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２９日規程第３９９号

RIKEN

Regulations for Information Security

Joho Security Taisaku Kitei

September 13, 2018, Reg. No 69

Updated March 29, 2021, Reg. No 399

Table of contents

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 information security measures at National Research and Development Institute RIKEN (hereinafter “the Institute”). 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. Other than the rules stipulated herein, will be provided in the “Standards for Information Security” and the “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 this Regulations for Information Security (hereinafter “the Policies”) at the Institute

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

(3) Division: an organizational group to implement information security measures that is stipulated separately

(4) Section: section, group or laboratory, etc. which is the smallest organizational unit set up in the Division concerning information security measures

(5) Executives and employees: executives and employees who are in service for RIKEN under the employment agreements with the Institute

(6) External personnel: personnel other than executives and employees

(7) Users: executives, employees and external personnel outside of RIKEN who use information assets as defined in the next item, the information system defined in item (10), and the Institute’s network defined in item (13)

(8) Information: the information that is generated, collected and obtained through activity of the Institute

(9) Information service: processing, accumulating, accepting and providing information for users

(10) Information systems: a system, hardware and software that provide information services for the work of the Institute

(11) External Information systems: Information systems such as PCs, servers, smart phones, tablet devices, and USB memory devices that are not assets of the Institute.

(12) Network: hardware such as cables, routers and switches to connect multiple information systems or equipment; software such as IP addresses, protocols and programs

(13) Institute network: a network that is used to connect, control and operate information systems for the work of the Institute

(14) Information security: to maintain the following balanced characteristics of information, information systems and the Institute network

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

b) Integrity, state of the accurateness and completeness of processing

c) Availability, state of affairs in which permitted persons can access information and related asset without interruption when it is needed

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

Article 3 Scope of these Regulations

1. The personnel applicable to these Regulations are users stipulated in the preceding Article, item (7).
2. The information applicable to these Regulations is the information stipulated in the preceding Article, item (8).
3. The information system applicable to these Regulations is the information system that is stipulated in the preceding Article, item (10).
4. The network applicable to these Regulations is the Institute network that is stipulated in the preceding Article, item (13).

Chapter 2 Organization Structure

Article 4 Chief Information Security Officer

1. The Institute 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 the Institute.
4. The CISO must formulate a plan (hereinafter “the Promotion Plan”) to promote general measures for information security at the Institute.
5. The CISO shall conduct information security measures based on the Promotion Plan.

6. The CISO shall define divisions as management units related to information security measures.

Article 5 Deputy Chief Information Security Officer

1. The Institute 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. The Institute shall designate an assistant Chief Information Security Officer who has expertise in information security.
2. The assistant CISO shall be appointed by the CISO.
3. The assistant CISO assists the CISO and perform a part of duties on behalf of CISO's instructed by the CISO.

Article 7 Information Security Advisor

1. The Institute 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. The Institute 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 the Institute and provides the CISO with audit reports.

Article 9 General Information Security Section

1. The Institute shall set up the General Information Security Section.
2. The General Information Security Section is the Information Security and User Support Section, Information Systems Division.
3. The General Information Security Section is in charge of taking information security

measures at the Institute and each Information Systems Office in branches shall support its task.

Article 10 Computer Security Incident Response Team

1. The Institute 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 act for the CISO's duties in emergency, such as suspension of use of the information, information systems and the Institute network, disclosure of necessary information and cooperation upon request, 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. The Institute shall designate Division Information Security Officers in each division.
2. The Division Information Security Officers shall be appointed by the CISO.
3. The Division Information Security Officers shall supervise the tasks relating to information security measures in their division.
4. The Division Information Security Officers shall provide a contact list of the Information Security Officers, Information Security Staff and the Information System Administrators in each division and report it to the CISO.

Article 12 Division Information Security Staff

1. The Institute shall designate a Division Information Security Staff in each division.
2. The 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 section.

2. The Information Security Officer is a leader of each section.

3. The Information Security Officer supervises tasks relating to information security measures of their division.

4. The Information Security Officer need to 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 section.

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 as a service.

2. The Information System Administrators shall be appointed by the Information Security Officer.

3. The Information System Administrator shall take the information security measures to the information systems in each jurisdiction.

Article 16 Area Information Security Officer

1. An Area Information Security Officer shall be appointed corresponding to the scope (hereinafter referred to as the “Management Areas”) where information security measures for facilities such as offices and server rooms are required.

2. The Area Information Security Officer shall supervise the operations concerning the information security measures in the Management Areas.

3. An Area Information Security Officer shall be appointed without fail, even if a Management Area is used by multiple divisions. The Area Information Security Officer shall be designated by the Branch Director.

4. When a management area is used by a single division, the information security officer shall act as the Area Information Security Officer of the division concerned.

Article 17 Appropriateness of approval, authorization and audit

1. RIKEN executives and employees shall not concurrently undertake the following roles when implementing information security measures.

   (1) A submitter of 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 approvers are not qualified for authorization to apply for, executives and employees can apply it to other supervisor of the approval authority, etc. or other appropriate person to get an approval.

Chapter 3 Information Security Committee

Article 18 Establishment of the Committee

The Institute shall establish an Information Security Committee.

Article 19 Responsibilities

The Committee shall deliberate the following matters.

(1) Important matters regarding information security at the Institute

(2) Other matters if the Committee deems it necessary

Article 20 Chair and Deputy Chair of the Committee

1. The CISO shall serve as a chair of the Committee.
2. The chair shall represent the Committee and preside over the work of the Committee.
3. The Deputy CISO serves as a 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) Another person 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 appoint a person other than committee members when it is deemed necessary.
4. The attendees referred to in the previous paragraph may give their opinions in a meeting.

Article 23 Secretariat

The administration of the Committee shall be managed by the General Information Security Section with the cooperation of the Information and Communication Infrastructure Section.

Article 24 Miscellaneous

What is not stipulated herein, the chair shall determine the matters concerning the Committee's administration with consulting the Committee.

Chapter 4 Information Security Subcommittee

Article 25 Establishment of the Subcommittee

The Institute 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 the Institute

(2) Other matters deemed important by the Committee

Article 27 Chair and Deputy Chair of the Subcommittee

1. The CISO shall serve as a 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) Another person 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 appoint a person other than subcommittee members when it is deemed necessary.
4. The attendees referred to in the previous paragraph may give their opinions in a meeting.

Article 30 Secretariat

The administration of the Subcommittee shall be managed by the General Information Section with the cooperation of the Information and Communication Infrastructure Section.

Article 31 Miscellaneous

What is not stipulated herein, the chair shall determine the matters concerning the Subcommittee's administration with 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 a chair of the Working Group.
3. The chair shall manage the matters of Working Group's secretariat.
4. Working Group members shall be appointed by the chair of the Subcommittee.

Chapter 5 Use of Information, Information Systems and the Institute Network

Article 33 Basic matters

1. Users must comply with the related laws, these Regulations and Procedures for Information Security when using information, information systems and the Institute network.
2. Users must prevent information security incidents by taking information security measures stipulated by the Information Security Officer.
3. Users are prohibited from using information, information systems and the Institute network for no-job related purpose.
4. Users must not damage or lose any items related to information, information systems and the Institute network.

Article 34 Classification of Information and Handling Restrictions

1. Users must comply with the classification of information and handling restrictions that are stipulated separately while creating, updating, collecting and obtaining information.
2. The Information Security Officer must supervise the classification of information and handling restrictions in each jurisdiction.
3. The Division Information Security Officer must supervise the classification of information and handling restrictions in each division.

Chapter 6 Management of Information and Information System

Article 35 Information and information handling scope

1. The Information Security Officer and/or the Area Information Security Officer must define Management Areas and establish Information Security measures based on the characteristics of the area and notify users of these in order to ensure compliance.
2. The Information Security Officer and/or the Area Information Security Officer must take and supervise information security measures in the Management Areas.
3. The Division Information Security Officer must take and supervise information security measures of the Management Areas in each division.

Article 36 Management of information and information systems

1. The Information Security Officer must take and supervise information security measures for the information and information systems.
2. The Information Security Officer must prevent information security incidents related to

information and information systems.

3. The Information Security Officer and the Information System Administrators must not use administrative privileges improperly.

4. The Information Security Officer and the Information System Administrators must keep logs of the operations of the information and information systems.

5. The Division Information Security Officer must supervise information security measures for the information and information systems in each division.

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 the information and information systems.

Article 38 Use of external information services

1. Users are prohibited from using the external information services for the efforts of the Institute without the permission specified in the following paragraph.

2. In granting permission to a user to use the external information service for the Institute's business, the Information Security Officer shall confirm that the said user complies with the requirements for the use of the external information service and these regulations in accordance with the separately prescribed procedures. Along with that, general information security section must be consulted in advance, and the services must be registered for use after the permission is granted.

Article 39 Taking Information systems out of the premises

1. Users are prohibited from taking the information system out of the areas requiring control measures without obtaining the permission specified in the next section.

2. In permitting users to take the information system out of the Management Area, the Information Security Officer shall confirm that the users will comply with these regulations (even when using these systems outside the Management Area) for the information system to be taken out of the Management Area, according to separately prescribed procedures. Along with this, these systems must be registered with the General Information Security Section.

Article 40 Use of external information systems for official duties

1. It is prohibited for a user to use an external information system for effort purposes or to handle information of the Institute on an external information system without obtaining the permission prescribed in the following paragraph.

2. When the Information Security Officer permits a user to use the external information system for effort purposes, to handle the information of the Institute on the external information system, to bring the external information system into the area requiring control measures, or to connect the external information system to the network of the Institute, the Information Security Officer shall confirm that the user complies with these regulations in accordance with the procedures separately prescribed. After the permission is granted, the service shall be registered with the General Information Security Section.

3. When a user terminates the use of an external information system that handles the information of the Institute, the Information Security Officer shall confirm that the information of the Institute recorded in the said information system has been erased. However, this does not apply to the case where the information is provided in accordance with the regulations of the Regulations for Tangible Property Derived from Research (Regulation No. 10 of 2006) and the Provision and Receipt of Tangible Property Derived from Research (Circular No. 8 of 2006), and the case where the information is transferred 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 report it to the designated section immediately.

2. A user must take countermeasure to prevent the information security incident from spreading as efficiently as possible.

Article 42 Emergency response

When the Information Security Officer and the Information System Administrators find or are notified of an information security incident, they must take countermeasure to prevent the incident from spreading swiftly.

Article 43 Post response

1. The Information Security Officer and the Information System Administrators must establish and execute a plan to prevent the reoccurrence of information security incidents (hereinafter "Plan to prevent reoccurrence") and report it to the Division Information Security Officer.

2. The Division Information Security Officer must report the plan to prevent reoccurrence to the Subcommittee.

3. The Subcommittee shall judge the appropriateness of the submitted plan concerning the information system's restart.

Chapter 8 Operation of Information Security

Article 44 Education

1. The CISO shall conduct the education on information security to users as is stipulated in the Promotion Plan.

2. Users shall receive education conducted by the CISO. The Information Security Officer must ensure that the users of the division receive training.

Article 45 Acquiring knowledge of the information security

The CISO is responsible for acquiring knowledge of information security and notify them to users.

Article 46 Monitoring

1. The CISO must take measures to detect and monitor information security incidents in the Institute network.

2. The CISO is authorized to monitor information, information systems and the network of the Institute.

Article 47 Warning

1. The CISO shall request users to submit reports on the status of compliance with these Regulations.

2. The CISO shall warn and request improvements to a responsible Information Security Officer, a Division Information Security Officer and a user who violate these Regulations.

Article 48 Restriction of use

The CISO shall limit the use of information, information systems and the Institute network by a responsible Information Security Officer, a Division Information Security Officer and a user who violate these Regulations.

Article 49 External personnel

1. The Information Security Officer must supervise external personnel to comply with these Regulations when they use information, information systems and the Institute network.

2. The Division Information Security Officer must supervise the information security measures to external personnel in the division.

Article 50 Outsourcing

1. Users must obtain prior approval from their Information Security Officer when outsourcing information generation, processing, calculation, development, operation and management of information systems.
2. The Information Security Officer must clarify the requirements regarding information security measures in procurement specifications to avoid leakage, falsification and damage of information by the outsourcing parties and ensure that the contracted work is duly performed.
3. The Information Security Officer must clarify and oblige the outsourcing parties to ensure the requirements regarding information security measures for information systems in procurement specifications in order to avoid vulnerabilities in the system or the improper information system at delivery.
4. The Division Information Security Officer must oblige the outsourcing parties to ensure information security measures defined by each jurisdiction in procurement specifications.

Article 51 Check, conducting audit and continuous improvement

1. The CISO shall check and evaluate the implementation status of information security measures stipulated in Article 4, Paragraph 5.
2. The CISO must improve the Institute's information security measures by reviewing the Promotion Plan of measures based on the results of the check and evaluations stipulated in Paragraph 1, necessary improvements identified by 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 (Regulation 246 as of March 11, 2020)

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

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

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