retained information of the National Institutes of Natural Sciences if instructions from the CISO or Institute CISO were received; provided however, that if dissatisfied with those measures, one may file a petition to the CISO by clearly showing a basis for the invalidation of those measures.

(2) Response to Violation of Information Security Policy

If it is founded that Employee etc. has violated Information Security Policy, following measures should be taken immediately.

① If Information Security Officer confirms the Employee's violation, Information security Officer shall report the Information Security Manager of the office or section etc. to which the Employee is belong to and shall request the appropriate measures.

② If Information System Manager etc. confirms the Employee's violation, the person who confirmed the violation, shall report the Information Security Officer and the Information System Manager of section etc.to which the Employee is belong to and shall request the appropriate measures.

③ If nothing is improved with even advice of the Information Security Manger, Information Security Officer may suspend or deprive the right to use the Employee's network or information system. After that, Information Security Officer shall report promptly the suspension or deprivation of the Employee's right to Institute CISO and the Information Security Manager of the section etc. to which the Employee is belong to.

8. Use of External Service

8.1. Outsourcing

(1) Outsourcing Selection Criteria

① Information Security Manager shall make sure that the information security measures are guaranteed in accordance with the contents of entrusted work in corporation with information system managers at a selection of outsourcer as needed

② Information Security Manager shall select an outsourcer in reference with the status of obtaining the international standards for Information Security Management System and implementing of Information Security Audit.

③ When using the cloud services, Information Security Manager shall use the services in which security must be secured in accordance with the confidentiality in corporation with Information Security Managers as needed.

④ In the case where the institute intends to outsource some of its business with the approval of Institute CISO, based on the Handling Restrictions 4 and 3, from Appended Table 1, Basic Rules, “Classification of Information Assets by Confidentiality” the institute must gain permission from Institute CISO and submit documents which certifies the outsourcing security level is the same as those of the institute or higher. Furthermore, in the case where the outsource includes personal information or specific personal information, the outsource shall be complied with Personal Information Protection Rules of NINS (Rules No.54 April 1, 2005) and Specific Personal Information Handling Rules of NINS (Rules No.106, 2015).

(2) Items of the Contract

In the case where the institute outsources an information systems management and maintenance etc., it must conclude contract which stipulates following information security conditions as needed.

- Compliance with information security policies and other rules.
- To specify outsourcer’s supervisors, contents of outsourcing, persons in charge and working areas
- Guarantee for the quality of outsource services
- Types and ranges of the information which outsourcer is allowed to access, the way of access
- Provision of Education to employees of outsourcer
- Prohibition on using the provided information beyond the scope of the purpose and supplying provided information to un-contractor
- Confidentiality of information in the course of their works
- Compliance with limitation rules for re-outsourcing
- Return and abolishment, etc. of information assets at the completion of outsourced operation
- Obligation for Regular and emergency report of consignment
- Auditing and inspection by NINS
- Announcement of an information security incident by NINS
- Provision for Breach of Information Security Policy (compensation etc.)

(3) Confirmation and measures etc.

Information Security Manager shall make sure regularly that necessary security measures at outsourcing companies are secured, in the case of confidentiality 2 information assets, as needed, in the case of confidentiality 3 or higher, surely and periodically, and take measures if required based on the above contents of the contracts along with reporting findings to Information Security Officer. In addition, Information Security Officer shall report the findings Institute CISO as needed depending on an importance of report.

8.2. External Service Use Under the Rules

(1) Establishment of External Service Use Under the Rules

① "External service use under the rules" means information processing service where the rules are prepared and there is limited room to be chosen by users in information security matters; provided however, that those required to be managed as in the case of having in place an information system on physical servers including having in place an information system on virtual machines provided through Infrastructure as a Service (IaaS), etc. are handled as information system (server, software, etc.) specified in Item (ii), Article 3 of the Basic Rules even if the same is caused by the rules.

② The Information Security Officer shall make external service provisions which include following conditions if the external services are permitted under the Rules for information falling under Confidentiality 2.

In addition, when using these services, Information security Officer shall stipulate provisions that confidentiality 3 or higher information should not be used; provided however, except for "the cases where the Institute CISO permits" in the handling restrictions with the information of "confidentiality 3" in Appended Form 2 of Basic Rules on Information Security Countermeasures.

(i) Scope of use based on the Rules

(ii) External services to be used in the course of their works

(iii) Using and operating procedures

(iv) Designation and clear indication of the Information System Manager related to said service (limited to those cases in which it is necessary)

(2) Countermeasures When Using External Services Under the Rules

In the case where Executive Officers, Employees, etc. use external services based on the previous provision or for confidentiality 1 information, they shall apply for the uses to service providers and take appropriate measures before using the external services if they can confirm that risks of the usage are tolerated considering the contract and other conditions of the services.

8.3. Use of Social Media Service

① In the case where the Information Security Manager uses social media services using the account controlled by NINS shall take following measures for information security as well as set operation procedures for social media as needed.

(i) In order to certify that information is transmitted from NINS account, Information Security Manager shall post this information on NINS own website to make it possible to refer as well as take measures against spoofing, such as specifying an operating organization of this account in the free descriptive column, etc.

(ii) To take measures against unauthorized access in an appropriate management manner: using authentication information such as password, authentication code etc. and using recorded media (IC card, etc.)

② Transmitting information is limited to confidentiality 1 information.

③ Information Security Officer shall assign persons responsible for the social media services.

9. Assessment and Review

9.1. Handling Audit

(1) Designing Audit Plan and Cooperation for Implementation

The department subject to be audited shall cooperate with auditing.

(2) Response to Audit Results

Considering the advised matters based on the audit results, CISO should order responses for the advised matters to the Institutes CISO and Information Security Manager under jurisdiction. Furthermore, if it is highly possible to have a relevant issue or problem, the Institute CISO who doesn’t manage the matters must have the issue or problem checked. In addition, the Institute CISO shall take proper measures against Information Security Manager and Information System Manager as needed.

(3) Utilization for Review of Information Security Policy and Relevant Rules etc.

CISO, the Institute CISO and Information Security Committee must utilize the audit result when reviewing Information Security Policy etc. and other measures for information security.

9.2. Self-Check

(1) Regular Self Check Plan

The Institute CISO shall rule Self-Check Plan (including check items etc.) conducted by Information System Manager, Information Security Manager, Executive officer and Employee etc. and researchers involved in joint use and joint research, and shall make them self-check on the status of implementation of Information Security Policy (hereinafter referred as “regular self-check” once and more in a fiscal year in accordance with the provision of Article 26 of the Basic Rules. Provided however, the Institute CISO can deicide omitting all or part of the self-checks by researchers involved in joint use and joint research

(2) Self-Check by Information System Administrator and Information Security Administrator

① In the case where Information System Managers implement self-check, they must record the self-check results on the network, information system and lists of external electromagnetic recording media (an information asset ledger and an external electromagnetic recording media management ledger can be used) under jurisdiction, and if a problem is found, they must report it to the Institute CISO along with noting remediation measures.

② In the case where Information Security Managers implement regular self-check, they must write their results and if a problem is found, they must report it with noting remediation measures to the Institute CISO.

③ In the case where Information System Managers and Information Security Managers implement self-check as needed at any time, and if a problem is found, they must report it with noting remediation measures to the Institute CISO.

④ In the case where there is any report of a problem etc. about information security from Executives officers, employees, etc. and Researchers involved in Joint Use and Joint Researcher, Information System Manager and Information Security Manager must report Institute CISO along with taking remediation measures as needed.

(3) Self-Check by Executive Officers and Employees, etc. and Researchers involved in joint use and joint research

① Executive officers, Employees etc. shall implement regular inspection and self-inspection as needed. When they noticed any problem (including possibility) about information security, they shall report to the Information System Manager and Information Security Manager.

② Researchers involved in joint use and joint research shall implement regular self-inspection (limited to the case of being ordered by the Institute CISO) and self-inspection as needed and shall take remediation within scopes of their authorities based on the results. Furthermore, when they noticed any information security problem (including possibility), they shall report to Information System Managers and Information Security Managers.

(4) Report of Results from Regular Self-Check

The Institute CISO shall compile results of regular self-inspection and report to Institute Information Security Committee.

(5) Utilization of Self Check Results

① Executive officers, employee etc. must take remediation measures within scopes of their authorities based on the result of self-inspection.

② Institute CISO and Institute Information Security Committee must utilize the result of self-inspection when reviewing the Information Security Policy under jurisdiction and other information security measures (including training etc.)

③ Institute CISO shall report the results of self-inspection and measures to CISO.

④ CISO shall review Information Security Policy and Implementation Regulations based on the Article 27 of Basic Rules on Information Security Countermeasures.

9.3. Review of Information Security Policy and Relevant Rules etc.

Pertaining to the results of information security audit and self-inspection, and the change of information security circumstances, etc., CISO, Institute CISO, Information Security Committee and Institute Information Security Committee assess for each fiscal year the Information Security Policy, etc. including Information Security system when something important change happens at any time, it shall be improved periodically and as needed.

Upon reviewing Information Security Policy etc., they shall delve into important information such as confidentiality 3 or higher and comprehended the information, along with setting and implementing Security Policy based on a risk evaluation and an analysis.

10. Appendix

(1) National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Information System Operation Standard (April 1, 2008 Decision by Chief Information Officer) shall be abolished.

(2) This Countermeasures Standards shall be come into force from September 28, 2016 unless otherwise provided

(3) Notwithstanding the preceding paragraph, in the case (including the case requiring considerable amount of cost) where it is difficult to apply these standards to the settings etc. for information assets which have been operated since its effective date, the application of these guidelines may be extended until March 31, 2018, unless otherwise provided or except for the information assets categorized as confidentiality 3 and more. Provided however, further improvement must be done as early as possible along with paying attentions on information security.

(4) Rules for Important Server Managers and Appendix 2 " Encryption Guidelines" shall be applied from April 1, 2020. Provided however, it can be applied earlier than the said date.

Appended form 1

Guidelines for Data Disposal

In the case where information assets are disposed, one of the following methods should be used.

1) Physical destruction

   To destroy information assets by pulverizing, smelting, and incineration etc. and makes them unrecoverable

2) Logical destruction (Data destruction)

   To destroy information recorded in magnetic media by degaussing that makes them unrecoverable. The technique which makes the information unrecoverable by using software and hardware with a function of information destruction through the method that is generally confirmed as data-deletable such as NCSC-TG-025 (National Security Agency method) or AR380-19 (US Army Erasure Algorithm: overwriting multiple meaningless pseudorandom data and null type of data several times, and verifying the write etc.)

   Provided however, semiconductor memory such as USB etc. needs to be destroyed by physical destruction unless otherwise the logical destruction is guaranteed.

3) Logical destruction (Encryption key destruction)

   To make information which is encrypted with sufficient strength (It must to be complied with "Encryption Guidelines".) impossible to recover by discarding the encryption key.

   In the case where 1) physical destruction and 2) logical destruction (data destruction) are difficult(including the case that reuse is necessary due to personnel changes, etc.) and the recorded information (including the information recorded before is confidentiality 3 or lower and encrypted by an encryption method with sufficient strength, when the encryption key is deleted completely or discarded along with initializing (e.g. formatting the media), such case shall be handled as a logical destruction.

Appended form 2

Encryption Guidelines

When encrypting under the Information Security Policy, in principle following items and the cipher techniques in which security and implementation performance were confirmed by Advisory Board for Cryptographic Cryptography Research and Evaluation committees (hereinafter referred to as "CRYPTREC"), based on the “e-Government Recommended Ciphers List” in “The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List 1)”e-Government Recommended Ciphers List in "The list of ciphers that should be referred to in the procurement for the e-Government system (hereinafter referred to as " CRYPTREC Ciphers List ") should be applied. Provided however, if the information of Confidentiality 2 or lower has a problem about compatibility, cipher techniques based on CRYPTREC Ciphers List may be used.

※ Countermeasures etc. should be done by using other cipher techniques unlisted in e-Government Recommended Ciphers List when the cryptographic technology is found vulnerability in the e-Government Recommended Ciphers List, even though there is no problem in cypher technology, the unlisted algorism is used upon cypher derivation, or there is vulnerability

※ When encryption keys are needed, setting password provided in 5.4 (3) ② shall be complied.

Notwithstanding these guidelines, Institute CISO can rule other Encryption Guidelines as needed.

Note

1. TLS TLS1.2 and more
   (they are used in protocols such as HTTPS, SMTPS, LDAPS, FTPS, IMAPS, POP3)
   Refer to the TLS Encryption Setting Guidelines (CRYPTEC, July 2020) and use the “Suggested Security Design” or “High Security Design”. (When dealing with information higher than confidentiality 3 particularly, use the “High Security Design” in principle.)
2. WPA2
3. PGP
4. Encrypting Office 2010, Office 2013 and Office 2016
5. Acrobat
   Note : Acrobat X or more updated version (encryption level：256-bit AES) is required.

Appended form 3

References

1. Codes and Standards
   - Basic Act on Cybersecurity (Act No. 104 of 2014)
   - Order for Enforcement of the Basic Act on Cybersecurity (Act No. 400 of 2014)
   - Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (Cabinet Order No. 144 of 2000)
   - Uniform codes for information security countermeasures of governmental organizations
   - Uniform standards for information security countermeasures of governmental organizations
   - Guidelines for the operation, etc. of information security countermeasures of governmental organizations, etc.
   - Guidelines for standard formulation of countermeasures of governmental organizations, etc.
2. Applicable Security Laws and Regulations
   - Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003)
   - Unfair Competition Prevention Act (Act No. 47 of 1993)
   - Copyright Act (Act No. 48 of 1970)
   - Telecommunications Business Act (Act No. 86 of 1984)
   - Act on Electronic Signatures and Certification Business (Act No. 102 of 2000)
   - Act on Facilitation of Information Processing (Act No. 90 of 1970)
   - Act on the National Institute of Information and Communications Technology, Independent Administrative Agency (Act No. 162 of 1999)
   - Penal Code (Act No. 45 of 1907)
   - Unauthorized Computer Access Act (Act No. 128 of 1999)
3. Guideline etc. for wireless LAN operation (established by Ministry of Internal Affairs and Communications)
   - MIC Guideline for wireless LAN operation: First version Jun 25,2013, Second version September 23, 2016
   - MIC For safety introduction and implementation of wireless LAN by enterprise etc. (January 30, 2013)
   - IPA "The threat and the countermeasures when using wireless LAN"
4. Log's retention period

   In the case where Institute CISO sets a log's retention period based on 6.1(6), it should be set in a balanced and appropriate manner, taking into account of following points.

- Section 3 and 4, Article 197, Code of Criminal Procedure (Act No. 131 of July 10, 1948)

References:

Section 3 and 4, Article 197, Code of Criminal Procedure

(3) When a public prosecutor, a public prosecutor's assistant officer or a judicial police officer deems it necessary to execute a seizure or a seizure ordering records, he/she may specify the necessary electromagnetic records out of the electromagnetic records pertaining to the transmission source, the transmission destination, the date and time of the transmission and other transmission history of the electronic communications which are recorded in the course of business and, specifying a period not exceeding 30 days, may request in writing the person engaged in the business of providing facilities operating electronic communications for the use of the communications of other persons or the person establishing facilities operating electronic communications capable of intermediating the transmissions of many, unspecified persons for the purpose of its own business not to erase such history. In such case, if it is deemed no longer necessary to execute the seizure or the seizure ordering records with regard to such electromagnetic records, he/she shall revoke such request.

(4) The period requesting that the history not be erased pursuant to the provision of the preceding paragraph may be extended within a scope not exceeding 30 days if it is deemed particularly necessary; provided, however, that the total period requesting that the history not be erased shall not exceed 60 days.

5. Applicable Encryption Guidelines

- List of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)
- CRYPTREC Cryptographic Technology Guideline
- Framework for Designing Cryptographic Key Management Systems
- TLS Encryption Setting Guidelines

Appended form 4

Index