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
改正　令和５年１０月３１日規程第１０８号
改正　令和６年８月２９日規程第１８５号
改正　令和７年３月３１日規程第１４３号
改正　令和７年４月２４日規程第１８１号

# RIKEN
# Regulations for Information Security

*Joho security taisaku kitei*

September 13, 2018, Reg. No 69

With revisions effective May 1, 2025

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

**Table of contents**


**Chapter 1** **General Provisions** (Articles 1 & 2)

**Chapter 2** **Organization Structure** (Articles 3 - 20)

**Chapter 3** **Information Security Committee** (Articles 21 - 24)

**Chapter 4** **Use of Information, Information Systems, and the RIKEN Network** (Articles 25 & 26)

**Chapter 5** **Management of Information and Information Systems** (Articles 27 - 32)

**Chapter 6** **Emergency Response** (Articles 33 & 34)

**Chapter 7** **Other Matters** (Articles 35 - 41)

**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 Standards of Cybersecurity Measures for Government Agencies and Related Agencies.

Article 2 Definitions of terms

Key terms in this document are defined as follows.

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

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

(3) Employees: executives and employees engaged in RIKEN activities (all personnel directly employed by RIKEN)

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

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

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

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

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

(9) 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

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

(11) Users: executives, employees, and external personnel who use information, information systems, and RIKEN network.

(12) 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

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

(14) 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.

## Chapter 2. Organization Structure

Article 3 Chief Information Security Officer

1. RIKEN designates a Chief Information Security Officer (the “CISO”) who is appointed by the President.
2. The CISO organizes information security measures at RIKEN.
3. The CISO must formulate a plan for Information Security to promote general measures for information security at RIKEN, and conduct information security measures based on the plan.
4. The CISO stipulates the divisions to act as management units related to information security measures.

Article 4 Chief Information Security Technical Officer

1. RIKEN designates a Chief Information Security Technical Officer (the “CISTO”) who is appointed by the President.
2. The CISTO assists the President and CISO on technical work regarding information security measures at RIKEN from an expert perspective.
3. The CISTO meets with the CISO to determine the severity of information security incidents and cooperate closely with the President and CISO based on the severity, responding to incidents to prevent the spread of damage.

Article 5 Deputy Chief Information Security Officer

1. RIKEN designates a Deputy Chief Information Security Officer (the “Deputy CISO”) who is appointed by the CISO.
2. 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 designates an Assistant Chief Information Security Officer (the “assistant CISO”) who has expertise in information security, and who is appointed by the CISO.
2. 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 designates an Information Security Advisor.

2. The Information Security Advisor is appointed or commissioned by the CISO from among individuals who have expertise in information security.
3. The Information Security Advisor provides advice to the CISO on information security measures.

Article 8 Chief Information Security Auditor

1. The director of the Internal Audit Office serves as the Chief Information Security Auditor, conducts audits for RIKEN's information security measures, and reports to the CISO.

Article 9 Section in charge of general information security

1. Information Security & Systems Division is the section in charge of general information security, and handles information security measures for RIKEN.

Article 10 Computer Security Incident Response Team

1. RIKEN establishes a Computer Security Incident Response Team (the "CSIRT").
2. The administrative tasks related to CSIRT operations will be performed by the Information Security & Systems Division.
3. The CSIRT carries 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.

Article 11 Organization of CSIRT

1. The CSIRT is composed of five or more members from among the following personnel.

(1) Persons designated by the Director of the Information Security & Systems Division from among the personnel of the Information Security & Systems Division

(2) Other persons designated by the CISO.

Article 12 CSIRT Leader and Deputy CSIRT Leader

1. CSIRT has a CSIRT Leader and a Deputy CSIRT Leader, and are appointed by the CISO.
2. In the event that the CSIRT Manager is unable to perform their duties, the Deputy CSIRT Leader acts on their behalf.

Article 13 Duties of CSIRT

1. The CSIRT carries out the activities listed in the following items.

(1) Collect information and accurately grasp the facts when an information security incident occurs.

(2) Provide technical support and advice related to preventing damage expansion, recovery, and

prevention of recurrence.

(3) Communicate and coordinate with internal departments and related organizations, and share information regarding information security incidents.

(4) Consolidate information security incidents occurring within RIKEN and provide support related to countermeasures and preventive measures.

(5) Conduct training and exercises for CSIRT members as necessary to improve the ability to respond to information security incidents.

2. Users must cooperate with the CSIRT in responding to information security incidents.

3. The CSIRT may seek advice from specialized divisions as necessary for its activities.

Article 14 Division Information Security Officer

1. A Division Information Security Officer is designated in each division, and is appointed by the CISO.

2. Division Information Security Officers organize and supervise tasks related to information security measures in the division under their jurisdiction.

3. Division Information Security Officers 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 15 Division Information Security Staff

1. Division Information Security Staff are designated in each division, and are appointed by the Division Information Security Officer after consultation with the CISO

2. The Division Information Security Staff assists the Division Information Security Officer.

Article 16 Information Security Officer

1. An Information Security Officer oversees and supervises tasks related to information security measures in the section under their jurisdiction.

2. 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.

Article 17 Information Security Staff

1. An Information Security Staff may be designated in each laboratory, section, office, or equivalent, and is appointed by the Information Security Officer.

2. The Information Security Staff assists the Information Security Officer in matters related to

information security measures.

Article 18 Information System Administrator

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

Article 19 Area Information Security Officer

1. Area Information Security Officers are appointed in correspondence 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 are appointed from among the persons listed in each item below, as applicable.
   (1) When one Management Area is used by one section: Information Security Officer
   (2) When one Management Area is used by multiple sections: A person designated by the Operations Division Director
3. Area Information Security Officers oversees and supervise tasks related to information security measures in the Management Area under their jurisdiction.

Article 20 Appropriateness of approval, authorization, and audit

1. RIKEN executives and employees cannot 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, executives and 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 21 Establishment of the Committee

RIKEN establishes an Information Security Committee (hereinafter referred to as "the Committee")

within RIKEN to examine and deliberate on important matters related to information security.

Article 22 Committee members

The Committee is composed of the following members.

(1) CISO
(2) Deputy CISO
(3) RIKEN Information R&D and Strategy Headquarters Director
(4) Information Security & Systems Division Director
(5) General Affairs Division Director
(6) Research Integrity and Economic Security Division Director
(7) Division Information Security Staff appointed by the Chair
(8) Other persons appointed by the Committee Chair

Article 23 Chair and Deputy Chair of the Committee

1. The Committee designates a Chair, who is the CISO.
2. The Chair presides over the work of the Committee.
3. The Committee designates a Deputy Chair, who is the Deputy CISO.
4. The Deputy Chair assists the Chair and acts on the Chair's behalf in case of accidents or the like.

Article 24 Committee meetings, etc.

1. The Committee Chair convenes the Committee meetings.
2. At least one-half of the members constitutes a quorum at any Committee meetings.
3. Chief Information Security Auditor may attend the Committee meetings and give opinions.
4. The Committee Chair may allow a person other than Committee members to attend when it is deemed necessary.
5. The attendees referred to in the previous paragraph may give their opinions on matters for consideration in a meeting.
6. The administration of the Committee is managed by the Information Security & Systems Division.

## Chapter 4. Use of Information, Information Systems, and the RIKEN network

Article 25 Basic matters

1. Users must comply with the related laws, these Regulations, and Information Security Standards (the Standards for Information Security and the Implementation Procedures 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 26 Classification of information and handling restrictions

1. Users must comply with the classification of information and handling restrictions stipulated in the Implementation Procedures for Information Security when generating, updating, collecting, and obtaining information.

## Chapter 5. Management of Information and Information System

Article 27 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.

Article 28 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.

Article 29 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 30 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 confirms 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 Information Security & Systems Division in advance, and registration to use external services must only be completed after permission is granted.

Article 31 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 confirms that users will comply with these Regulations (even when using these systems outside the Management Area), according to the procedures stipulated in the Implementation Procedures for Information Security. Along with this, these systems must be registered with the Information Security & Systems Division.

Article 32 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 confirms that the user will comply with these Regulations in accordance with the procedures stipulated in the Implementation Procedures for Information Security. After permission is granted, the service must be registered with the Information Security & Systems Division.
3. When a user terminates the use of an external information system that handles the information of RIKEN, the Information Security Officer confirms 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 6. Emergency Response

Article 33 Emergency response

1. When a user finds or is informed of an information security incident, they must immediately report it to the supervisor or to the CSIRT.
2. A user must take countermeasures wherever possible to prevent the spread of damage from the information security incident.
3. 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 34 Post response

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

## Chapter 7. Other Matters

Article 35 Education, etc.

1. The CISO must educate users on information security as is stipulated in the Promotion Plan.
2. Users must receive education on information security stipulated in the preceding paragraph.
3. The CISO is responsible for acquiring knowledge about information security and disseminating it to users.

Article 36 Monitoring, etc.

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 RIKEN network.

Article 37 Warnings, etc.

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 38 Restriction of use

The CISO limits 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 39 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 40 Outsourcing, etc.

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 41 Inspection, auditing, and continuous improvement

1. The CISO inspects and evaluates the implementation status of information security measures.
2. The CISO must improve RIKEN’s information security measures based on the results of the

inspections and evaluations audit results 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

**Supplementary Provisions (Regulations 108 as of October 31, 2023)**

These Regulations for Information Security are valid from November 1, 2023

**Supplementary Provisions (Regulations 185 as of August 29, 2024)**

These Regulations for Information Security are valid from September 1, 2024

**Supplementary Provisions (Regulations 143 as of March 31, 2025)**

These Regulations for Information Security are valid from April 1, 2025

**Supplementary Provisions (Regulations 181 as of April 24, 2025)**

These Regulations for Information Security are valid from May 1, 2025