Kyushu University Rules on Information Security Measures

Kyushu University Rule No. 119 of 2023

Effective date: March 29, 2024

The Kyushu University Rules on Information Security Measures (Kyushu University Rule No. 105 of 2022) are hereby amended in their entirety.

(Purpose)

Article 1 These Rules shall provide for the necessary matters relevant to the basic security measures concerning the information assets (hereinafter referred to as the “information security measures”) of National University Corporation Kyushu University (hereinafter referred to as the “University”).

(Scope of Application)

Article 2 These Rules apply to all persons who operate, manage, or use the University’s information assets.

(Definitions)

Article 3 In these Rules, the terms listed in each of the following items have the meanings provided in the respective items.

(i) "Information systems" refers to systems (including those provided by means of cloud services) related to information processing and information networks (as defined in the following item; the same applies hereinafter) that fall under any of the following categories:

(a) Those owned or managed by the University

(b) Those provided through contracts or agreements with the University

(c) Those connected to the University’s information networks

(ii) "Information networks" refers to those composed of information equipment and software (including that provided by means of cloud services) that fall under any of the following categories:

(a) All information equipment and software owned or managed by the University

(b) All information equipment and software provided through contracts or agreements with the University

(c) Information equipment and software owned by employees, etc. (as defined in item (iv)) and students, etc. (as defined in item (v)) of the University that are required for education and research

(iii) "Information assets" refers to those as defined in Article 2 of the Kyushu University Information Ethics Rules (Kyushu University Rule No. 73 of 2012).

(iv) "Employees, etc." refers to officers, employees (including those working at the University under dispatch contracts), and researchers of the University, along with other individuals approved by Information Security Officers (as defined in Article 7; the same applies in the

following item).

(v) "Students, etc." refers to undergraduate students, graduate students, credited auditors, auditors, special auditors, research students, special students, special research students, and others approved by Information Security Officers.

(vi) "CIO" refers to the Executive Vice President designated by the President pursuant to Article 2, paragraph (1) of the Kyushu University Chief Information Officer Rules (Kyushu University Rule No. 121 of 2023).

(vii) "Departmental Information System Administrator" refers to the person who operates and manages the departmental information system built by each school, institute or faculty.

(viii) "Departmental information system users" refers to the employees, etc. and students, etc. who use the information systems built by schools, institutes and faculties.

(ix) "Information security" refers to maintaining the confidentiality, integrity, and availability of information assets.

(x) "Electromagnetic records" refers to any record which is produced by electronic, magnetic, or any other means unrecognizable by natural perceptive functions and is used for data-processing by a computer.

(xi) "Incident" refers to accidents or events related to information security that violate relevant laws and regulations and the University's regulations, etc., whether intentionally or accidentally.

(xii) "Schools, institutes and faculties" refers to the organizations provided in Article 3 through Article 17-2 of the Regulations of Kyushu University (Kyushu University Regulation No. 1 of 2004).

(Chief Information Security Officer)

Article 4 (1) A Chief Information Security Officer (hereinafter referred to as the “CISO”) is appointed by the CIO from among the University’s employees, etc. to hold overall authority and responsibility for information security at the University.

(2) Under the direction of the CIO, the CISO implements strategies and measures related to information security, and deal with information-related laws and regulations, and reports the results to the CIO.

(3) The CISO may appoint an expert with specialist knowledge and experience of information security to serve as an Information Security Advisor.

(Deputy Chief Information Security Officer)

Article 5 (1) A Deputy Chief Information Security Officer (hereinafter referred to as the “Deputy CISO”) is appointed or commissioned by the CISO.

(2) The Deputy CISO performs the duties of the CISO in the event that the latter is incapacitated.

(Assistant Chief Information Security Officer)

Article 6 An Assistant Chief Information Security Officer (hereinafter referred to as the "Assistant CISO") is appointed or commissioned by the CISO to assist the Deputy CISO.

(Information Security Officers)

Article 7 (1) The director, etc. of each school, institute or faculty serves as its Information Security Officer.

(2) Information Security Officers determine operational policies and implement measures to address information system problems and the like within the school, institute or faculty.

(3) Information Security Officers shall report to the CISO any procedure manuals and the like instituted in the school, institute or faculty.

(Departmental Information System Administrators)

Article 8 (1) Departmental Information System Administrators are responsible for the departmental information systems that they operate and manage, and bear responsibility for maintaining information security within those systems.

(2) If issues or problems related to the Departmental information system's information security measures come to light, the Departmental Information System Administrator must identify the issues to be resolved and take appropriate measures.

(3) Departmental Information System Administrators must comply when their cooperation in the maintenance and management of information security is requested by Kyudai Computer Security Incident Response Team (Kyudai CSIRT), an Information Security Officer, or a Branch LAN Manager (as defined in Article 8 of the Kyushu University Integrated Information Transmission Environment Operating Regulations (Kyushu University Regulation No. 61 of 2004)).

(Committee)

Article 9 (1) Deliberations on information security measures at the University are conducted by the Information Policy Committee (hereinafter referred to as the "Committee").

(2) The Committee deliberates on the following matters concerning the security of information systems as provided in Article 2, paragraph (4) of the Kyushu University Information Policy Committee Rules (Kyushu University Rule No. 104 of 2022).

(i) Matters concerning the establishment, amendment, and abolition of regulations related to information security.

(ii) Matters concerning measures for maintaining and improving information security.

(iii) Other important matters concerning information security.

(Departmental Information System Management Committee)

Article 10 (1) Each school, institute or faculty has in place a Departmental Information System Management Committee.

(2) The director, etc. of each school, institute or faculty serves as chair of its Departmental

Information System Management Committee.

(3) The Departmental Information System Management Committee may be substituted by another deliberative body in which the director, etc. participates. In such cases, the Information Security Officer shall report the name, etc. of the Departmental Information System Management Committee to the CISO.

(4) The Departmental Information System Management Committee deliberates and implements matters concerning information security in the school, institute or faculty.

(Compliance with the Security Policy, etc.)

Article 11 (1) Employees, etc. and students, etc. must maintain the University's information security by complying with relevant laws and regulations concerning information security, the Kyushu University Information Security Policy (hereinafter referred to as the "Security Policy"), and these Rules, etc.

(2) Departmental information system users must not engage in actions that risk lowering the University's level of information security.

(3) Departmental information system users must comply when their cooperation in the maintenance and management of information security is requested by the Departmental Information System Administrator.

(4) Schools, institutes and faculties accepting dispatched workers under outsourcing contracts with external contractors must ensure that workers understand and comply with the Security Policy by which they should abide, along with the content of these Rules.

(5) When outsourcing information system development and maintenance duties to external contractors, contracts must stipulate the Security Policy and the parts of these Rules with which those contractors and any subcontractors should comply.

(Education and Training)

Article 12 (1) The CISO conducts training for Information Security Officers, Branch LAN Managers, and Departmental Information System Administrators to enable them to acquire the necessary skills.

(2) The CISO supports training on the Security Policy, etc. carried out for employees, etc. within each school, institute and faculty as needed. In addition, the CISO cooperates with orientations or lectures concerning the Security Policy, etc. for students, etc. when requested by employees, etc.

(3) Employees, etc. and students, etc. must strive to gain an understanding of the Security Policy and these Rules, etc. by attending workshops, briefings, orientations, or lectures.

(Self-Assessment of Information Security)

Article 13 (1) Self-assessments of information security are conducted to verify compliance with the Security Policy and these Rules, etc., make improvements as needed, and raise awareness

among employees, etc. and students, etc.

(2) The self-assessments specified in the preceding paragraph are prescribed separately by the CISO after discussion by the Committee.

(Information Security Audits)

Article 14 (1) An Information Security Audit Officer is appointed by the CISO to hold responsibility for matters related to audits of information security at the University.

(2) The Information Security Audit Officer conducts information security audits to verify the validity of procedures based on the Security Policy and these Rules, etc., confirm operational compliance, and improve information security measures.

(3) The audits specified in the preceding paragraph are prescribed separately by the CISO after discussion by the Committee.

(Management and Operation)

Article 15 Information security measures shall be managed and operated by each school, institute and faculty in accordance with the Security Policy and these Rules, etc.

(Kyudai CSIRT)

Article 16 (1) Kyudai Computer Security Incident Response Team (Kyudai CSIRT) is established under the CISO as an organization working to maintain and strengthen the security of Kyushu University's cyberspace through emergency response to any information security incidents at the University, investigation and response measures afterwards, daily monitoring of the status of information security, and the prevention of incidents.

(2) The requisite matters relating to the organization and operation of Kyudai CSIRT are prescribed separately by the CISO after discussion by the Committee.

(Formulation and Review of the Basic Plan for Information Security Measures)

Article 17 (1) Following deliberation by the Committee, the CISO establishes a Basic Plan for Information Security Measures to comprehensively promote information security measures.

(2) The CISO comprehensively evaluates the implementation of information security measures, along with the results of self-assessments and audits, and, following deliberation by the Committee, periodically reviews the Basic Plan for Information Security Measures, taking into account any significant changes in information security.

(3) The CISO may have in place a Basic Plan for Information Security Measures Office to serve as an organization engaged in formulating and reviewing the Basic Plan for Information Security Measures, and ensuring information security based on the plan.

(Updating of Information Security Regulations, etc.)

Article 18 After discussion by the Committee, the CISO shall update the Security Policy and these Rules, etc. to take account of any significant changes in information security, and shall also take any other information security measures required.

(Classification of Information)

Article 19 (1) Employees, etc. shall classify information handled in the course of their duties in accordance with the following classification levels and criteria:

(i) Classification levels and criteria relating to confidentiality

Classification Level	Classification Criteria
Confidentiality Level 3 Information	Information handled in the course of duties at the University that needs to be handled as confidential documents, as provided in Article 27 of the Kyushu University Corporate Document Management Rules (Kyushu University Rule No. 97 of 2023).
Confidentiality Level 2 Information	Information handled in the course of duties at the University that is deemed highly likely to fall into the category of non-disclosure information as listed in the items of Article 5 of the Act on Access to Information Held by Incorporated Administrative Agencies (Act No. 140 of December 5, 2001; hereinafter referred to as the "Information Disclosure Act"), excluding Confidentiality Level 3 Information.
Confidentiality Level 1 Information	Information handled in the course of duties at the University that is not deemed highly likely to fall into the category of non-disclosure information as listed in the items of Article 5 of the Information Disclosure Act.

(ii) Classification levels and criteria relating to integrity

Classification Level	Classification Criteria
Integrity Level 2 Information	Information (excluding paper documents) where falsification, errors, or damage risks violating the rights of the University's stakeholders or being impediment to the proper conduct of the University's operations (excluding minor cases).
Integrity Level 1 Information	Information other than Integrity Level 2 Information (excluding paper documents).

(iii) Classification levels and criteria relating to availability

Classification Level	Classification Criteria
Availability Level 2 Information	Information (excluding paper documents) where destruction, loss, or unusability of the information in question risks violating the rights of the University's stakeholders or being impediment to the stable conduct of the University's operations (excluding minor cases).
Availability Level 1	Information other than Availability Level 2 Information (excluding

Information	paper documents).

(2) Of the classification levels specified in item (i) of the preceding paragraph, Confidentiality Level 3 and Level 2 Information are referred to as information requiring confidentiality.

(3) Of the classification levels specified in paragraph (1), item (ii), Integrity Level 2 Information is referred to as information requiring preservation.

(4) Of the classification levels specified in paragraph (1), item (iii), Availability Level 2 Information is referred to as information requiring stability.

(Indication of Information Classifications and Handling Restrictions)

Article 20 Employees, etc. shall specify information classifications and handling restrictions and, as a general rule, indicate them in a recognizable way.

(Compliance with Handling Restrictions)

Article 21 In handling information, employees, etc. must comply with the information handling restrictions specified in accordance with the preceding Article and the guidelines based thereon prescribed separately by the CISO (hereinafter referred to as the "Information Classification Guidelines").

(Exceptions to Information Classification and Handling Restrictions)

Article 22 (1) In the case of information held by the University where it is found that the application of Articles 19 and 20 would seriously impede the conduct of duties, and where relevant laws and regulations, etc. and the University's regulations, etc. contain provisions regarding the handling of information, the information in question may be handled in accordance with the relevant laws and regulations, etc.

(2) Information that meets the requirements of the preceding paragraph is prescribed separately in the Information Classification Guidelines.

(Penalties)

Article 23 The CISO shall take the requisite measures, such as suspending use of information systems, in the event that a person specified in Article 2 falls under any of the following:

(i) Failure to comply with specific orders or warnings from the CISO

(ii) Repeated actions recognized as reducing the University's level of information security

(iii) Negligence in taking the measures required to maintain the University's information security

(Miscellaneous Provisions)

Article 24 Beyond what is provided in these Rules, the requisite matters relating to the technical handling of information security measures are prescribed separately by the CISO, following discussion by the Committee.

Supplementary Provisions

These Rules come into effect as of April 1, 2024.

Supplementary Provisions（Kyushu University Rule No. 75 of 2024）
These Rules come into effect as of April 1, 2025.