Tokai National Higher Education and Research System Information Security Measures Basic Rules

(THERS Rule No. 14 of June 19, 2024)

Table of Contents

Chapter 1. General Provisions

(Purpose)

Article 1. These Rules stipulate basic Information Security measures pertaining to information and Information Systems at the Tokai National Higher Education and Research System (hereinafter referred to as "THERS") and serve to ensure the protection and proper utilization of information held by THERS and the maintenance and improvement of Information Security standards.

(Definition)

Article 2. In these Rules, the meanings of the terms set forth in the following items are as follows:

(i) Information System(s): A system consisting of hardware and software used for information processing or communications, procured or developed by THERS (including systems whose management is entrusted by THERS to other parties);

(ii) Information Security: Maintaining the confidentiality, integrity, and availability of information;

(iii) Employees: Officers and employees of THERS;

(iv) External Electromagnetic Recording Medium: Recording media related to electromagnetic records external to an Information System (records made in electronic, magnetic, or other formats that are imperceptible to human senses and are used for information processing by an electronic computer);

(v) Information Security Incident(s): An accident or incident (including cases where there is a suspicion or possibility of such an incident) that occurs intentionally or accidentally and violates THERS rules, etc. or laws regarding Information Security;

(vi) Users: Employees and Students (meaning students of the national university (hereinafter referred to as "University") students and their affiliated school students and pupils organized under THERS; the same applies in the following item) who use THERS information and Information Systems with the necessary permission;
(vii) Temporary Users: Persons other than Employees and Students who use THERS information and Information Systems with the necessary permission; and
(viii) Policy: The Tokai National Higher Education and Research System's Basic Policy on Information Security Measures (approved by the Executive Board on June 19, 2024) and these Rules.

(Scope of Applicability)
Article 3 (1) These Rules apply to all persons who operate, manage or use THERS information and Information Systems.
(2) The types of information to which these Rules apply are as described in the following items.
(i) Information recorded in an Information System or External Electromagnetic Recording Medium to be used in the course of their duties by Employees (including information written in documents output from the Information System or External Electromagnetic Recording Medium and information input from documents to the Information System or External Electromagnetic Recording Medium).
(ii) Information recorded in an Information System or External Electromagnetic Recording Medium (including information written on documents output from an Information System or External Electromagnetic Recording Medium and information input from documents into the Information System or External Electromagnetic Recording Medium, and excluding information as described in the preceding item) that is handled by Employees in the course of their duties.
(iii) In addition to the types of information described in the preceding two items, information concerning the design or operation management of Information Systems procured or developed by THERS.
(3) The Information Systems to which these Rules apply are all Information Systems which handle information listed in the items of the preceding paragraph.

Chapter 2. Information Security Management System
(Chief Information Security Officer)
Article 4 (1) A Chief Information Security Officer (hereinafter referred to as "CISO") shall be appointed to bear responsibility for the appropriate management of information and THERS Information Security measures, and the Executive Director of Administration shall serve in this role.
(2) The CISO shall be responsible for the following tasks:

(i) Establishment of an organization and system for promoting Information Security measures.
(ii) Determination and review of standards for Information Security measures.
(iii) Determination and review of plans related to Information Security measures
(iv) Issuance of instructions and execution of other necessary measures in the event of an Information Security Incident.
(v) Other tasks related to Information Security measures.

(Vice Chief Information Security Officer)
Article 5 (1) Under the CISO, a Vice Chief Information Security Officer (hereinafter referred to as the "Vice CISO") shall be appointed, and the Director of Administration shall serve in this role.
(2) The Vice CISO shall assist the CISO and, if the CISO is incapacitated, the Vice CISO shall perform the duties of the CISO.

(Establishment of a Computer Security Incident Response Team)
Article 6 (1) In order to respond to Information Security Incidents that occur within THERS, a Computer Security Incident Response Team (hereinafter referred to as "CSIRT") shall be established.
(2) As the reporting desk for Information Security Incidents within THERS, CSIRT shall receive information about Information Security Incidents that occur within THERS, and shall endeavor to accurately understand the nature of Information Security Incidents by utilizing information obtained via monitoring of the THERS information network.
(3) In the event of an Information Security Incident, CSIRT will, as necessary, provide technical support and advice pertaining to damage containment and recovery, and the prevention of recurrence.
(4) The CISO shall make necessary budgetary arrangements, delegations of authority, etc. to create an environment conducive to the smooth operation of CSIRT.
(5) The Gifu University CISO and the Nagoya University CISO shall, in cooperation with CSIRT, develop necessary systems for communication, reporting, information collection, and emergency response for damage containment in the event of an Information Security Incident.
(6) Necessary matters concerning CSIRT shall be prescribed separately.

(Appointment of Information Security Advisors)
Article 7 (1) THERS may appoint individuals with specialized knowledge and experience in Information Security as Information Security advisors.
(2) The Information Security Advisors shall provide instruction and advice regarding THERS Information Security measures.

(Information Security Audit Officer)
Article 8 (1) THERS shall appoint an Information Security Audit Officer, and the Audit Office Director shall serve in this capacity.
(2) The Information Security Audit Officer shall conduct audits related to Information Security.

(Prohibition of holding concurrent positions)
Article 9 (1) When implementing Information Security measures, a person who seeks approval or permission cannot also be the person who provides that approval or permission.
(2) The subject of an Information Security audit cannot also serve as the person conducting the audit.

(Information & Communications Council)
Article 10 Matters relating to Information Security measures shall be discussed at the THERS Information & Communications Council (hereinafter referred to as the “Information & Communications Council").

Chapter 3. Restrictions of Use pertaining to Information Security
(Responsibilities of Users, etc.)
Article 11 (1) Users and Temporary Users must endeavor to ensure and improve the level of Information Security.
(2) The standards for achieving the provisions of the preceding paragraph shall be prescribed separately.

(Prevention of actions that could lead to a decline in Information Security standards outside THERS)
Article 12 The CISO shall take measures to prevent any actions that could lead to a decline in Information Security standards outside of THERS.

(Restriction of Use)
Article 13 The CISO may impose restrictions on the operation and use of THERS information and Information Systems, or take other necessary measures against anyone who violates the Policy or other rules related to Information Security (hereinafter referred to as the "Policy, etc.").

(Outsourcing of Operations)
Article 14 When the CISO outsources all or part of the operations related to THERS information and Information Systems, the CISO must endeavor to thoroughly protect Information Security, such as by clarifying the responsibility management system, etc. of the outsourcee in the contract.

(Accessing communication details)
Article 15 The CISO may, to the extent necessary for the protection of THERS Information Security, access communication details on THERS communications infrastructure, and may entrust the access of communication details to an institution other than THERS.

(Exceptional Measures)
Article 16 (1) If the application of the Policies, etc. significantly impedes the proper execution of duties at THERS, the CISO may take measures necessary for the execution of duties (hereinafter referred to as "Exceptional Measures") notwithstanding the provisions of the Policies, etc.
(2) Necessary matters concerning Exceptional Measures shall be prescribed separately.

Chapter 4. Information Rating
(Information Rating, etc.)
Article 17 (1) The CISO shall develop standards for classification and handling restrictions of information held by THERS in accordance with confidentiality, integrity, and availability.
(2) Necessary matters concerning the classification and handling restrictions of information within THERS shall be prescribed separately.

Chapter 5. Responding to a State of Emergency
(Information Security Incident)
Article 18 Necessary matters concerning responses in the event of an Information Security Incident shall be prescribed separately.

(Restrictions on the use of information and Information Systems)
Article 19 (1) If an Information Security Incident occurs or if the CISO or Vice CISO deems it necessary, they may restrict the use of information and the Information System in order to prevent the occurrence of an Information Security Incident..
(2) The CISO shall take necessary measures, such as suspending the use of information and the information System, if any Users or Temporary Users fall under any of the following items:
(i) If they do not follow specific orders or warnings from the CISO;
(ii) If they repeatedly engage in acts that are deemed to lower THERS Information Security standards; and
(iii) If they fail to take measures necessary to maintain Information Security.

Chapter 6. Education and Training

(Education and Training)

Article 20 Each fiscal year, the CISO must formulate a plan to conduct education and training aimed at ensuring and improving Information Security standards at THERS and take the necessary measures to implement that plan.

Chapter 7. Inspections and Evaluations

(Audits)

Article 21 In order to ascertain whether Information Security is being maintained, the Information Security Audit Officer shall conduct audits to check the status of Information Security in THERS on a regular and ad-hoc basis and report the audit results to the CISO.

(Inspections and Evaluations)

Article 22 (1) The CISO shall inspect or evaluate the status of Exceptional Measures, audit results, the occurrence of Information Security Incidents, etc.

(2) Based on the inspection or evaluation under the preceding paragraph, the CISO shall consider whether there is need to revise the Policy, etc. and present their opinion to the Information & Communications Council at least once each year.

Chapter 8. Miscellaneous Provisions

(Miscellaneous Provisions)

Article 23 (1) In addition to what is prescribed in these Rules, necessary matters concerning Information Security measures at THERS shall be prescribed separately.

(2) Information Security measures at the University shall be governed by the Policy and other rules set forth by the University.

(Supplementary Provisions)

These Rules shall come into effect on June 19, 2024.