Kanazawa Institute of Technology School System
Information Security Policy (English translation)

Implemented April 1, 2005
Revised April 1, 2018

1. Guidelines

The educational foundation known as the Kanazawa Institute of Technology (hereinafter referred to as "KIT") has established a wide range of web systems, including educational and study support systems, via systemization and networking, for various operations related to education, research, and the administration of KIT and the International College of Technology, Kanazawa (ICT). As a result, ensuring the security of information used for education, research, and administrative operations has become an important issue in maintaining the sound management of KIT.

In addition, the exchange of information with researchers, educators, and other related parties both within the university and outside it via the campus network and the internet has come to require an international level of security and a high degree of network reliability. For these reasons, KIT has established this Information Security Policy to protect information assets and to ensure that information security is properly managed.

From among the eight principles of the OECD Privacy Guidelines adopted in 1980, this Security Policy shall be based upon the following: the "Data Quality Principle," which requires information to be accurate, complete, and up to date; the "Use Limitation Principle," which requires restrictions on the use of data for purposes other than those specified; and the "Security Safeguards Principle," which requires protections against risks such as loss, destruction, modification, and disclosure of information.

2. Scope and objectives of the security policy

The scope of this security policy shall apply to information assets related to education, research, and school management (hardware, software, data, information, networks and their related facilities, equipment, documents, storage media, etc.) owned by KIT, and to all of the following that handle such information assets:

(1) The KIT Board of Directors
(2) KIT faculty and staff
(3) KIT undergraduate students, graduate students, ICT students, research students, and auditing students
(4) Persons who conduct education and research jointly with the faculty and staff of KIT
(5) Persons deemed appropriate by the Chief Information Security Officer
(6) Part-time faculty and staff
(7) In addition to (1) through (6) above, temporary employees, contracted workers, and others who use KIT's information systems, regardless of their employment status, position, or work location.

3. Security policy management system

This Security Policy shall be established and operated under the supervision of the Chief Information Security Officer (hereinafter referred to as the "CISO").

In addition, an information security committee headed by the CISO (hereinafter referred to as the "Security Committee") may be established as necessary in accordance with changes in KIT's operating environment and its system usage environment, as well as with changes due to advances in information technology.

In the event a Security Committee is established, its members shall be as follows:

(1) Chief Information Security Officer (CISO)
(2) Personal Information Management Officer
(3) Information System Division Manager
(4) Information System Division Engineer
(5) Information Asset Manager Representative

4. Security management responsibility

(1) Responsibilities of Information Asset Manager

Each department shall appoint an Information Asset Manager to manage the information assets held by the department. The Information Asset Manager is responsible for continuously monitoring whether the information assets under his/her control are protected in accordance with the provisions of this security policy. If he/she finds any violations, he/she is obliged to make improvements and report them to the CISO.

(2) Responsibilities of information asset users

Users of information assets (hereinafter referred to as "users") shall have the obligation and responsibility to comply with this Security Policy in accordance with their affiliated departments and their authorization to use information assets related to their work.

5. Computer network usage rules

In order to guarantee authorized users access to the network and server computers and to ensure stable operations, KIT has established the following standards (norms) of behavior for users to observe.

In addition, users are responsible for their actions when using the network and are obliged to comply with information security laws and regulations.

(1) You must not fraudulently apply for a user ID or fraudulently use another person's user ID.
(2) You must not allow others to use your user ID.
(3) You must not interfere with the normal use of other users by consuming a disproportionate amount of system resources or causing inconvenience or damage to other users by any action that interferes with the normal operations of the computer systems. (The sending of unsolicited spam email or chain letters is prohibited. Also, the intentional act of disrupting the computer systems or introducing malware is prohibited.)
(4) Commercial use, whether for-profit or nonprofit, is prohibited.

(5) You may not invade the privacy of others or slander others.
(6) Harassment, acts against public order and morals, and other threatening behaviors are prohibited.
(7) You must not infringe on copyrighted material, using it without the permission or proper license of the copyright holder.

In addition, the following compliance rules have been established to ensure the safety of the campus network and information systems.
(1) The campus network must not be used for any purpose other than education, research, and the administration of the school in which it is established.
(2) Anyone who wishes to connect a computer or network device to the campus network must follow the necessary network connection procedures.
(3) Anyone who wishes to connect a computer to the campus network must take measures to prevent viruses from infecting his/her device.
(4) If a computer is infected with a virus, or is suspected of being infected, the computer must be immediately disconnected from the network to prevent the virus from spreading.

The following measures shall be taken to ensure the safety of the campus network and web systems.
(1) In order to protect the campus network from malicious attacks and viruses, packet filtering by firewalls and virus detection by email servers shall be performed at network entry and exit points.
(2) When accessing important information such as personal information, measures such as authentication, access control, and encryption shall be taken at the time of information registration and retrieval to establish safety and reliability.

6. General compliance

In order to protect the information assets of KIT, users must comply with the following:
(1) Restrictions on taking items off campus

For the purposes of preventing data leakage and data falsification, computer equipment and storage media on which information assets are stored must not be taken off campus.
(2) Restrictions on the reproduction of information assets

Based on the Data Quality Principle, which requires information to be accurate, complete, and up to date, data from the server system containing information assets managed by the Information System Division shall not be duplicated. If duplication is unavoidable due to the necessity of business operations, prior approval from the CISO is required.
(3) Confidentiality

It is prohibited to disclose, provide, or leak to any third party any information or technology obtained in the course of performing one's duties, except in cases where it is deemed necessary to give priority to the public interest, or where it is deemed necessary for the performance of those duties.

When handling information related to personal privacy, care must be taken to protect it, and measures must be taken to prevent any accidents from occurring.

(4) Protection of intellectual property rights

The intellectual property rights held by KIT shall be protected, and the intellectual property rights held by third parties shall not be infringed upon.

(5) Obligation to report accidents and failures

When an accident or failure is discovered or is predicted to occur, it must be promptly reported to the Information Asset Manager of each department involved and action must be taken to minimize the damage.

(6) Security management when outsourcing

When outsourcing work related to information assets, measures must be taken to prevent information assets from being leaked to outside parties, such as clearly specifying in the contract with the outsourcing contractor the items for which responsibility is to be assigned in the event of a problem, as well as actions to be taken if the information security policy of KIT is breached.

(7) Obligation to comply with information-security–related laws and regulations

The users must comply with the Act on the Protection of Personal Information, the Act on the Prohibition of Unauthorized Computer Access, the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers, and the Act on Disclosure of Identification Information of the Senders (commonly called the Provider Liability Act), the Electronic Signature Certification Act, the Electronic Bookkeeping Act, copyright law, criminal law, and information-security–related laws to be established in the future.

7. Prohibited acts related to information security

The following acts that threaten information security must not be performed under any circumstances. In addition, users should be aware that there are persons who maliciously commit these acts and should take sufficient precautions against them, such as preventive measures to avoid being victimized.

(1) Unauthorized access

Unauthorized access to network servers or information systems by using another person's user ID and password without the permission of the rightful owner to wiretap, steal, leak, falsify, destroy, or erase information.

(2) Unauthorized infiltration

Exploiting security holes (system flaws) or inappropriate server settings to gain administrative privileges and gain unauthorized access to the system to rewrite web pages, leak information, falsify data, or destroy data.

(3) Unauthorized attacks

A port attack by a person with malicious intent that interferes with the operation of a network or information system, resulting in an abnormal outage.

(4) Transmission of spam email

Sending a large amount of unwanted email to those who do not want to receive it, causing confusion.

(5) Sending mail bombs

Sending large volumes of email or large attachments to specific email servers or individuals, causing confusion or disrupting operations.

(6) Spoofing

Using another person's user ID and password to obtain services from network servers or information systems in place of the rightful owner, or to steal, leak, or falsify information.

(7) Wiretapping

Eavesdropping on password information, email content, and other information flowing over the network resulting in information theft and/or leakage.

(8) Theft

Theft or leakage of information from stolen or misplaced computers or storage media.

(9) DoS (Denial of Service) attacks

Intentionally sending large numbers of packets to temporarily or permanently disable certain services, computers, or networks.

(10) Distribution of computer viruses

The act of destroying or erasing data or causing malfunction by widely distributing a malicious program, the spread of which can cause damage to many computers.

(11) Others

Leakage or theft of confidential information due to lack of ethical and moral standards, sending spam email or making inappropriate/offensive posts on message boards, violation of copyrights or portrait rights, violation of human rights, invasion of privacy, etc.

8. Obligation to report accidents

Even with appropriate information security management based on this security policy, exposure to various types of attacks, unforeseen accidents, or outages may occur. In the event of such a contingency, the CISO shall be notified promptly.

9. Compliance obligations and penalties

This Security Policy obliges all users specified in the scope of the application to comply with it. In addition, penalties may be imposed on violators of this Security Policy.

Furthermore, if a user subject to the security policy is found to have committed an act that seriously affects the information security system of KIT, an act that constitutes a violation of personal privacy, or a malicious act that causes loss of assets, the user may be subject to disciplinary action in accordance with employment regulations, university rules and other relevant policies.

In cases where the loss of public confidence is inevitable due to unforeseen circumstances, the CISO, at his/her discretion, is not precluded from taking exceptional measures until other remediation can be enacted.

10. Relationship to other regulations and policies

The National Institute of Informatics's "Rules on the use of SINET (Science Information NETwork)" shall be given precedence to any and all sections related to the academic information network.

11. Disclosure of security policy

KIT will disclose this security policy through its website in order to make it known to all persons who use KIT's information assets.

12. Effective period

1. These policies were established on March 22, 2005 and take effect as of April 1, 2005.
2. These policies were revised and re-implemented as of April 1, 2018.

Note: The original Japanese version of this Information Security Policy is the binding policy and retains precedence over this English translation.