National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Basic Rules on Information Security Countermeasures

September 23, 2016
NINS Rules No. 111

Table of Contents

Chapter 1 General Provisions

(Purpose)

Article 1

The purpose of these Rules is to ensure information security in NINS as well as contribute to the smooth operation and protection of information assets of NINS based on the Basic Policy of Ensuring Information Security (Decision by the Board of Directors of 2016; hereinafter referred to as the "Basic Policy") of the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation (hereinafter referred to as "NINS").

(Information Security Countermeasures Policy)

Article 2 In order to achieve the objectives of the Basic Policy, NINS shall observe the following information security countermeasures policy and implement countermeasures:

(i) Construction and maintenance of the information security management system
(ii) Ensuring the necessary budget to implement the information security countermeasures
(iii) Protection of information assets and personal information

(iv) Implementation of information security education, training, and awareness raising activities for information system users including executive officers and employees

(v) Infiltration of the organization of the information security policy and related rules

(vi) Information system security maintenance and improvement

(vii) Improve the system, procedure manual, etc. against information security incidents.

(viii) Network monitoring, etc. and use information acquisition

(ix) To grasp the situation of managing the information system and implementation of required measures

(x) Review of information security policy based on self-inspection for information security countermeasures, audit implementation, and their results, or the like.

(xi) Other countermeasures in responding to information security threats, etc. surrounding NINS

(Definitions)

Article 3 In this rule, the definitions of the terms listed in the following items shall be as provided in the respective items:

(i) Networks mean information system(s) implemented with a collection of interconnected components including communication lines, routers.

(ii) Information systems mean a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(iii) Information facilities and equipment mean computer rooms, communications branch panel, distribution boards, power supply cables, communications cables, etc.

(iv) Electronic or magnetic storage media mean physical devices or writing surfaces including magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, onto which information is recorded, stored, or printed within an information system

(v) Information handled in networks and information system means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

(vi) System-related documents mean system design documents, program specifications, operation manuals, terminal management manuals, network configuration diagrams, etc.

(vii) Information assets mean Networks, Information systems, Information facilities and equipment, Electronic or magnetic storage media, Information handled in networks and information system and System-related documents.

(viii) Information security means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability based on the information asset classification provided in Appended Table 1.

(ix) Information security policy means the Basic Policy, these rules, and the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Security Countermeasures Standards (hereinafter referred to as the "Countermeasures Standards") provided by the Chief Information Security Officer (hereinafter referred to as the "CISO") based on Paragraph 3, Article 5.

(x) Implementation regulations mean regulations and plans provided by the CISO based on the information security policy.

(xi) Incidents mean a violation or imminent threat of violation of the security policy of NINS, laws, acceptable use policies, or standard security practices intentionally or accidentally.

(xii) Personal information means personal information prescribed in the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Personal Information Protection Rules (NINS Rules No. 54 of 2005).

(xiii) Each institute means the inter-university research institutes provided in Paragraph 1, Article 2 of the National Institutes of Natural Sciences, an Inter University Research Institute Corporation, General Rules for Organization and Operation (General Rules No. 1 of 2004; hereinafter referred to as the "General Rules for Organization and Operation).

(xiv) Each institute, etc. means the category including institutes set forth in Appended Table No. 2.

(xv) Executive officers, employees, etc. mean executive officers and all persons who are employed based on the employment regulations provided by NINS.

(xvi) Joint users, joint researchers, etc. mean all persons other than those listed in the preceding item who use information assets of NINS.

(xvii) Electronic or magnetic storage means records made by an electronic form, a magnetic form, or any other form not recognizable to human perception, which is used in information processing by computers.

(xviii) Research information means information arising from research activities (including analysis) from among information, etc. listed in Item 5 and Item 6.

(Scope)

Article 4 The scope of application of the information security policy shall be the scope prescribed in any of the following items; provided however, that it excludes those provided in the countermeasures standards by the CISO.

(i) Information assets owned or managed by NINS

(ii) Information equipment linked to the network and information system owned or managed by NINS and those deemed not to fall under the preceding item

(iii) Information assets provided based on a contract or agreement concluded with NINS

(iv) Information which was prepared or acquired for research, education, or other operations of NINS by persons who use information assets provided in Item 1 or the preceding item or information equipment provided in Item 2 (including persons other than executive officers, employees, joint users and joint researchers and the same applies hereinafter) and those stored in such information system or information equipment

(v) Information which was prepared and acquired for research, education, or other operations of NINS by executive officers, employees, joint users, joint researchers, etc. and those deemed not to fall under the preceding two items

2 Persons who operate, manage, or use information assets provided in the items of the preceding paragraph shall observe the information security policy.

Chapter 2 Organization

(Chief Information Security Officer)

Article 5 The CISO shall be assigned to NINS and the Executive Director in charge of information or Vice President in charge of information shall serve as the CISO.

2 The CISO shall have comprehensive authority and responsibility concerning the development, management, and operation of information assets of NINS and information security countermeasures (hereinafter referred to as “Information Security Countermeasures, etc.”)

3 The CISO shall have full powers concerning the Countermeasures Standards and shall establish these to appropriately implement matters provided in the Basic Policy and these rules.

4 The duties and responsibilities of the CISO shall be provided in the Countermeasures Standards.

(Institute Information Security Officer)

Article 6 The Institute Information Security Officer (hereinafter referred to as the "Institute CISO") shall be established as shown in Appended Table No. 2.

2 The Institute CISO shall conduct overall management concerning the implementation of Information Security Countermeasures provided in Article 25, etc. at the organization under his/her jurisdiction.

3 The duties and responsibilities of the Institute CISO shall be provided in the Countermeasures Standards.

(Information Security Auditing Office)

Article 7 NINS shall have an Information Security Auditing Office and it shall be organized to consist of persons who falls under any of the following items to audit the observance of the information security policy at NINS.

(i) Information Security Audit Manager

(ii) Information Security Audit Implementer

2 The Information Security Audit Manager shall be the Information Security Auditing Office Director.

3 The duties of the Information Security Auditing Office shall be as follows:

(i) Establish the information security audit schedule and audit plan at NINS.

(ii) Implement the information security audit at NINS.

(iii) Compile the results of the information security audit into a report

(iv) Other matters relating to the information security audit at NINS

4 Other necessary matters concerning the Information Security Auditing Office shall be provided by the Information Security Auditing Office Director.

(Information Security Audit Manager)

Article 8 The Information Security Audit Manager shall be appointed by the President from among the executive officers, employees, etc. of NINS.

2 The Information Security Audit Manager shall conduct overall management concerning the information security audit provided in Article 25.

(Information Security Audit Implementer)

Article 9 The Information Security Audit Implementer shall be appointed by the Information Security Audit Manager from among the executive officers, employees, etc.

2 Notwithstanding the provisions of the preceding paragraph, where the Information Security Audit Manager deems necessary, a person outside NINS including an expert in

the private sector may be selected as the Information Security Audit Implementer with the consent of the President.

3 The Information Security Audit Implementer shall be a person independent of the department being audited.

4 The Information Security Audit Implementer shall be a person with expert knowledge on audit and information security.

5 The Information Security Audit Implementer shall implement the audit provided in Article 25 based on the instructions of the Information Security Audit Manager.

(Information Security Advisor)

Article 10 NINS may establish an Information Security Advisor as needed.

2 The Information Security Advisor shall be commissioned by the CISO from among NINS employees who have expert knowledge and experience on information security.

3 Notwithstanding the provisions of the preceding paragraph, where the CISO deems necessary, a person outside NINS including an expert in the private sector may be selected as the Information Security Advisor with the consent of the President.

4 The duties of the Information Security Advisor shall be provided by the CISO.

(Information Security Officer)

Article 11 The Information Security Officer shall be established under the Institute CISO and assumed by a person appointed by the Institute CISO.

2 The duties and responsibilities of the Information Security Officer shall be provided in the Countermeasures Standards.

(CSIRT)

Article 12 A CSIRT (Computer Security Incident Response Team) shall be established under NINS.

2 The CSIRT shall consists of Institute CSIRTs as prescribed in the following paragraph.

The Institute CSIRT shall be established under the Institute CISO and composed of persons appointed by the Institute CISO.

4 The Institute CISO may designate persons by dispatch and entrustment of business other than executive officers and employees as the Institute CSIRT ; provided however, that not less than 1 person shall be designated from among executive officers and employees.

5 The duties and responsibilities of the CSIRT and Institute CSIRT shall be provided in the Countermeasures Standards.

(Information System Manager)

Article 13 The Information System Manager shall be established under the Institute CISO and assumed by a person appointed by the Institute CISO.

2 The Information System Manager may be appointed more than one, however, one information system shall have one Information System Manager; provided however, that this shall not apply in cases where the Institute CISO deemed it necessary.

3 The Institute CISO shall designate the Information System Manager in cases where networks, information system, and external electronic or magnetic storage media (limited to those which falls under Item (i) and Item (iii), Paragraph 1, Article 4; hereinafter referred to as the "Management Information System") are operated.

4 The Institute CISO may designate the Information System Manager if necessary with regard to networks, information systems, external electronic or magnetic storage media other than the Management Information System set forth in the preceding paragraph.

5 The duties and responsibilities of the Information System Manager shall be provided in the Countermeasures Standards.

(Person in Charge of Information System)

Article 14 The person who engages in work including the development of information assets, change, operation, update, etc. of settings under the order of the Information System Manager shall be the person in charge of information system.

2 The person in charge of information system shall be assumed by a person appointed by the Information System Manager.

(Technical Officer, etc.)

Article 15 The Institute CISO may establish an Information System Deputy Manager, Information Security Technical Officer, Information Security Deputy Technical Officer, etc. as needed.

2 Necessary matters in the preceding paragraph shall be provided by the Institute CISO of the relevant institute.

(Information Security Manager)

Article 16 The Institute CISO shall have an Information Security Manager and assumed by the Document Controller provided in Article 5 of the National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Corporate Document Management Rules (NINS Rules No. 50 of 2004).

2 The Information Security Manager shall have authority and responsibility concerning information security measures of the division, office, etc. under his/her jurisdiction.

(Information Security Committee)

Article 17 Based on Article 12-6 of the General Rules for Organization and Operation, an information security committee led by the CISO in NINS as the chairperson shall be established to make decisions on important matters concerning Information Security Countermeasures, etc. in NINS as a whole including information security, matters concerning crisis management, and matters concerning ethics.

2 Necessary matters concerning the organization and operation of the committee provided in the preceding paragraph shall be provided for separately.

(Institute Information Security Committee)

Article 18 An information security committee led by the Institute CISO in institutes, etc. as the chairperson shall be established to carry out Information Security Countermeasures, etc. to be treated individually in NINS and make decisions on important matters concerning Information Security Countermeasures, etc. including information security policies in institutes, etc.

2. Necessary matters concerning the organization and operation of the committee provided in the preceding paragraph shall be provided for separately.

(Prohibition of concurrent service)

Article 19 The following roles may not concurrently be served by the same person in principle in the implementation of Information Security Countermeasures.

(i) Person who obtains approval or permission and person who provides the approval or permission (excluding cases acknowledged by the Institute CISO)

(ii) Person who receives the audit and person who conducts the audit

2 Notwithstanding the preceding paragraph, the CISO may hold a concurrent position as Information Security Audit Manager.

Chapter 3 Protection of Information Assets

(Classification, Rating, and Handling Restrictions of Information Assets)

Article 20 The Information Security Manager shall classify information assets under jurisdiction into confidentiality, integrity, and availability, assign an appropriate rating, and implement handling restrictions based on the classification, rating, and handling restrictions of information assets provided in Appended Table 1.

2 With respect to research information, when the Institute CISO finds the assigning of classification, rating, and handling restrictions of information assets provided in

Appended Table 1 grossly unreasonable, the Institute CISO may provide for this separately.

3 Necessary matters concerning the application of the provisions of Paragraph 1 shall be provided in the Countermeasures Standards.

Chapter 4 Information System Life Cycle

(Information System Life Cycle)

Article 21 Necessary matters concerning the installation, operation, and disposal of information systems owned or managed by NINS shall be provided in the Countermeasures Standards.

Chapter 5 Handling of Incidents

(Handling of Incidents)

Article 22 Necessary matters concerning the handling of incidents shall be provided in the Countermeasures Standards.

Chapter 6 Monitoring, etc. of Networks

(Monitoring, etc. of Networks)

Article 23 The person who manages, operates, or uses information assets provided in Item (i) or Item (iii), Paragraph 1, Article 4 or information equipment provided in Item (ii) of the same paragraph must not intercept transmission conducted via networks. Provided however, that the person appointed by the CISO or Institute CISO in advance and Information System Manager who manages the network (limited to the scope of the jurisdiction) (hereinafter referred to as the "network supervisor") may conduct the monitoring of transmission conducted via networks (hereinafter referred to as "monitoring") for the purpose of ensuring security.

2 The network supervisor in the preceding paragraph must not communicate the contents of the transmission or personal information known by monitoring to another person except in cases specified by the Countermeasures Standards as necessary for the prevention of critical security infringement inside or outside NINS.

3 The scope and procedure of the monitoring, handling of the records collected by monitoring and other necessary matters shall be provided by the Countermeasures Standards.

(Record of Use)

Article 24 The collection and handling of the record of use of the information system shall be provided by the Countermeasures Standards.

Chapter 7 Information Security Audit and Inspection

(Audit)

Article 25 The Information Security Audit Manager shall engage in the audit of the status of implementation of the information security policy and implementation regulations and status of the Information Security Countermeasures pertaining to information assets periodically for each year or as needed.

2 Where entrusted to an outsourcing company, the Information Security Audit Manager shall engage in the audit of the observance of the information security policy as needed including the trustee company as a subcontractor from the outsourcing company.

3 The Information Security Audit Manager shall formulate the audit plan and obtain approval of the President and CISO in engaging in the audit.

4 The Information Security Audit Manager shall compile the results of the audit and report to the President and CISO in case of conducting the audit.

5 The Information Security Audit Manager shall appropriately retain the audit evidence collected through the conduct of the audit and audit record for the preparation of the audit report to prevent loss, etc.

(Self-inspection)

Article 26 The Institute CISO shall conduct self-inspection of the status of implementation of the information security policy and implementation regulations in the institute and report to the CISO, more than once a year.

Chapter 8 Information Security Policy, etc. Review

(Renewal of the Policy and Implementation Regulations)

Article 27 The CISO shall regularly review the information security policy and implementation regulations taking into account the audit in Article 25, result of the self-inspection in the preceding article, and incidents in NINS.

Chapter 9 Miscellaneous Provisions

(Other)

Article 28

In addition to what is provided for in these Rules, necessary matters concerning the information security of NINS shall be specified by the Countermeasures Standards.

Supplementary Provisions

1 These Rules shall come into force from September 23, 2016.

2 The National Institutes of Natural Sciences, an Inter-University Research Institute Corporation, Basic Rules on Informatization of Business and Assurance of Information Security (NINS Rules No. 67 of 2007) shall be abolished.

Supplementary Provision

These Rules shall come into force from December 22, 2016.

Supplementary Provision

These Rules shall come into force from March 1, 2018.

Supplementary Provision

These Rules shall come into force from April 1, 2018.

Supplementary Provision

These Rules shall come into force from November 1, 2018.

Supplementary Provision

These Rules shall come into force from December 1, 2019.

Supplementary Provision

These Rules shall come into force from December 4, 2020.

Appended Table 1 Classification, Rating, and Handling Restrictions of Information Assets (related to Article 3 and Article 20)

Classification of information assets by confidentiality

Classification	Classification Standards	Handling Restrictions
Confidentiality 4 (Top Secret)	Information assets that have serious and material impact to the operations of NINS where contents including those in regard to national security, specific personal information, etc. are leaked	In addition to the handling restrictions of confidentiality 3, unless permitted by the Institute CISO, measures are set forth below. ・Prohibition of reproduction and distribution ・Prohibition of access to other than the designated place ・The operation shall be limited to the scope of standalone or independent networks.
Confidentiality 3 (Secret)	Among information assets handled in NINS, information assets requiring confidentiality equivalent to Confidential Documents	In addition to the handling restrictions of confidentiality 2 (excluding exceptional measures), measures except in such cases as permitted by the Institute CISO are set forth below. ・General prohibition of work in other information system terminals which are assets of NINS ・Prohibition of reproduction and distribution that are more than necessary ・Retention of a place where electronic or magnetic storage media can be locked

Classification	Classification Standards	Handling Restrictions
Confidentiality 2 (NINS Confidential)	Among information assets handled in the operations of NINS, confidentiality equivalent to Confidential Documents is not required, however, information assets that have a possibility of breaching the rights of individuals or interfering with the performance of operations of NINS upon disclosure (including personal information when the person in question has given consent to handle it in classification category)	・ Restriction on place of storage and prohibition of bringing electronic or magnetic storage media, etc. that is more than necessary into the place of storage ・ Encryption and password setting during transmission of information, transport and provision of information assets and storage in a locked case ・ Disposal subjected to treatment beyond restoration ・Choice of a secure network line ・Provisions of measures to ensure security management when conducting information processing externally 【Exceptional measures】 Exceptional measures of the Countermeasures Standards shall apply notwithstanding the foregoing in cases where it is provided for in exceptional measures by the Countermeasures Standards.

Classification	Classification Standards	Handling Restrictions
Confidentiality 1 (Disclosure)	Published information, information that is allowed to be published, and other information and information assets other than information assets of more than confidentiality 2	

Classification of information assets by integrity

Classification	Classification Standards	Handling Restrictions
Integrity 3	Information assets which are difficult to recover due to damage and alteration and information assets which would have serious and material impact to the operations of NINS	In addition to the handling restrictions of integrity 2, measures are set forth below. ・ Multiple backups of different storage areas ・ Detection of tampering by digital sign, storage of hash, time stamp authentication, etc. or implementation of prevention measures
Integrity 2	Among information assets handled by NINS, information assets that are likely to infringe the rights of individuals or obstruct the appropriate execution of operations of NINS (excluding minor ones) and information assets that do not fall under integrity 3 due to alteration, error, and damage	・ Backups and granting of electronic signature ・ Detection of tampering by digital sign, storage of hash, time stamp authentication, etc. or implementation of prevention measures[1] Excluding cases where it is recognized by the Institute CISO ・ Provisions of measures to ensure security management when conducting information processing externally ・ Retention of a place where electronic or magnetic storage media can be locked
Integrity 1	Information assets other than information assets of more than confidentiality 2	

1 Require no tamper prevention measures on media in the case where tamper-proof media (WORM media, etc.) are used

Classification of information assets by availability

Classification	Classification Standards	Handling Restrictions
Availability 3	Information assets which would have serious and material impact to the operations of NINS unless used regularly	In addition to the handling restrictions of availability 2, measures are set forth below. ・ Clustering configuration based on fail-over and failsafe
Availability 2	Among information assets handled by NINS, information assets that are likely to infringe the rights of individuals or obstruct the appropriate execution of work of NINS (excluding minor ones) and information that does not fall under confidentiality 3 due to extinguishment, loss, or it is impossible to use the information assets between one hour and 24 hours	・ Backups and recovery within the designated time ・Retention of a place where electronic or magnetic storage media can be locked
Availability 1	Information assets other than information assets of more than availability 2	

Appended Table 2 (related to Article 6)

<table>
<tr><th>Category including Institutes</th><th>Institutes, etc.</th><th>Institute CISO</th></tr>
<tr><td>National Astronomical Observatory of Japan</td><td>National Astronomical Observatory of Japan</td><td>A person designated by the Director General of the National Astronomical Observatory of Japan</td></tr>
<tr><td>National Institute for Fusion Science</td><td>National Institute for Fusion Science</td><td>Director General of the National Institute for Fusion Science</td></tr>
<tr><td rowspan="4">Three Okazaki Institutes</td><td>National Institute for Basic Biology</td><td rowspan="4">Deputy Director General, Vice-Director General,
Executive Director, or Chief Chairperson designated together by the three (3) Director Generals</td></tr>
<tr><td>National Institute for Physiological Sciences</td></tr>
<tr><td>Institute for Molecular Science</td></tr>
<tr><td>Joint Use Research Facilities, Organizations, etc. for the Three Okazaki Institutes</td></tr>
<tr><td>Exploratory Research Center on Life and Living Systems</td><td></td></tr>
<tr><td>Administrative Bureau, etc.</td><td>Among the Administrative Bureau and organizations, etc. provided for in Paragraph 1, Article 2-2 and Article 3 of the General Rules for Organization and Operation, organizations, etc. that do not fall under the foregoing</td><td>Concurrent service by the CISO</td></tr>
</table>

Note: In regard to the Center for Novel Science Initiatives specified in Item (i), Article 2-2, Astrobiology Center specified in Item (ii) of the same article, and International Research Collaboration Center specified in Item (iv) of the same article of the General Rules for Organization and Operation, the Institute CISO of the institutes, etc. shall have jurisdiction.