National University Corporation Tokyo Institute of Technology
Information Security Policy

April 2005
Revised: September 2013, June 2021

Contents

1. Basic Principles of Information Security

Tokyo Institute of Technology (the “Institute”) aims to achieve a security level appropriate for the information infrastructure of a world-leading science and technology university, and also aims to ensure continuous and stable education, research, and management operations. For these principal aims, the Information Security Policy, which is a comprehensive regulation of the information security measures to be taken by the Institute members and related individuals, is established.

2. Purpose of the Information Security Policy

The purpose of this Information Security Policy is to:
1. Protect the information assets of the Institute
2. Prevent infringements on the information assets of the Institute or affiliated outside organizations

The users, temporary users, and subjects targeted by this policy are as follows.

Users, etc.
Users: Board members, staff, and students, etc. who use information assets with approval from the Institute
Temporary users: Individuals other than board members, staff, and students, etc. who are temporarily approved to use information assets

Subjects
Information system: A system that is related to information processing or an information network that falls under any of the following:
(1) A system that is owned or managed by the Institute
(2) A system that is provided to the Institute in accordance with a contract or agreement
(3) A device that is connected to an information network of the Institute
Information content: All information managed or used by the Institute; recorded on paper, electromagnetically, or in any other medium; and pertaining to education, research, or clerical work

Information assets: The combination of information systems and information content
Personal information: Information that can identify (or specify) a specific individual and all data associated with that information

3. Basic Principles of the Information Security Policy

3.1 Organizational structure

- Chief Information Security Officer
  The Chief Information Security Officer makes a comprehensive decision regarding information security at the Institute and has full authority over and responsibility for information security.

- Departmental Chief Information Security Officer
  The Departmental Chief Information Security Officer has full authority over and responsibility for departmental information security.

3.2 Establishment of the information security regulations and implementation procedures

The Chief Information Security Officer must separately establish the Information Security Regulations including organizational structure and implementation procedures.
The Departmental Chief Information Security Officer must establish information security implementation procedures that are tailored to the conditions of each department on the basis of risk analysis, etc. The procedures must be specific and also can be used as standard measures when individuals comply with the Information Security Regulations.
However, the Chief Information Security Officer must review the Information Security Regulations and implementation procedures, etc. regularly or when it is necessary, while cooperating with each department and comprehending risk to the Institute as a whole.

3.3 Rating and management of information content

Information content must be rated, and appropriate management methods for information content must be established.

3.4 Management of information systems

Management methods for information systems must be established.

3.5 Clarification of information security factors

The safety of Users, etc. and information assets of the Institute or organizations outside the Institute must be ensured against the following:

(1) The leaking or falsification of information content or personal information

(2) The destruction of information systems or the obstruction of the operation thereof

3.6 Personnel Security

Users, etc. must understand and take responsibility for the Information Security Policy, and actively play their roles.

All Users, etc. who use the information assets of the Institute must comply with the Information Security Regulations to prevent conduct that could threaten the information security of the Institute or organizations outside the Institute.

3.7 Measures against those who infringe the Information Security Policy

Punishments and usage restrictions on the information assets in cases where Users, etc. infringe the Information Security Policy and the Information Security Regulations, etc. can be stipulated in each policy and in regulations.