RIKEN
Standards for Information Security

Version 4.0 April 2022

Information Security Committee

Table of contents

Revision History

Date	Ver.	Revisions
Apr 1, 2019	1.0	Initial Version
Mar 26, 2020	2.0	Chapter 3 – Classification of Information and Handling Restrictions/Confidentiality Classifications Chapter 9 – Information security audit/Responding to audit results
Apr 1, 2021	3.0	Chapter 4 – Added the “Area Information Security Officer” in the areas requiring control measures Chapter 10 – Specified procedures for using external services according to the t general terms and conditions, social media services, and cloud services. Chapter 12 – Added “Authentication data management”
April 1, 2022	4.0	Compliance with the FY 2021 standards set by the government Chapter 3 – Classification of Information and HandlingRestrictions Chapter 12 – Information System Security Requirements Chapter 13 – Components of information systems Chapter 14.7 – Added “Teleworking”

Chapter 1. Purpose

RIKEN, National Research and Development Agency (hereinafter referred to as "RIKEN") enforced Regulations for Information Security that set forth basic matters for assurance of information security as of October 1, 2018 in order to employ information security measures in RIKEN. The Regulations are based on the Common Model of Information Security Measures for Government Agencies and Related Agencies (formulated by the Cybersecurity Strategic Headquarters on August 31, 2016).

To set forth necessary matters and procedures for enforcing the Regulations for Information Security, these Standards for Information Security were formulated by the Information Security Committee (hereinafter referred to as "Committee") based on the Common Standards for Information Security Measures for Government Agencies and Related Agencies (effective as of July 25, 2018) and were revised in accordance with the Common Standards for Cyber Security Measures for Government Agencies and Related Agencies (effective as of July 7, 2021)

Chapter 2. Definition of Terms

The definition of terms in this Standards for Information Security have the following meanings:

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

(2) Division/section/office or equivalent: the smallest organizational unit concerned with the information security measures. Set up by each group

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

(4) External personnel: personnel other than employees

(5) Users: employees and the external personnel who use Information defined in the next Article, the RIKEN information system in Article 10, and the RIKEN network in Article 13

(6) Information: information that is generated, collected, or obtained through RIKEN activity

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

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

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

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

(11) RIKEN network: a network used to connect, control, and operate information systems to conduct RIKEN activity

(12) Information security: to soundly maintain the following characteristics, which are essential attributes of

information, information systems, and the RIKEN network:

(a) Confidentiality, to ensure that only authorized persons are able to access the information.

(b) Integrity, to ensure the accuracy and completeness of information and its processes

(c) Availability, the assurance that information is accessible without interruption when needed

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

(14) External service: provision of part or all of the functions of the information system to the public by an external party, provided that the said functions handle the information of RIKEN.

(15) 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."

Chapter 3. Classification of Information and Handling Restrictions

3.1. Scope of information

The scope of the term “information” in the Standards for Information Security shall be equivalent to the information in “official documents” defined in Article 2, paragraph 1 of RIKEN Document Management Regulations (October 1, 2003, Reg. No. 29) (hereinafter referred to as "Document ManagementRegulations"). However, research data, laboratory notebooks, etc. that are out of the scope of the "official documents" in Article 3 shall also be included.

3.2. Prohibition of use of information other than intended purposes

All users (hereinafter, if the subject of sentence is not described, the subject is “all users”) shall create, obtain, utilize, store, provide, transport, transmit, delete, copy, or process (hereinafter referred to as "utilization, etc.") information only to perform their assigned duties.

3.3. Classification of information and handling restrictions

When utilizing information, all users shall assign information classification and handling restrictions in terms of confidentiality, integrity, and availability upon approval of the Information Security Officers.

(a) Confidentiality, to ensure that only authorized persons are able to access the information

	Classification (Government Common Standards)	Classification (RIKEN)	Classification criteria of information
Confidential information	Confidentiality class-3 information	Top secret	Information handled at RIKEN in the scope of information set forth in Article 3.1 which requires the confidentiality of information and is required to be handled as "Highly Confidential" as set forth in Article 26 of the Document Management Regulations.
		Secret	Information handled at RIKEN in the scope of information set forth in Article 3.1 which requires the confidentiality of information and is required to be handled as "Confidential" as set forth in Article 26 of the Document Management Regulations.
	Confidentiality class-2 information	Information shared within division/section/ office or equivalent	Information that includes information that is highly probable to be considered as falling under non-disclosure information under Article 5 of the Act of the Information Disclosure Law for Independent Administrative Institutions, etc., that can be known within the division/section/office or equivalent, and that is not intended to be immediately released to the public, other than Confidentiality class-3 information
		Internal Information	Information that includes information that is highly probable to be considered as falling under non-disclosure information under Article 5 of the Act of the Information Disclosure Law for Independent Administrative Institutions, etc., that can be known within RIKEN, that and is not intended to be immediately released to the public, other than Confidentiality class-3 information.
Confidentiality class-1 information		No plan to be released to the public	Information that excludes information that highly probable to be considered as falling under non-disclosure information under Article 5 of the Act of the Information Disclosure Law for Independent Administrative Institutions, etc., and that is not scheduled to be released to the public.
		Open to the public	Information that will be or has been released to the public.

(Example) Handling restrictions for confidentiality

Types of handling restrictions	Specification
Redistribution	Redistribution prohibited, approval is required for redistribution
Storage place	Designated area only, management area only, RIKEN premises only
Disclosure	Non-disclosure, no restrictions
Restrictions on handling persons	Limited to a certain group, limited to committee members, limited to the specified persons, NDA required
Restrictions on places for handling	RIKEN internal use, limited to a certain division, limited to a certain room
Validated date	xx is prohibited until mm/dd/yyyy, xx is prohibited during yy
Combined conditions	If handling restrictions on any information are wide-raging, classification and handling restrictions shall be separately designated to the information.
Others	Information that requires especially stringent handling shall be described as necessary.

(b) Integrity, the accuracy and completeness of information and its processes

Classification	Classification criteria
Critical information	Information handled at RIKEN (except for written information) whose falsification, errors, or damage may hamper the proper operations of RIKEN (except for negligible cases)
Non-classified	Information other than information that requires integrity (except for written information)

(Example) Handling restrictions for integrity

Types of handling restrictions	Specification
Storage period	Store until mm/yyyy
Storage location	Store in xx
Rewriting	Rewriting prohibited, permission is required for rewriting
Deletion	Deletion prohibited, permission is required for deletion
Measures after expiration of storage period	Erase all, making it completely unrestorable after expiration of the storage period

(c) Availability, the assurance that information is accessible without interruption

Classification	Classification criteria
Vital information	Information handled in RIKEN (except for written information) whose destruction, loss, or unavailability may infringe upon the stable operations of RIKEN (except for negligible cases).
Non-classified	Information other than information that requires availability (except for written information)

(e.g.) Handling restrictions for availability

Types of handling restrictions	Specification
Permissible recovery time	Within xx sec
Backup	Backup needed, backup is not needed
Storage location	Store in xx

Chapter 4. Assignment of Management Areas

4.1. Class assignment and measures for management areas

The Group Information Security Officers and Area Information Security Officers shall assign the necessary classes for areas requiring control measures and define the persons who are not authorized to enter these areas (hereinafter referred to as "outside persons") to secure the safety of sections within their jurisdiction, as well as the security of information, information systems, etc., in the management areas.

(a) Class assignment and measures for management areas (e.g.)

Class	Description	Example	Measures
class-3	An area that requires stringent measures to restrict entry to the area to the administrators and maintenance workers of the information system and related devices	A server room where an information system that handles confidential information, important networking devices such as security device, core switches, and WAN routers are located.	No admittance except for authorized persons with ID cards, biometric authentication, a locking system, etc. Access control to network racks is the same.

class-2	An area that requires measures for information security, such as entry restrictions for all persons other than employees of RIKEN and related parties	Facilities such as offices, safes, and lockable cabinets where confidential information may be handled or stored.	Limit easy entry by outside persons using doors, etc. Facilities must be locked while employees are away.
class-1	An area, other than class-2 and class-3, where entry of outside persons is restricted (such as the inside of a building)	Areas where employees and authorized outside personscan enter, such as lobbies, reception rooms, and meeting rooms inside buildings.	No admittance to outside persons without ID card,etc. at the entrance of the building.
class-0	An area where outside persons may enter after following the entry procedures	Areas where outside persons may enter followingthe entry procedures at the guardhouse, such as RIKEN premises, halls, and cafeteria.	Only persons who follows the entry procedures at the gatehouse may enter.

4.2. Implementing measures in management areas

(a) The Area Information Security Officer shall designate the class of the management area, inform the users of the necessary measures, have them implement the measures, and supervise them.

(b) The Area Information Security Officer shall devise and implement disaster countermeasures to protect information systems in the management area.

(c) All users shall comply with the measures taken in the management area.

Chapter 5. Information Handling

5.1. Assignment of information classification and handling restrictions

Classification and handling restrictions for information which has been assigned handling restrictions shall be clearly expressed in a way that those browsing this information can identify.

5.2. Re-assignment of information classification and handling restrictions

When using (especially processing) information with assigned classification and handling restrictions, users shall re-assign appropriate classification and handling restrictions in consideration of the confidentiality, integrity, and availability of the information, under the approval of the Information Security Officers of the division, section, office, or equivalent which originally assigned information classification and handling restrictions.

5.3. Change of information classification and handling restrictions

When changing information classification and handling restrictions, approval shall be obtained from the Information Security Officers of the division, section, office, or equivalent that has assigned classification and

handling restrictions to the information.

5.4. Information handling

All users shall handle information in accordance with the handling restrictions assigned to the information.

5.5. Storage of information

(a) Information shall be assigned an appropriate access privilege and stored based on the handling restrictions.

(b) Requirements for backup, redundancy, and measures against earthquakes at storage locations shall be formulated based on the handling restrictions on information to take necessary measures.

(c) Information systems that handle information shall be installed in a management area based on the handling restrictions.

5.6. Provision or disclosure of information

(a) Information shall be provided or disclosed based on handling restrictions.

(b) Parties receiving information shall be obliged to properly observe the restrictions on handing of the information and shall be subject to RIKEN's supervision.

(c) Unnecessary ancillary parts of information, including properties and proofreading history, shall be erased based on the handling restrictions when the information is disclosed or provided.

5.7. Utilization, etc. outside management areas

When taking information off of premises in mobile terminals, external storage media, etc.; or handling information outside management areas via emails, file sharing, etc.; approval shall be obtained in particular from the Information SecurityOfficers, and information security measures such as encryption, password lock, etc., shall be taken based on information handling restrictions.

5.8. Deletion of information

(a) Information used outside management areas shall be immediately erased based on handling restrictions when its usage is complete.

(b) When disposing of external storage media in which confidential information is stored, measures shall be taken to ensure that all stored information is completely unrecoverable.

5.9. Backup of information

Information shall be backed up in accordance with the information handling restrictions.

(a) The backup information described in the preceding paragraph shall be appropriately managed by deciding the place, manner, storage period, etc., of the information, in accordance with the information handling restrictions.

(b) The backup information shall be erased or discarded after the retention period by taking measures to ensure that the information is completelyunrestorable.

Chapter 6. Information Security Measures

6.1. Operation of information security measures

(a) The section in charge of general information security (specified by the Regulations for Information Security) shall maintain the operational procedures for informationsecurity measures at RIKEN.

(b) If the Information Security Officer is informed by a user of issues and problems related to the Standards and the Procedures for Information Security, the Information Security Officer shall report them to the section in charge of general information security.

(c) The section in charge of general information security shall examine the report prescribed in the preceding paragraph. If action is necessary, the section in charge of general information security shall report the issues to the Chief Information Security Officer (hereinafter referred to as "CISO") and shall consult with the Information Security Committee.

(d) The CISO shall direct the section in charge of general information security to take action as necessary.

6.2. Exceptional measures

(a) If the Regulations for Information Security, the Standards for Information Security, or thePromotion Plan for Information Security hinder the efforts of RIKEN, exceptional measures may be applied for as necessary after consultation with the section in charge of general information security. The CISO shall determine the person who decides whether or not to approve applications for exceptional measures and the review procedure.

(b) The section in charge of general information security shall maintain records of applications for exceptional measures and request that applicants of the exceptional measures report the status periodically.

6.3. Response to information security incidents

(a) If an information security incident is discovered or reported, a report shall be made in accordance with the procedures separately designated. This shall be considered the initial response to the incident.

(b) Upon receiving a report of information security incident, the Computer Security Incident Response Team (hereinafter referred to as "CSIRT") shall report it to contact persons and sections in accordance with procedures separately designated. This shall be considered the response to the information security incident.

(c) The CISO shall direct the section in charge of general information security to review and implement measures to prevent recurrence of the information security incident.

(d) The section in charge of general information security shall collect information on the situation, countermeasures, and measures to prevent recurrence of information security incidents; and shall announce them to all users in RIKEN.

Chapter 7. Information Security Education

7.1. Establishment of educational structures

(a) The section in charge of general information security shall formulate education plans and establish educational structures for information security.
(b) The section in charge of general information security shall review the education plans appropriately in accordance with the changing environment of information security.

7.2. Enforcement of education

(a) All users must take the information security education immediately after commencing actual use of information systems and RIKEN networks. If lack of training persists, the CISO shall request that Group Information Security Officers make improvements and take necessary measures, including suspending the use of the network and information services by the relevant users and the division/section/office or equivalent.
(b) The CISO shall ensure that CSIRT members take the security education required for their training as CSIRT members.
(c) The section in charge of general information security shall report the implementation status of information security education to the CISO.

Chapter 8. Self-check

8.1. Formulation and implementation of self-check plan

(a) The section in charge of general information security shall formulate and conduct a plan for self-checks concerning the implementation status of information security measures based on the Promotion Plan for Information Security, as necessary.
(b) The section in charge of general information security shall revise the self-check plan according to changes in the information security environment.

8.2. Conducting self-checks

(a) The section in charge of general information security shall instruct groups and divisions/sections/offices or equivalent to conduct self-checks in accordance with the self-check plan.
(b) Groups, divisions, sections, offices, etc. shall promptly conduct self-checks and report the results to thesection in charge of general information security when they are instructed to conduct a self-check.

8.3. Responding to self-check

(a) The section in charge of general information security shall collect, analyze, and evaluate the self-check results.
(b) If serious problems are found through the evaluation of the self-check, the section in charge of general information security shall instruct the Group Information Security Officers and Information Security Officers to correct the problems and shall report the problems to the CISO.
(c) The section in charge of general information security shall report the results of the analysis and evaluation of self-check to the CISO.

(d) If the CISO find problems when evaluating self-check results, the CISO shall instruct the section in charge of general information security and the Group Information Security Officers to correct the problems.
(e) The section in charge of general information security and the Group Information Security Officers shall regularly report the status of the corrections instructed by the CISO.
(f) The CISO shall review the Promotion Plan for Information Security with consideration to the evaluation result of the self-check.

Chapter 9. Information Security Audit

9.1. Formulation of audit plans

The Chief Information Security Auditor shall formulate a plan to implement information security audits in accordance withthe status of information security and the Promotion Plan for Information Security.

9.2. Conducting information security audit

(a) The Chief Information Security Auditor shall conduct audits relating to the RIKEN information security measures based on the audit implementation plan and shall report audit results to the CISO.
(b) The Chief Information Security Auditor may establish an information security audit team to conduct audits.

9.3. Responding to audit results

(a) Should any improvements be deemed necessary as a result of an audit, the CISO shall review the Promotion Plan for Information Security, and shall provide instructions for the section in charge of general information security and the Group Information Security Officers to make improvements as necessary.
(b) The section in charge of general information security and the Group Information Security Officers shall formulate and implement an improvement plan per the instructions and report them to the CISO.

Chapter 10. Outsourcing

10.1. Outsourcing

(a) The section in charge of general information security shall examine as necessary the requirements of information security measures for the outsourcing of construction, operation, and maintenance of information systems; or the development and maintenance of application software; and shall set the implementation procedures.
(b) When outsourcing whole or a part of tasks relating to information or information systems to any external parties, it required to receive approval from the Information Security Officers, stipulate requirements of information security measures in accordance with the procedures in the preceding paragraph, and describe the measures in contractual documents.
(c) When outsourcing, Information Security Officers shall have the party performing outsourced work

observe the requirements of the information security measures and shall check their implementation status.

(d) When parties performing outsourced work handle confidential information, approval shall be obtained from the Information Security Officer. The parties performing outsourced work shall comply with handling restrictions and be obliged to follow necessary procedures and implement information security measures.

(e) In case of an information security incident by parties performing outsourced work, a contact system with the party performing outsourced work and measures to deal with such an incident shall be established as necessary.

(f) In the case that outsourcing parties subcontract a part of outsourced tasks to any other party, the requirements of information security measures shall be observed at the same level as those of the outsourcing parties, and the subcontractor's implementation status shall be checked.

(g) Upon the termination of contract, the information of RIKEN handled by the party performing outsourced work shall be returned or deleted, and this shall be confirmed, unless otherwise prescribed.

(h) When information security incidents are discovered or reported at parties performing outsourced work, the provisions in Chapter 6, Article 3 "Response to informationsecurity incidents" shall be observed.

10.2. Use of external services

(a) The section in charge of general information security shall establish rules for the use of external services (criteria for the use of external services, selection criteria for external service providers, procedures for use, and management on status of use).

(b) Information Security Officers shall designate a responsible person for each external service contracted so that such external services can be supervised.

(c) When handling confidential information, the Information Security Officer shall consider the use of external services based on the classification and handling restrictions of the information handled, and the scope of roles and responsibilities concerning information security. After consulting with the section in charge of general information security, the information Security Officer shall select external services in accordance with the provisions in (a) above, and take appropriate information security measures.

(d) When procuring external services, the Information Security Officer shall include the selection criteria and selection conditions of the external service provider, as well as the security requirements specified at the time of selection of the external service, in the procurement specifications and contracts.

(e) The Information Security Officer shall select external services after confirming that the risk of using the service is acceptable based on the conditions of service provision, etc., and take appropriate information security measures, even if the service will not handle confidential information.

(f) The Information Security Officer shall check the contents of use and inspection items in accordance with the separately specified procedures, consult with the section in charge of general information security about the use of external services before giving permission to the user, and register the application with the section in charge of general information security after giving permission to the

user.

10.3. Measures for using cloud services

(a) The section in charge of general information security shall formulate requirements and procedures for information security measures for handling information of RIKEN through cloud services (that are provided through a model of accessing scalable, flexible, and sharable physical or virtual resources that can be shared via a network; using an interface defined by the operator; and where the resources can be freely configured and managed by the user, with sufficient room for setting conditions regarding information security)

(b) Information Security Officers shall designate a system administrator for each cloud service within the division/section/office or equivalent under their jurisdiction in order to supervise the use of the service.

(c) If it is necessary to handle the information of RIKEN on a cloud service, the Information Security Officer shall confirm the contents of use and inspection items according to the separately specified procedures, consult with the section in charge of general information security before granting permission to the user to use the cloud service, and register the application with the section in charge of general information security after granting permission to the user.

(d) If RIKEN's information is used with cloud services, users should comply with the procedures in paragraph (a) and the information's handling restrictions.

Chapter 11. Information System Lifecycles

11.1. Maintenance of information system inventories

(a) The section in charge of general information security shall establish procedures for all information systems to register and operate an information system inventory for matters pertaining to the security requirements of the information systems.

(b) The Information System Administrators shall maintain the information system inventory by utilizing or modifying the inventory in accordance with the procedures set forth in the preceding paragraph.

(c) The Information System Administrators shall record the necessary matters in the information system inventory when newly constructing, updating, or modifying an information system.

(d) Information Security Officers shall maintain the information system inventory and monitor the operation status of information systems within their jurisdiction.

(e) The section in charge of general information security may request sharing of the information system inventory.

11.2. Establishment of measures for information system lifecycles

The Chief Information Officer (hereinafter referred to as "CIO") and the CISO shall establish a system to maintain information security through the entire lifecycle of information systems concerning procurement, construction, and operation.

11.3. Procurement and construction of information systems

(a) The section in charge of general information security shall formulate the procedures for procurement and construction of information systems in RIKEN as necessary, and establish selection criteria for devices, etc.

(b) Information Security Officers and Information System Administrators shall comply with the procedures set forth in the preceding paragraph when procuring and constructing information systems.

11.4. Operation of information systems

(a) The Information System Administrators shall maintain the information security functions of information systems and operate them appropriately.

(b) The Information System Administrators shall store and manage records of operation, such as information system logs within their jurisdiction.

(c) The Information System Administrators shall disclose records of configuration, logs, and operations of information systems upon CSIRT's request.

11.5. Update and disposal of information systems

(a) When updating information systems, the Information System Administrators shall take the necessary information security measures, based on the classification and handling restrictions of the information handled by the systems.

(b) When disposing of information systems, the Information System Administrators shall erase unnecessary information and confirm deletion of the information, based on the classification and handling restrictions of the information handled by the systems.

11.6. Review of information security measures

The Information System Administrators shall regularly inspect and review information security measures for information systems within their jurisdiction, based on the status of information security and knowledge obtained by operation and monitoringof said systems.

11.7. Operational continuity plan of information systems

(a) The section in charge of general information security, Group Information Security Officers, and Information Security Officers shall examine operational continuity of the information systems which support emergency priority business at RIKEN and take measures for said systems as necessary.

(b) The section in charge of general information security, Group Information Security Officers, and Information Security Officers shall regularly conduct trainings and inspections of information security measures regarding major information systems that support the emergency priority business set forth in the preceding paragraph.

Chapter 12. Information System Security Requirements

12.1. User authentication function

(a) A user authentication function shall be used to identify users who have access rights to information or information systems. In doing so, measures must be taken to prevent unauthorized access by impersonating users with access rights or exploiting system vulnerabilities.

(b) In information systems that perform user authentication, measures must be taken to detect or prevent unauthorized logins in order to prevent fraudulent conduct due to the leakage of information on user authentication.

(c) Measures must be taken to properly assign and manage identification codes and information on user authentication.

(d) The section in charge of general information security must establish a policy for the management and operation of authentication data in the basic services related to information and personnel management that confirms the identity of the individual (hereinafter referred to as “authentication”), which are used by RIKEN employees and relevant personnel to use information services provided by RIKEN, and must show the policy to the person in charge of the information systems related to the information services provided by RIKEN.

12.2. Countermeasures for information security threats

(a) The section in charge of general information security shall establish procedures to take measures against software vulnerabilities, malware, denial-of-service attacks, and targeted attacks.

(b) Information systems that are not protected against malware must not handle RIKEN's information and must not be connected to RIKEN's network.

(c) If it is recognized that an information system may have been infected with malware, the information system must be promptly disconnected from the network, and the procedures described in Article 6.3 "Response to information security incidents" must be followed.

12.3. Measures when using encryption and electronic signatures

(a) The section in charge of general information security shall establish procedures for encryption and cryptographic key management, which are required to handle information that requires confidentiality and integrity.

(b) When encrypting information or attaching digital signatures to information, the procedures prescribed in the preceding paragraph shall be followed as necessary.

(c) For cryptographic keys used for decrypting encrypted information and for digital signatures, the cryptographic key management procedures in the paragraph (a) shall be followed as necessary.

Chapter 13. Components of Information Systems

13.1. Terminals and server devices, etc.

(a) For terminals and servers that handle information requiring protection, measures shall be implemented against physical threats such as theft, unauthorized removal of terminals or display devices, unauthorized operation by third parties, shoulder surfing of display devices, etc., and against vulnerabilities that are exploited by malware.

(b) For multifunction devices and special-purpose equipment (IoT devices), security requirements shall be clarified at the time of purchase, and information security measures such as appropriate settings and data deletion after the end of use shall be taken.

13.2. Email, websites, etc.

When using email, websites, Domain Name System (DNS), or databases to send and receive data, measures shall be taken to protect confidentiality against fraudulent use of email including information leakage through inappropriate use and spoofing by malicious third parties.

13.3. Communication lines

When installing and operating communication lines and communication line devices that connect to the relevant server equipment and terminals of RIKEN, any probable risks in information security must be taken into account, depending on the entity operating the communication lines or the type of physical lines.

Chapter 14. Use of Information Systems

14.1. Procedures for use of information systems

(a) The section in charge of general information security shall examine the requirements of information security concerning the use of information systems and establish procedures as necessary.

(b) Users shall comply with the Regulations for Information Security, the Standards for Information Security, and procedures set forth in the preceding paragraph when using information systems.

14.2. Basic measures for the use of information systems

(a) Users must not use information systems for purposes other than business of and permitted by RIKEN.

(b) Users must obtain permission from the Information Security Officer when using external information systems for RIKEN’s business and when handling RIKEN's information on external information systems.

(c) Users must obtain permission from the Information Security Officer when an external information system is brought into a management area and connected to RIKEN’s network.

(d) Users shall not connect information systems to communication lines other than those authorized by Information Security Officers.

(e) Users must not use any software prohibited by RIKEN on information systems or on external

information systems used for business. If it's requiredto use such prohibited software for the business of RIKEN, approval must be obtained from the section in charge of general information security.

(f) Users must not take information systems and external electromagnetic media outside of management areas without the approval of Information Security Officers.

(g) Users must comply with the licenses for software and hardware, and any other licenses.

(h) Users must not infringe the copyrights of software or other copyrighted works.

(i) Users must prevent the illegal use and the theft of information by third parties by locking information systems' terminal screens, etc.

(j) Users shall take information security measures such as encryption, password lock, and locking information systems in accordance with the information classification and handling restrictions when using information systems in which confidential information are stored.

(k) Users shall comply with the information security measures set forth in the preceding paragraph, and requirements defined by Information Security Officers, when taking information systems and electromagnetic storage media in which confidential information are recorded outside of management areas.

(l) Information Security Officers shall establish and inform users of the requirements for information security measures when users take confidential information within their jurisdiction out of management areas, and shall oblige all users to comply with them.

14.3. Exceptional assignment of domain names to IP address

(a) When assigning any domain name other than RIKEN domain name (riken.jp/riken.go.jp) to RIKEN's IP address (134.160.0.0/16), users shall follow the procedures set forth in Article 6.2 "Exceptional measures".

(b) When assigning any IP address other than RIKEN's IP address to the RIKEN domain name (riken.jp/riken.go.jp), users shall follow the procedures set forth in Article 6.2 "Exceptional measures".

(c) In both cases of (a) or (b), all users shall comply with the Regulations for Information Security and the Standards for Information Security.

14.4. Use of external storage media

All users shall comply with the following measures when handling confidential information in electromagnetic storagemedia such as USB memory devices, SD cards and external hard disk drives.

- Users shall ensure the safety of electromagnetic media by using anti-virus software, etc.
- Users shall take measures such as encryption and password locking of information.
- Users shall delete information promptly after terminating its intended use in accordance with the proceduresthat make electromagnetic media non-restorable.

14.5. Procedures for the use of external information systems

(a) When a user of the division/section/office or equivalent uses an external information system for

RIKEN business, or handles RIKEN's information using an external information system, the Information Security Officer shall grant permission and register the application with the section in charge of general information security after confirming the contents of the application form provided separately.

(b) Users must not, in principle, store any confidential information of RIKEN in external information systems when using external information systems as described above. In addition, users shall comply with the conditions described in the application form.

(c) The Information Security Officer shall check the permission period and usage status of the external information system, and if any inappropriate usage is found, recommend or instruct the relevant user to make improvements. RIKEN may conduct an inspection of the relevant external information system in order to confirm these conditions.

(d) Any user who has received a recommendation, instruction, etc., as described in the preceding paragraph shall promptly improve the situation. If no improvement is made, RIKEN may quarantine the relevant external information system. RIKEN may also instruct the deletion of inappropriate applications.

14.6. Dissemination of information via social media services

(a) The CISO shall establish, as necessary, requirements and procedures for information security measures for using social media services to disseminate RIKEN's information.

(b) When it is necessary to disseminate information of RIKEN via social media services, the Information Security Officer shall appoint an administrator for each social media service to be used, and have them manage such services.

(c) The Information Security Officer must confirm the contents of use and inspection items in accordance with the separately specified procedures, consult with the section in charge of general information security before granting permission to users to use social media services, and register the use of the social media services with the section in charge of general information security after granting permission to users.

(d) When it is necessary to use social media services to disseminate RIKEN’s information, the procedures stipulated in (a) above and the restrictions on the handling of such information must be observed.

(e) When social media services are used to provide information that requires integrity, such information must also be posted on RIKEN’s website.

14.7. Teleworking

(a) The section in charge of general information security shall develop regulations concerning information security measures for telework, and procedures for the information security measures for telework. In principle, teleworking shall be implemented using terminals provided by RIKEN. However, even when using terminals owned by not RIKEN but the user for teleworking, the above

procedures shall be followed.

(b) The Information Security Officer shall take information security measures so that employees will follow the established procedures, and so that information security will be ensured when they use the environment and terminals necessary for teleworking.

(c) The Information Security Officer shall have employees check the items necessary for information security measures before and after teleworking in accordance with the procedures concerning measures taken at the time of teleworking. Employees shall telework only at their homes or other authorized locations in accordance with the established procedures.