Nara Institute of Science and Technology

Information Security Policy

June 22, 2006
Date of revision: August 1, 2010
Date of revision: April 1, 2012
Date of revision: December 1, 2013
Date of revision: December 1, 2014
Date of revision: September 20, 2016
Date of revision: April 1, 2017
Date of revision: December 19, 2017

TABLE OF CONTENTS

I. Fundamental information security policy

1. Fundamental information security policy

It is essential for Nara Institute of Science and Technology (hereinafter referred to as “NAIST”) to prepare an information infrastructure and ensure the security of the NAIST’s information Assets in order to expand academic research, educational activities, and social contributions in an advanced information society. For the purposes of making all NAIST constituent members (its faculty, staff members, students etc.) thoroughly aware of the importance of information security and for the strict protection of information Assets, this information security policy is stipulated based on the Information Security Policy Guidelines (decided upon by the information security measures promotion committee on July 18, 2000).

Based on this policy, NAIST shall strive to undertake the items stated below.

(1)	Prevention of infringement of information security
(2)	Prevention of damaging actions that harm information security
(3)	Ranking and management according to the degree of importance of Information Assets
(4)	Support for obtaining information related to information security

Additionally, due to the fact universities differ from ordinary agencies in which a small number of System Managers provide Information Systems and specific users use them, consideration shall be given to points such as those below.

- Users include not only faculty and staff, but also students
- Information devices that are brought into academic conferences, lectures, and symposiums that are held at NAIST may also be subject to the policy

At NAIST, information security shall be secured by the measures below.

1) Organizations and systems

The Chief Information Security Officer shall serve as the chairperson of the Information Security Committee and promote information security measures at NAIST. In addition, stipulations shall be made for the procedures that should be taken, and the systems and organizations where they should be implemented as measures for Information Assets, such as network isolation against attacks from

outside NAIST and damaging actions from within NAIST.

2) Rating and managing information

Stipulations shall be made to rank all electromagnetically recorded information handled at NAIST, based on the information's degree of importance and methods of management, and management liability. All departments shall conduct ranking based on the degree of importance and analyze the risks due to falsification and destruction.

3) Physical measures

Safety shall be maintained and measures established to prevent improper entry to places where Information Systems are maintained. Protection shall also be maintained for Information Assets, such as desktop and notebook computers that are presumed to be carried around.

4) Technical measures

The necessary technical measures shall be implemented for the control and management of access to information networks to prevent destruction of Information Assets due to fraudulent access by external parties.

5) Human measures

All constituent members shall be made thoroughly aware of this policy, stipulations shall be made for the authority and liability that each person has for Information Assets, and measures shall be implemented for education and educational activities in order to ensure information security.

6) Evaluation and reconsideration

Naist shall regularly reconsider this policy and strive to constantly raise security levels in response to information technology developments and compliance with formulated policies. In addition, measures for auditing security shall also be implemented.

2. Definitions

The definitions of terms used in this policy shall be as stated below.

2.1 Information Systems

Systems at NAIST that consist of the hardware, software, and recording media, and that process work by using these as a whole

2.2 Information Assets

The general term for information and mechanisms that manage information (Information Systems and materials for developing, operating, and maintaining systems)

2.3 Users

Refer to directors, faculty and staff members, students, and others engaged in education, research, clerical work, or technical duties at NAIST and who use NAIST information networks

2.4 System Manager

Refers to the Director of the Information Initiative Center or another person who manages NAIST's Information Systems

3. Subject scope

The subject scope of the policy shall be, of Information Systems such as hardware, software, and recording media (including documents such as system configuration diagrams) and all information, the information that is electromagnetically recorded in Information Systems, and those who come into contact with such information. For that reason, in this policy, information about Information Assets shall be limited to that which has been electromagnetically recorded. In addition, computers outside NAIST that are temporarily connected to a NAIST network shall be included.

Directors, faculty and staff members (full-time and fixed-term contract faculty and staff members, adjunct lecturers and temporary employees [including external consignment]), students (including special auditing students, special research students, credited auditors, research students, and visiting students), and visitors shall be subject to this policy.

4. Creation of implementation procedures

Each department shall stipulate specific implementation procedures in accordance with this fundamental policy.

II. Basic information for measures

1. Organizations and systems

1.1 Management and operation organization

1.1.1 Chief Information Security Officer

The Chief Information Security Officer shall be in charge of comprehensive decision-making related to campus-wide information security, organizations within NAIST, and parties outside NAIST. The Executive Director in charge of information management or the Vice President shall serve in this position.

1.1.2 Campus System Administrator

The Campus System Administrator shall assist the Chief Information Security Officer in the comprehensive handling of cases of emergency, etc. in relation to

implementation of NAIST's campus-wide Information System management. The Director of the Information Initiative Center Shall serve in this position.

1.1.3 Department System Administrator

The Department System Administrator shall be in charge of System Managers for handling communication with the Campus System Administrator, etc. in relation to implementation of Information System management within departments. The manager of each department (for the Administration Bureau, the director-general) or the person designated by the manager of that department shall serve in this position.

1.1.4 Information Security Committee

The Information Security Committee shall formulate fundamental security policies, decide about important matters, and handle external parties in relation to campus information security. It shall conduct advanced education for Department System Administrators and System Managers concerning education related to information security and conduct introductory education for a broad range of ordinary Users. It shall consist of persons such as the Chief Information Security Officer and Campus System Administrator.

1.1.5 System Management Subcommittee

A System Management Subcommittee shall be established under the Information Security Committee, and shall coordinate communication to perform security management for NAIST's campus-wide Information Systems to provide support such as technical advice for Department System Administrators. It shall consist of persons such as the Campus System Administrator and the System Managers designated by Department System Administrators.

1.1.6 Computer Security Incident Response Team (CSIRT)

A Computer Security Incident Response Team (hereinafter referred to as the "CSIRT") shall be established under the Information Security Committee, and that team shall quickly and smoothly handle information security incident occurs at NAIST. The necessary matters related to CSIRT shall be stipulated separately by the Information Security Committee.

1.2 Handling of information security incidents

In the event that the CSIRT learns of an information security incident from a party within or outside NAIST, it shall follow the written procedures for handling information security incidents stipulated by the Information Security Committee and block related communication or disconnect the relevant information devices. To restore the relevant information devices, the Information Security Committee

shall make judgments based on reports by the System Manager for the relevant system and CSIRT.

1.3 Contact system for emergencies

The contact system for emergencies shall be as stipulated in the information management section of edition 2 of Type-III improprieties in NAIST's *Crisis Management Manual*. The necessary organization, such as the Ministry of Education, Culture, Sports, Science and Technology, shall be contacted as promptly as possible with information related to cyberattacks for which damage was incurred, after the Chief Information Security Officer's decision and based on the *Crisis Management Manual*.

2. Ranking and management of information

2.1 Access restriction

In accordance with the content of information, System Managers must limit the people who have authority to access this information to the minimum number of Users necessary in order to accomplish the purpose of use of this information. Users may not access Information Systems or information for which they do not have access rights.

2.2 Ranking of information

Department System Administrators shall implement the measures necessary to ensure that ranking for each item of information is conducted appropriately.

2.3 Limited public release of information

In the event that specific information will be released to a specific user, authentication and access restriction functions must be set so that registration of and access to the information may be conducted only by an operation that is permitted. In addition, the situation must be regularly confirmed to see whether abnormal registration or access is being conducted.

2.4 Prevention of information falsification and dissemination of false information

For original copies of information, originality must be guaranteed by saving them on storage media for which rewriting is not possible. In addition, a System Manager must be established for each respective Information System.

2.5 Disposal of information devices and storage media

In the event that information devices or storage media will be disposed of, disposal must be conducted so that external parties cannot decipher recorded content.

3. Physical measures

For each client, server, network device, and network cable, it is necessary to implement physical measures against security infringement.

4. Human measures

4.1 Duties

All Users must comply with this policy.

4.2 Consideration for the convenience of education and training

For points that significantly impair the convenience of education and training or points for which compliance is difficult in practice for Information System security measures, faculty, staff members, and students may ask the Chief Information Security Officer to improve policy implementation procedures.

4.3 Education and training

The information security committee must support training related to the policy that is intended for faculty and staff members and conducted by System Managers. It must also cooperate with orientation or lectures related to the policy that are intended for students and conducted by faculty members.

4.4 Faculty and staff members, and external consignment

4.4.1 Educational affairs and clerical work

For the conclusion of employment agreements, faculty and staff members (including consigned external companies) shall be made to understand the policy contents they should obey and to implement and comply with these policies.

4.4.2 Development of Information Systems, maintenance, and management duties

In the event an order will be placed to a consigned external company for development or maintenance of an Information System or system management duties, an agreement that clearly states compliance with this policy's content with the consigned external company, including businesses that receive consignment subcontracted from the consigned external company, must be concluded. An agreement with a consigned external company must stipulate the boundaries of liability and provisions for cases in which a party does not comply with this policy.

5. Technical measures

5.1 Network operation policy

It is necessary for the Information Security Committee to design, construct, and operate networks to allow the handling of threats from external parties and attacks made by internal parties against external parties. Users must accept network intrusion detection system and other installed protective software traffic

inspections, and measures for blocking communication when incidents occur.

5.2 Criteria related to terminal equipment

Equipment that connects to a network must be able to conduct authentication of Users by some method. A person who intends to install equipment may not connect to a network any devices for which settings, including security measures, has not been completed. For a System Manager, it must be possible to identify the Users of installed equipment. System Managers must disclose to the Information Security Committee any information related to the operation of logs upon request of the committee.

6. Evaluation and reconsideration

6.1 Actual operation of the policy

The Campus System Administrator must regularly hold system management subcommittee meetings, analyze and organize collected information, and then make a report to the Information Security Committee. The Information Security Committee must then consider this policy based on the state of operation of this policy throughout NAIST.

6.2 Measures for improving the security level

The Information Security Committee must evaluate this policy’s effectiveness at least once a year and, if improvement is necessary, must decide changes of content and the time of implementation, and update the policy to improve security and make it a policy for which compliance is possible. The Information Security Committee must create information security plans and budget drafts based on the results of evaluation and reconsideration.

Nara Institute of Science and Technology Information Security Organization Diagram