お国立研究開発法人 理化学研究所
情報セキュリティ対策規程
（平成３０年９月１３日規程第６９号）
改正　令和２年３月１１日規程第２４６号
改正　令和３年３月２４日規程第３８０号
改正　令和３年３月２９日規程第３９９号
改正　令和４年３月２４日規程第５０７号

RIKEN
Regulations for Information Security

Joho security taisaku kitei

September 13, 2018, Reg. No 69

With revisions effective April 1, 2022

This is an English translation of the regulations written in Japanese and is for information purposes only.

Table of contents

Chapter 1 **General Provisions** (Articles 1 - 3)

Chapter 2 **Organization Structure** (Articles 4 - 17)

Chapter 3 **Information Security Committee** (Articles 18 - 24)

Chapter 4 **Information Security Subcommittee** (Articles 25 - 32)

Chapter 5 **Use of Information, Information Systems, and the RIKEN Network** (Articles 33, 34)

Chapter 6 **Management of Information and Information Systems** (Articles 35 - 40)

Chapter 7 **Emergency Response** (Articles 41 - 43)

Chapter 8 **Operation of Information Security** (Articles 44 - 51)

Supplementary Provisions

Chapter 1. General Provisions

Article 1 Objective

1. The purpose of these Regulations is to protect and utilize information assets by defining the basic principles for cybersecurity measures at National Research and Development Agency RIKEN (hereinafter “RIKEN”). The regulations are based on “Common Model of Information Security Measures for Government Agencies and Related Agencies” (decided by Cybersecurity Strategic

Headquarters on August 31, 2016).

2. In addition to those stipulated herein, matters necessary for implementing these Regulations will be provided in the "Standards for Information Security" and the "Implementation Procedures for Information Security" set by the Information Security Committee (hereinafter "the Committee") based on the information security policies.

Article 2 Definitions of terms

Key terms in this document are defined as follows.

(1) Information security policies: the Basic Policy for Information Security and these Regulations for Information Security (hereinafter "the Regulations") at RIKEN

(2) Information security standards: the Standards for Information Security and the Implementation Procedures for Information Security set forth by the Committee

(3) Division: an organizational group in charge of information security measures that are stipulated separately

(4) Section: section/laboratory/unit or equivalent: the smallest organizational unit concerned with the information security measures. Set up by each division

(5) Employees: directors and employees engaged in RIKEN activities (all personnel directly employed by RIKEN)

(6) External personnel: personnel other than employees

(7) Users: employees and external personnel who use Information as defined in the next item, the information systems defined in item (10), and the RIKEN network defined in item (13)

(8) Information: the information that is generated, collected, and obtained through RIKEN activities

(9) Information service: the processing, storage, and transfer of information, and its provision to users

(10) Information systems: systems, hardware, and software that provide information services for RIKEN activities

(11) External information systems: information systems such as PCs, servers, cell phones, tablet devices, and USB memory devices that are not RIKEN assets.

(12) Network: hardware (such as cables, routers, and switches) and software (such as IP addresses, protocols, and programs) used to connect and coordinate operations of multiple information systems

(13) RIKEN network: a network that is used to connect, control, and operate information systems for RIKEN activities

(14) Information security: to soundly maintain the following characteristics, which are essential attributes of information, information systems, and the RIKEN network

a) Confidentiality: the state of affairs in which only permitted persons can access information

b) Integrity: accurate and complete processing

c) Availability: the state of affairs in which permitted persons can access information and related assets without interruption when they are needed

(15) Information security incident: damage to information, information systems and the RIKEN network through outflow, leakage, falsification, destruction, or disabling of information

(16) External service: provision of part or all of the functions of an information system to the public by a person outside RIKEN, provided that said functions handle the information of RIKEN.

(17) Outsourcing: having an external party perform part or all of the business of RIKEN under a contract, provided that the party handles the information of RIKEN in the course of conducting the said business. "Outsourcing" shall include all types of contracts, such as "delegation," "quasi-delegation," and "contracting."

Article 3 Scope of these Regulations

1. The personnel to whom these Regulations apply are users stipulated in the preceding Article, item (7).
2. The information to which these Regulations apply is the information stipulated in the preceding Article, item (8).
3. The information systems to which these Regulations apply are the information systems stipulated in the preceding Article, item (10).
4. The network to which these Regulations apply is the RIKEN network stipulated in the preceding Article, item (13).

Chapter 2. Organization Structure

Article 4 Chief Information Security Officer

1. RIKEN shall designate a Chief Information Security Officer (hereinafter “the CISO”).
2. The CISO shall be appointed by the President.
3. The CISO organizes information security measures at RIKEN.
4. The CISO must formulate a Promotion Plan of Measures for Information Security (hereinafter “the Promotion Plan”) to promote general measures for information security at RIKEN.
5. The CISO shall conduct information security measures based on the Promotion Plan.
6. The CISO shall stipulate the divisions to act as management units related to information security measures.

Article 5 Deputy Chief Information Security Officer

1. RIKEN shall designate a Deputy Chief Information Security Officer (hereinafter “the Deputy CISO”).

2. The Deputy CISO shall be appointed by the CISO.
3. The Deputy CISO assists the CISO and acts on the CISO's behalf in case of accidents or the like.

Article 6 Assistant Chief Information Security Officer

1. RIKEN shall designate an assistant Chief Information Security Officer (hereinafter "the assistant CISO") who has expertise in information security.
2. The assistant CISO shall be appointed by the CISO.
3. The assistant CISO assists the CISO and performs part of the CISO's duties as instructed by the CISO.

Article 7 Information Security Advisor

1. RIKEN shall designate an Information Security Advisor who has expertise in information security.
2. The Information Security Advisor shall be appointed or commissioned by the CISO.
3. The Information Security Advisor provides advice to the CISO on information security measures.

Article 8 Chief Information Security Auditor

1. RIKEN shall designate a Chief Information Security Auditor.
2. The Chief Information Security Auditor shall be designated by the CISO.
3. The Chief Information Security Auditor conducts audits for information security measures at RIKEN and provides the CISO with audit reports.

Article 9 Section in charge of general information security

1. RIKEN shall establish a section in charge of general information security.
2. The section in charge of general information security shall be the Information Security and User Support Section, Information Systems Division.
3. The section in charge of general information security conducts duties related to information security measures at RIKEN, and each branch's Information Systems Office shall support its duties.

Article 10 Computer Security Incident Response Team

1. RIKEN shall set up a Computer Security Incident Response Team (herein after "the CSIRT").
2. The organization, etc., of the CSIRT will be stipulated separately.
3. The CSIRT shall carry out the CISO's duties in emergencies, such as suspending the use of the

information, information systems, and the RIKEN network; and requesting the disclosure of necessary information or cooperation with requests, etc.

4. The CSIRT shall respond to detected or expected information security incidents.
5. Users must cooperate with the CSIRT in responding to information security incidents.

Article 11 Division Information Security Officer

1. A Division Information Security Officers shall be designated in each division.
2. Division Information Security Officers shall be appointed by the CISO.
3. Division Information Security Officers shall supervise tasks related to information security measures in the division under their jurisdiction.
4. Division Information Security Officers shall prepare a contact list of the Information Security Officers, Information Security Staff, and Information System Administrators in the division under their jurisdiction. and report it to the CISO.

Article 12 Division Information Security Staff

1. Division Information Security Staff shall be designated in each division.
2. Division Information Security Staff shall be appointed by the Division Information Security Officer after consultation with the CISO.
3. The Division Information Security Staff assists the Division Information Security Officer.

Article 13 Information Security Officer

1. An Information Security Officer shall be designated in each laboratory, section, office, or equivalent.
2. The Information Security Officer is the leader of each laboratory, section, office, or equivalent.
3. The Information Security Officer supervises tasks relating to information security measures in the laboratory, section, office, or equivalent under their jurisdiction.
4. The Information Security Officer must report to the Division Information Security Officer when the Information Security Staff or the Information System Administrator has been appointed or changed.

Article 14 Information Security Staff

1. An Information Security Staff may be designated in each laboratory, section, office, or equivalent.
2. The Information Security Staff shall be designated by the Information Security Officer.
3. The Information Security Staff assists the Information Security Officer.

Article 15 Information System Administrator

1. Information System Administrators shall be designated for each information system that provides information services to users, and for each external service under their jurisdiction.
2. Information System Administrators shall be appointed by the Information Security Officer.
3. Information System Administrators shall take information security measures for the information systems and external services under their jurisdiction.

Article 16 Area Information Security Officer

1. Area Information Security Officers shall be appointed corresponding to the scope of facilities where information security measures are required (hereinafter referred to as the "Management Areas") such as offices and server rooms.
2. Area Information Security Officers shall supervise operations concerning information security measures in the Management Areas under their jurisdiction.
3. Area Information Security Officers shall be appointed without fail, even if a Management Area is used by multiple laboratory, sections, offices, or equivalent. Such Area Information Security Officers shall be designated by the Branch Director.
4. When a Management Area is used by a single laboratory, section, office, or equivalent, the Information Security Officer of the concerned laboratory, section, office, or equivalent shall act as the Area Information Security Officer.

Article 17 Appropriateness of approval, authorization, and audit

1. RIKEN employees shall not concurrently undertake the following roles when implementing information security measures.
   (1) An applicant for an approval or authorization (hereinafter "approval, etc.") and an approver of the application (hereinafter "the approval authority, etc.")
   (2) An auditee and an auditor
2. If the approval authority is not qualified to approve/deny applications, employees may apply for approval with the approval authority's supervisor, or another appropriate person, in order to get an approval.

Chapter 3. Information Security Committee

Article 18 Establishment of the Committee

RIKEN shall establish an Information Security Committee.

Article 19 Responsibilities

The Committee shall deliberate the following matters.

(1) Important matters regarding information security at RIKEN

(2) Other matters if the Committee deems it necessary

Article 20 Chair and Deputy Chair of the Committee

1. The CISO shall serve as Chair of the Committee.
2. The Chair shall represent the Committee and preside over the work of the Committee.
3. The Deputy CISO shall serve as Deputy Chair of the Committee.
4. The Deputy Chair assists the Chair and acts on the Chair's behalf in case of accidents or the like.

Article 21 Committee members

The Committee consists of the following members.

(1) Division Information Security Officer

(2) Director of the Compliance Division

(3) Director of the Policy Planning Division

(4) Director of the General Affairs Division

(5) Director of the Information Systems Division

(6) Director of the Human Resources Division

(7) Other persons appointed by the Committee Chair

Article 22 Committee meetings

1. The Committee Chair shall convene the Committee meetings.
2. At least one-half of the members shall constitute a quorum at any Committee meetings.
3. The Committee Chair may allow a person other than Committee members to attend when it is deemed necessary.
4. The attendees referred to in the previous paragraph may give their opinions on matters for consideration in a meeting.

Article 23 Secretariat

The administration of the Committee shall be managed by the section in charge of general information security with the cooperation of the ICT Infrastructure and Technical Support Section, Information Systems Division.

Article 24 Miscellaneous

When not stipulated herein, the Chair shall determine matters concerning the Committee'sadministration after consulting the Committee.

Chapter 4. Information Security Subcommittee

Article 25 Establishment of the Subcommittee

RIKEN shall establish an Information Security Subcommittee (hereinafter "the Subcommittee") to discuss and deliberate necessary matters upon the instructions of the Committee.

Article 26 Responsibilities

The Subcommittee shall deliberate the following matters under commission of the Committee.

(1) Matters related to information security at RIKEN
(2) Other matters deemed necessary by the Committee

Article 27 Chair and Deputy Chair of the Subcommittee

1. The CISO shall serve as Chair of the Subcommittee.
2. The Chair of the Subcommittee shall represent the Subcommittee and preside over the work of the Subcommittee meetings.
3. The Deputy CISO shall serve as a Deputy Chair of the Subcommittee.
4. The Deputy Chair of the Subcommittee assists the Chair and acts on the Chair's behalf in case of accidents or the like.

Article 28 Subcommittee members

The subcommittee consists of the following members.

(1) Division Information Security Officers designated by the chair
(2) Director of the General Affairs Division
(3) Director of the Compliance Division
(4) Director of the Safety Management Division
(5) Director of the Information Systems Division
(6) Other persons appointed by the Chair

Article 29 Subcommittee meetings

1. The Chair shall convene the Subcommittee meetings.
2. At least one-half of the members shall constitute a quorum at any Subcommittee meetings.
3. The chair may allow a person other than Committee members to attend when it is deemed necessary.
4. The attendees referred to in the previous paragraph may give their opinions on matters for

consideration in a meeting.

Article 30 Secretariat

The administration of the Subcommittee shall be managed by the section in charge of general information security with the cooperation of the ICT Infrastructure and Technical Support Section, Information Systems Division

Article 31 Miscellaneous

When not stipulated herein, the Chair shall determine the matters concerning the Subcommittee's administration after consulting the Subcommittee.

Article 32 Working Group

1. A Working Group shall be set up to examine and study specific matters for the Subcommittee.
2. A person appointed by the Subcommittee Chair shall serve as Chair of the Working Group.
3. The Chair shall preside over the business of Working Group meetings.
4. Working Group members shall be appointed by the Chair of the Subcommittee.

Chapter 5. Use of Information, Information Systems, and the RIKEN network

Article 33 Basic matters

1. Users must comply with the related laws, these Regulations, and the Standards for Information Security when using information, information systems and the RIKEN network.
2. Users must prevent information security incidents by taking the information security measures stipulated by the Information Security Officer.
3. Users are prohibited from using information, information systems and the RIKEN network for purposes other than work duties.
4. Users must not damage or lose information, information systems, or the RIKEN network, or damage or lose related items.

Article 34 Classification of information and handling restrictions

1. Users must comply with the separately stipulated classification of information and handling restrictions when generating, updating, collecting, and obtaining information.
2. Information Security Officers must supervise the classification of information and handling restrictions in the laboratories, sections, offices or equivalent under their jurisdiction.
3. Division Information Security Officers must supervise the classification of information and handling restrictions in the division under their jurisdiction.

Chapter 6. Management of Information and Information System

Article 35 Scope of handling information and information systems

1. Information Security Officers and/or the Area Information Security Officers must define Management Areas, establish information security measures based on the characteristics of the area, notify users of these measures, and ensure compliance with these measures.
2. Information Security Officers and/or Area Information Security Officers must conduct and supervise information security measures in the Management Areas of the laboratories, sections, offices, or equivalent under their jurisdiction.
3. Division Information Security Officers must conduct and supervise information security measures in the Management Areas of the division under their jurisdiction.

Article 36 Management of information and information systems

1. Information Security Officers must stipulate, apply, and supervise information security measures for the information and information systems under their jurisdiction.
2. Information Security Officers must prevent information security incidents related to information and information systems.
3. Information Security Officers and Information System Administrators must not use administrative privileges improperly.
4. Information Security Officers and Information System Administrators must keep logs of information and information systems' operations.
5. Division Information Security Officers must supervise information security measures for the information and information systems under their jurisdiction.

Article 37 Discontinuance of information and information systems

The Information Security Officer must take measures to prevent information leakage when terminating, disposing, returning, and transferring information and information systems.

Article 38 Use of external services

1. Users are prohibited from using external services for the work of RIKEN without obtaining permission as specified in the following paragraph.
2. In granting permission for a user to use an external service for RIKEN work duties, the Information Security Officer shall confirm that said user will comply with the requirements for the use of the external service and these Regulations. Along with that, Information Security Officer must consult with the section in charge of general information security in advance, and registration to use external services must only be completed after permission is granted.

Article 39 Taking information systems off of the premises

1. Users are prohibited from taking information systems out of Management Areas without obtaining permission as specified in the following paragraph.
2. In granting permission for users to take information systems out of a Management Area, the Information Security Officer shall confirm that users will comply with these Regulations (even when using these systems outside the Management Area), according to separately prescribed procedures. Along with this, these systems must be registered with the section in charge of general information security.

Article 40 Use of external information systems for official duties

1. It is prohibited for a user to use an external information system for work purposes, or to handle information of RIKEN on an external information system, without obtaining permission as specified in the following paragraph.
2. In granting permission for a user to use an external information system for work purposes, to handle the information of RIKEN on an external information system, to bring an external information system into the Management Area, or to connect an external information system to the RIKEN network, the Information Security Officer shall confirm that the user will comply with these Regulations in accordance with the procedures separately stipulated. After permission is granted, the service must be registered with the section in charge of general information security.
3. When a user terminates the use of an external information system that handles the information of RIKEN, the Information Security Officer shall confirm that the information of RIKEN recorded in said information system has been erased. However, this does not apply in cases where the information is provided in accordance with the Regulations for Tangible Property Derived from Research (2006, Reg. No. 10) and the Provision and Receipt of Tangible Property Derived from Research (2006, Dir. No. 8), and cases where the information is relocated to an outside organization due to a transfer.

Chapter 7. Emergency Response

Article 41 Emergency contacts

1. When a user finds or is informed of an information security incident, he/she must immediately report it to the separately stipulated contact person.
2. A user must take countermeasures wherever possible to prevent the spread of damage from the information security incident.

Article 42 Emergency response

When Information Security Officers and Information System Administrators find or are notified of an information security incident, they must promptly take countermeasures to prevent damage from the incident from spreading.

Article 43 Post response

1. Information Security Officers and Information System Administrators must establish and execute a plan to prevent the reoccurrence of information security incidents (hereinafter "Reoccurrence Prevention Plan") and report it to the Division Information Security Officer.
2. The Division Information Security Officer. must report the Reoccurrence Prevention Plan to the Subcommittee.
3. The Subcommittee shall review the operations of the affected information system and the restart of its use based on the reported Reoccurrence Prevention Plan.

Chapter 8. Operation of Information Security

Article 44 Education

1. The CISO must educate users on information security as is stipulated in the Promotion Plan.
2. Users must receive education conducted by the CISO. Information Security Officers must ensure that the users of their laboratory, section, office, or equivalent receive this education.

Article 45 Acquiring knowledge about information security

The CISO is responsible for acquiring knowledge about information security and disseminating it to users.

Article 46 Monitoring

1. The CISO must take measures to detect and monitor information security incidents in the RIKEN network.
2. The CISO is authorized to monitor information, information systems, and the Institute network.

Article 47 Warning

1. The CISO may request reports from users on the status of their compliance with these Regulations.
2. The CISO may warn and request improvements from users who violate these Regulations, and from Information Security Officers and Division Information Security Officers who monitor the users.

Article 48 Restriction of use

The CISO shall limit the operation and use of information, information systems, and the RIKEN network by users who violate these Regulations, and by Information Security Officers and Division Information Security Officers who monitor the users.

Article 49 External personnel

1. Information Security Officers must supervise external personnel and ensure they comply with these Regulations when they use information, information systems, and the RIKEN network.
2. Division Information Security Officers must supervise the information security measures taken when accepting external personnel in the division under their jurisdiction.

Article 50 Outsourcing

1. Users must obtain prior approval from their Information Security Officer when outsourcing the generation, processing, calculation, etc. of information; or the development, operation, management, etc. of information systems.
2. The Information Security Officer must clarify the requirements regarding information security measures to avoid leakage, falsification, and destruction of information by the parties performing outsourced duties, describe these requirements in procurement specifications, and oblige the parties performing outsourced work to properly implement these requirements.
3. The Information Security Officer must clarify the requirements regarding information security measures for the procurement of information systems, such as the presence of known vulnerabilities, and preventing the delivery of improper information systems, in procurement specifications. The Information Security Officer must also ensure that these requirements are properly implemented.
4. Division Information Security Officers must ensure that information security measures are implemented in the outsourcing of work by, and the procurement of information systems by each section under their jurisdiction.

Article 51 Inspection, auditing, and continuous improvement

1. The CISO shall inspect and evaluate the implementation status of information security measures stipulated in Article 4, Paragraph 5.
2. The CISO must improve RIKEN's information security measures by revising the Promotion Plan based on the results of the inspections and evaluations stipulated in Paragraph 1; necessary improvements identified by the audits stipulated in Article 8, Paragraph 3; and major changes concerning information security.

Supplementary Provisions

These Regulations for Information Security are valid from October 1, 2018

Supplementary Provisions (Regulations 246 as of March 11, 2020)

These Regulations for Information Security are valid from April 1, 2020

Supplementary Provisions (Regulations 380 as of March 24, 2021)

These Regulations for Information Security are valid from April 1, 2021

Supplementary Provisions (Regulations 399 as of March 29, 2021)

These Regulations for Information Security are valid from April 1, 2021

Supplementary Provisions (Regulations 507 as of March 24, 2022)

These Regulations for Information Security are valid from April 1, 2022