Earth-Life Science Institute

Tokyo Institute of Technology

Operating Guidelines for Information Security

2013

1. Purpose

The Operating Guidelines for Information Security (hereinafter, the “Operating Guidelines”) at the Earth-Life Science Institute, Tokyo Institute of Technology (hereinafter, the “Institute”), is intended to define the operating procedures for faculty, administrative and technical staff, and students to ensure the security of information assets in compliance with the National University Corporation Tokyo Institute of Technology Information Security Regulations (Regulation No. 32 of 2005) (hereinafter, the “Information Security Regulations”).

Hereinafter, “staff” includes all individuals employed by the Institute in an administrative, technical, full-time, short-time, or fixed-term capacity, as well as outsourcing contractors, “student” includes both degree and non-degree students, such as special register students and research students, and “duties” includes but is not limited to education, research, and administrative work performed at the Institute.

2. Organization

The organization is established as below in order to ensure the smooth performance of the Institute related duties.

Information Security Chief Supervisor: Director, Earth-Life Science Institute
Information Security Deputy Supervisor: Vice Director, Earth-Life Science Institute
Information Security Supervisor: Head of Administration and appointed by Chief Supervisor
Information Assets Administrator: Staff member
Contact Person: Appointed by Information Assets Administrator
Information Systems Administrator: Appointed by Information Assets Administrator

3. Compliance Provisions

Those who intend to use Institute information systems and comprised data shall observe the items listed below, in accordance with the National University Corporation Tokyo Institute of Technology Information Ethics Policy and National University Corporation Tokyo Institute of Technology Information Security Policy, for the purpose of preventing illegal access to Institute information assets.

For Faculty and Staff:

1) Perform your duties in accordance with the Operating Guidelines to prevent failures in information security.

2) Comply with the National University Corporation Tokyo Institute of Technology Personal Information Protection Regulations (Regulation No. 5 of 2005) (hereinafter, the "Personal Information Protection Regulations") and National University Corporation Tokyo Institute of Technology Personal Information Management Regulations (Regulation No. 6 of 2005). If you are unclear about any of the aforementioned regulations, consult the Information Assets Administrator and/or Chief Supervisor immediately.
3) In the event that you discover conduct in violation of the Personal Information Protection Regulations, contact the Information Security Chief Supervisor and Information Security Supervisor immediately.
4) In the event that you discover an information security incident, system vulnerability, or system malfunction, contact the Information Assets Administrator. For major incidents, the Information Assets Administrator should report to the Information Security Chief Supervisor and Information Security Supervisor and take measures as directed.

For Faculty, Staff, and Students:

1) When using the information systems, do so in an ethical and defensive manner in accordance with the Guide for Information Ethics and Security, Article 5 of the National University Corporation Tokyo Institute of Technology Information Ethics Regulations (Regulation No. 31 of 2005).

4. Management and Use of Information

Hereinafter, pursuant to Article 2 of the Information Security Guidelines, "information" refers to all content data written on paper or electromagnetic media concerning education, research and administrative matters undertaken by the Institute.

Information Subject to the Operating Guidelines:

1) Information which is created or obtained in the process of pursuing the Institute's activities and is required to be classified or preserved by law, contract, or Institute regulations.
2) Copies of information which belong to another department (here and hereinafter including administrative departments, research laboratories, and all other Institute affiliations) and are classified under category II or IV, described in Information Categories, by that department.
3) Other information which the Information Security Chief Supervisor, Information Security Supervisor, or the Information Assets Administrator deems important.

The Information Security Chief Supervisor, in cooperation with the Information Security

Supervisor, is responsible for ensuring that faculty and staff abide by the Operating Guidelines to prevent leakage of confidential information (through such incidents as loss or theft of media) as well as unintended alteration or deletion (incidents in which the information cannot be restored). The same applies for outsourcing contractors.

Information Categories

In accordance with Article 4 of the Information Security Regulations, all information is classified into the four categories below based on importance level of confidentiality, uniformity and availability.

I) Information that should not be disclosed outside of the Institute or to other departments at the Institute

II) Information that should not be disclosed outside of the Institute

III) Information of high importance that can be disclosed to the public

IV) Information of high importance other than those listed above

The term “information of high importance” is interpreted as information whose loss or leakage could hinder duties.

Due care should be paid to the following regarding categorization.

1) In general, the Information Assets Administrator of the particular department that created or obtained the information is responsible for categorization. For information made in cooperation between multiple departments, the Information Assets Administrator appointed by the Information Security Chief Supervisor or the Information Security Supervisor shall hold responsibility. The same applies for recategorization of existing information.
2) Information that should be confidential is to be classified as Category I or II. If it is not necessary to categorize as confidential and is not currently intended for public disclosure, the information should be classified as Category IV. Information for public disclosure should be classified as Category III.
3) The date of deletion or recategorization can be established beforehand. For Categories I and II, the date is considered on a minimum requirement, and the information should be deleted or recategorized within the period in which such status will not hinder duties.
4) When obtaining a copy of information managed by another department, treat the information according to its category decided by that department. No deletion measures are required in this case.

Data Administration

1) Access to confidential information (Category I, II) should be limited to only faculty and staff who require it. Control methods should be chosen depending on the situation, such as physical restriction using a lock or electronic restriction using encryption. Countermeasures should be taken against illegal access to networked computers. Furthermore, these measures should be applied not only for original information but copies as well.
2) Taking confidential information (Category I, II) outside of the Institute (including electronic transmission) requires authorization from the Information Assets Administrator. In order to prevent data leakage, communications should be encrypted and removable media containing data should be physically or electronically secured.

   In cases where applying such measures is difficult (equipment repair, etc.), establish a non-disclosure agreement with persons (technical contractor, etc.) who may be able to access the information.
3) Creating or destroying copies of confidential information (Category I, II) requires authorization from the Information Assets Administrator. The destroyed copy should not be restorable. Use specialized software or physically destroy the media, as using operating system commands or formatting disks does not guarantee complete erasure of the data stored therein.
4) For data (all Categories) stored electromagnetically, backups should be made to protect against unexpected incidents.
5) In addition to items (1) through (4) above, observe all laws, contracts, and Institute regulations.

Outsourcing Data Processing and Storage Services

1) When outsourcing data processing and storage services, outsourcing contracts should be made in accordance with Article 13 of the Information Security Regulations.

5. Security Systems Management

Anti-Theft Security

1) Lock the door when leaving a room with computer equipment unattended. If, due to relevant circumstances, it is difficult to lock the door, make appropriate arrangements such as using a surveillance camera, etc.

Prevention of Illegal Access

1) Access should be limited appropriately to prevent use of information systems by unauthorized persons. Means to prevent illegal access include physical entrance restrictions,

passwords, hardware tokens (IC card, RFID, etc.), and biometric authentication.

Security against Cyber Threats

1) Apply the latest OS and application security patches as soon as they are available.
2) Keep pattern files for your antivirus software, personal firewall, and other intrusion detection/prevention systems as up to date as possible.

Security against Power Failures

1) Install uninterruptible power supply systems for important computer equipment.

Outsourcing Information System Development, Administration, and Maintenance Services

1) When outsourcing information system development, administration, and maintenance services, outsourcing contracts should be made in accordance with Article 13 of the Information Security Regulations.

6. Personnel Management

Operating Guidelines Familiarization

1) The Information Security Chief Supervisor, in cooperation with the Information Security Supervisor, is responsible for ensuring that faculty and staff (as well as students) who use the information systems abide by the Information Security Regulations and the Operating Guidelines. The same applies for outsourcing contractors.
2) The Information Security Chief Supervisor shall take actions to make the Information Security Regulations and Operating Guidelines referable at all times.

Compliance Review

1) Both the Information Security Chief Supervisor and Information Security Supervisor must periodically review compliance with the Information Security Regulations and verify the absence of information security failures.

Incident Reports

1) In the event that an information security incident, system vulnerability, or system malfunction is reported, the Information Assets Administrator must take necessary measures under the direction of the Information Security Chief Supervisor. Depending upon the impact of the incident, the Information Security Chief Supervisor may contact the relevant departments and submit a report to the Chief Information Security Officer.