RIKEN
Standards for Information Security

Version 3.0 April 2021

Information Security Committee

Table of contents

Chapter 1. Purpose 1
Chapter 2. Definition of Terms 1
Chapter 3. Classification of Information and Handling Restrictions 2
3.1. Scope of information 2
3.2. Prohibition of use of information other than intended purposes 2
3.3. Classification of information and handling restrictions 2
Chapter 4. Assignment of Management Areas 5
4.1. Class assignment and measures for management areas 5
Chapter 5. Information Handling 6
5.1. Assignment of information classification and handling restrictions 6
5.2. Re-assignment of information classification and handling restrictions 6
5.3. Change of information classification and handling restrictions 6
5.4. Information handling 6
5.5. Storage of information 6
5.6. Provision or disclosure of information 6
5.7. Utilization and so on outside management areas 7
5.8. Deletion of information 7
5.9. Backup of information 7
5.10. Implementation of measures in management areas 7
Chapter 6. Information Security Measures 7
6.1. Operation of information security measures 7
6.2. Exceptional measures 8
6.3. Response to information security incidents 8
Chapter 7. Information Security Education 8
7.1. Establishment of structures for education 8
7.2. Enforcement of education 8
Chapter 8. Self-check 9
8.1. Formulation and implementation of self-check plan 9
8.2. Conducting self-check 9
8.3. Responding to self-check 9
Chapter 9. Information security audit 9
9.1. Formulation of audit plans 9
9.2. Conducting information security audit 10
9.3. Responding to audit results 10
Chapter 10. Outsourcing 10
10.1. Requirements for outsourcing 10
10.2. Use of external services on general terms and conditions 11

10.3. Dissemination of information via social media services....11
10.4. Measures for using cloud services....11
Chapter 11. Construction and Maintenance of Information Systems....12
11.1. Maintenance of information system inventories....12
11.2. Establishment of measures for information system lifecycles....12
11.3. Procurement and construction of information systems....12
11.4. Operation of information systems....12
11.5. Update and disposal of information systems....13
11.6. Review of information security measures....13
11.7. Operational continuity plan of information systems....13
Chapter 12. Use of Information Systems....13
12.1. Procedures for use of information systems....13
12.2. Basic measures for the use of information systems....13
12.3. Measures against computer viruses....14
12.4. Exceptional assignment of domain names to IP address....14
12.5. Use of external storage media....14
12.6. Management of accounts and the entity authentication information....15
12.7. Measures for use of digital signatures....15
12.8. Procedures for the use of external information systems....15
12.9. Authentication data management....16

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).

These Standards for Information Security are formulated by the Information Security Committee (hereinafter referred to as "Committee") to set forth necessary matters and procedures for enforcing the Regulations for Information Security. The Standards are based on the Common Standards for Information Security Measures for Government Agencies and Related Agencies (effective as of July 25, 2018)

Chapter 2. Definition of Terms

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

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

(2) Section, office, etc.: the smallest organizational unit that is set up by each division, concerned with the information security measures

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

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

(5) Users: directors, 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: processing, gathering, accepting and providing information for the benefit of the users

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

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

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

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

(12) Information security: to maintain the secureness of the characteristics given below that are essential attributes for information, information systems and the RIKEN network:

  (a) Confidentiality, to secure a confidentiality to prevent information from accessing the unauthorized individuals

  (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 and the RIKEN network through outflow, leakage, falsification, destruction or interruption of information

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 "Corporate Document" defined in Article 2, paragraph 1 of the Policies for RIKEN Document Management Regulations (October 1, 2003, Reg. No. 29) (hereinafter referred to as "Document Management Regulations"). However, research data, experiment notebooks, etc. that are out of the scope of the "Corporate Documents" in Article 3 shall 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

All users shall assign information classification and handling restrictions in terms of confidentiality, integrity and availability when you utilize information upon approval of the information security officers.

(a) Confidentiality, property that information is not disclosed to unauthorized individuals

Classification		Classification in Government Common Standards	Classification criteria
Confidential information	Top secret	Confidentiality class-3 information	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 labelled 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 labelled as “Confidential” as set forth in Article 26 of the Document Management Regulations.
	Within Division/ Section Information	Confidentiality class-2 information	Information that may contain non-disclosure information under Article 5 of the Administrative Information Disclosure Law, other than Confidentiality class-3 information, which can be known within a division/section, that is not intended to be immediately released to the public.
	Internal Information		Information that may contain non-disclosure information under Article 5 of the Administrative Information Disclosure Law, other than Confidentiality class-3 information, which can be known within RIKEN, that is not intended to be immediately released to the public.
Confidentiality class-1 information		Confidentiality class-1 information	Information other than confidential information

(e.g.) 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, or xx is prohibited during xx period
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 assurance of information and its processes

Classification	Classification criteria
Critical information	Among information handled in RIKEN (except for written information) whose falsification, errors or damages may hamper the proper operations of RIKEN (except for negligible cases).
Not-classified	Information other than critical information (except for written information)

(e.g.) Handling restrictions for integrity

Types of handling restrictions	Specification
Saving period	Stored until mm/yyyy
Storage location	Stored in xx
Rewriting	Rewiring 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 saving period

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

Classification	Classification criteria
Vital information	Among information handled in RIKEN (except for written information) whose disappearance, loss or unavailability may infringe the stable operations of RIKEN (except for negligible cases).
Not-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	Save in xx

Chapter 4. Assignment of Management Areas

4.1. Class assignment and measures for management areas

The divisional 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 "external person(s)") to secure the safety of sections within the jurisdiction, as well as the security of information and information system, 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. The access control to network racks is as well.
class-2	An area that requires measures for information security, such as entry restriction to external 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 an easy entry of external person(s) by doors, etc. Facilities must be locked while employees, etc. are away.

class-1	An area, other than class-2 and class-3 (where entry of external persons is restricted, such as inside of the building)	Areas where employees and authorized external person(s) can enter, such as lobbies, reception rooms and meeting rooms inside the building	No admittance to external person(s) without ID card, etc. at the entrance of the building.
class-0	An area where external person(s) may enter following the entry procedure	Areas where an external person(s) may enter following the entry procedures at the guardhouse, such as RIKEN premises, halls, and cafeteria	Limit the entry to the person(s) who follows the entry procedures at the gatehouse.

Chapter 5. Information Handling

5.1. Assignment of information classification and handling restrictions

Classification and handling restrictions shall be specified to the information which requires handling restrictions in a way other can identify.

5.2. Re-assignment of information classification and handling restrictions

When using (especially process) 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 which originally assigned information classification and handling restrictions.

5.3. Change of information classification and handling restrictions

When changing information classification and handling restrictions, users shall get an approval of the information security officers of the division which 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) Users shall store information with an appropriate access privilege based on handling restrictions.
(b) Users shall formulate requirements for backup, redundancy and storage location against earthquake based on information handling and shall take necessary measures.
(c) Users shall install information systems that handle information based on the handling restrictions for information in a management area.

5.6. Provision or disclosure of information

(a) Users shall provide or disclose information based on handling restrictions.

(b) Users shall ensure that the handling restrictions for the information is observed properly at the receiving party.
(c) Users shall erase unnecessary ancillary information from property, proofreading history, etc. of the information based on handling restrictions upon disclosure or provision.

5.7. Utilization and so on outside management areas

Users who handle information outside management areas by transferring information in mobile terminals, external storage media, via emails, or in files, etc., shall particularly obtain approval of the information security officers and take information security measures by encryption and password lock, based on information handling restrictions and so on.

5.8. Deletion of information

(a) Users shall immediately erase information which is used outside a management area, based on handling restrictions when it becomes unnecessary.
(b) When disposing of an external storage media in which confidence information is stored, users shall erase all stored information making it completely unrestorable.

5.9. Backup of information

(a) Users shall backup information in accordance with the classification and handling restriction of information.
(b) Users shall determine the place, manner, storage period and so on, of the backup information, and appropriately manage it in accordance with the classification and handling restriction of information.
(c) Users shall delete, erase or dispose of the backups beyond the retention period by making it completely unrestorable.

5.10. Implementation of measures in areas requiring control measures

(a) Area information security officers shall ensure users duly understand the classification and the necessarymeasures in the designated management area.
(b) Area information security officers shall devise and implement countermeasures against disaster to protectof information systems in management areas.
(c) Users shall comply with the measures in the management areas.

Chapter 6. Information Security Measures

6.1. Operation of information security measures

(a) The general information security section shall maintain the operational procedures for information security measures at RIKEN.
(b) If the information security officer is informed by a user of tasks and problems related to the Standards and the Procedures for Information Security, the information security officer shall report them to the general information security section.

(c) The general information security section shall examine the report prescribed in the preceding paragraph. If necessary, the general information security section 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 general information security section to take actions over the issues as necessary.

6.2. Exceptional measures

(a) If the operation of Regulations for Information Security, the Standards for Information Security, or the Promotion Plan for Information Security shall hinder the efforts of RIKEN, the institute is able to consult with the general information security section and may apply for exceptional measures as necessary. The CISO shall determine the person who decides whether or not to apply for exceptional measures and the review procedure.

(b) The general information security section shall maintain records of the application of exceptional measures and request the applicants of the exceptional measures to report the status periodically.

6.3. Response to information security incidents

(a) If a user detected or is informed an information security incident, the user shall report following the procedures separately designated and take an 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 and shall respond to the information security incident.

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

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

Chapter 7. Information Security Education

7.1. Establishment of structures for education

(a) The general information security section shall formulate education plans and establish structures for information security education (hereinafter referred to as "Information security education").

(b) The general information security section shall review the education plans appropriately according to the changing environment of information security.

7.2. Enforcement of education

(a) All users of information systems and RIKEN networks must take the information security education immediately after commencing actual work. If the lack of training persists, the CISO shall request the divisional information security officer to make improvements and take necessary measures,

including suspending the use of the laboratory network and information services by the relevant user and division.

(b) The CISO shall ensure CSIRT members to take the required security education as CSIRT members properly.

(c) The general information security section shall inform the implementation status of the information security education to the CISO.

Chapter 8. Self-check

8.1. Formulation and implementation of self-check plan

(a) The general information security section shall formulate and conduct a plan for self-check (hereinafter referred to as "self-check") about the implementation status of information security measures based on the promotion plan, as necessary.

(b) The general information security section shall revise the self-check plan according to changes in the information security environment.

8.2. Conducting self-check

(a) The general information security section shall instruct divisions and departments of RIKEN to conduct self-check in accordance with the self-check plan.

(b) Divisions and departments of RIKEN shall promptly conduct self-check and report the results to the general information security section when they are instructed to conduct self-check.

8.3. Responding to self-check

(a) The general information security section shall collect, analyze and evaluate the self-check results.

(b) The general information security section shall instruct the divisional information security officers and information security officers to correct the problems if serious problems are found through the evaluation of the self-check and report it to the CISO.

(c) The general information security section shall report the results of the analysis and evaluation of self-check to the CISO.

(d) The CISO instruct the general information security section and the divisional information security officers to correct the problems if they are found while evaluating self-check results.

(e) The general information security section and the divisional information security officers shall regularly report the response status of the corrections instructed by the CISO.

(f) The CISO shall review the promotion plan in view of 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 plans for information security audit in accordance with the environment of information security and the promotion plan.

9.2. Conducting information security audit

(a) The chief information security auditor shall conduct an audit relating to the RIKEN information security measures based on the audit implementation plan and shall report the audit result 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) The CISO shall review the Promotion Plan for Information Security should any improvements be deemed necessary as a result of an audit, and shall provide instructions for the general information security section and the divisional information security officers to make improvements as necessary.

(b) The general information security section and the divisional information security officers shall formulate and implement an improvement plan per the instructions and report them to the CISO.

Chapter 10. Outsourcing

10.1. Requirements for outsourcing

(a) The general information security section shall formulate the requirements of information security measures for outsourcing of the construction, operation, and maintenance of information systems or the development and maintenance of application software, as necessary 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 would be vital to receive approval of the information security officers and formulate the requirements for information security measures in contractual documents according to the procedures in the preceding paragraph.

(c) When outsourcing, information security officers shall conduct the outsourcing party to observe the requirements of the information security measures and check their implementation status.

Obtain approval of the information security officer if the outsourcing parties handle confidential information and conduct the outsourcing party to be comply with handling restrictions and to take necessary procedures and information security measures.

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

(e) In case that outsourcing parties will 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 officers shall check the subcontractor’s implementation status.

(f) Information security officers shall ensure an outsourcing party to return or erase information of RIKEN upon the termination of contract, unless otherwise prescribed.

(g) In case that information security officers become aware of or are informed of information security incidents by outsourcing parties, follow the directions in Chapter 6, Article 3 "Response to information security incidents".

10.2. Use of external services on general terms and conditions

(a) The general information security section shall formulate requirements and procedures for information security measures, for handling information of RIKEN in external services other than RIKEN such as emails and storage services, which can be started only by account registration and agreement to terms and conditions, etc., (however, it is unavailable to set sufficient information security conditions in using the information service; hereinafter referred to as "external services on general terms and conditions").

(b) Information security officers shall designate a responsible person in charge of each external services on general terms and conditions in order to supervise it.

(c) The information security officer shall check the contents of use and check list according to the separately specified procedures, consult with the general information security section about the use of external services on general terms and conditions before giving permission to the user, and register the application with the general information security section after giving permission to the user.

(d) To deal with RIKEN information in external services on general terms and conditions, users should comply with the procedures in paragraph (a) and handling restrictions of the said information.

10.3. Dissemination of information via social media services

(a) The CISO shall formulate information security requirements and procedures for dissemination of RIKEN information via social media services, as necessary.

(b) Information security officer shall designate a system administrator for each social media service to be used and have this person supervise the use of social media when information needs to be released to the public.

(c) The information security officer shall check the contents of use and inspection items according to the procedures specified separately, consult with the general information security section before giving permission to users for the use of social media services, and register the application with the general information security section after giving permission to users.

(d) To disseminate RIKEN information via social media services, users should comply with the procedures in paragraph (a) and the handling restrictions for the said information.

(e) If social media services are used for dissemination of information that requires integrity, same information should also be posted on the RIKEN website.

10.4. Measures for using cloud services

(a) The general information security section shall formulate requirements and procedures for information security measures for handling information of RIKEN through a service that does not need purchase of hardware, licenses, etc. providing environment and infrastructure for developing software and applications on the internet as necessary (though it is flexible about setting of information security conditions adequately; hereinafter referred to as "Cloud service").

(b) Information security officers shall designate a system administrator for a cloud service within the

jurisdictionin order to supervise the use of the service.

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

(d) If RIKEN information is used by cloud service, users should comply with the procedures in paragraph (a) and handling restrictions for the said information.

Chapter 11. Construction and Maintenance of Information Systems

11.1. Maintenance of information system inventories

(a) The general information security section shall define the format of inventories which describe system configurations, OS, installed software, information security requirements, and information security measures of information systems as services, as necessary.

(b) The information system administrators shall maintain the information system inventories by utilizing or modifying the formats set forth in the preceding paragraph as necessary.

(c) The information system administrators shall record the necessary matters in the information system inventories when newly constructing, updating or modifying an information system.

(d) Information security officers shall maintain the information system inventories and monitor the operation status of information systems within the jurisdiction.

(e) The general information security section may request sharing the information system inventories.

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 general information security section shall formulate the procedures for procurement and construction of information systems in RIKEN as necessary.

(b) Information security officers and information system administrator 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 the jurisdiction.

(c) The information system administrators shall disclose records of configuration, logs and operations of information systems upon request of CSIRT.

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 information classification and handling restrictions stored in said systems.

(b) When disposing information systems, the information system administrators shall erase unnecessary information and confirm deletion of the information based on information classification and handling restrictions stored in said systems.

11.6. Review of information security measures

The information system administrators shall regularly check and review information security measures for information systems within the jurisdiction, according to the knowledge obtained by operation and monitoring of said systems.

11.7. Operational continuity plan of information systems

(a) The general information security section, divisional information security officers and information security officers shall examine operational continuity of the information systems which support the highly prioritized tasks during emergencies at RIKEN and take the measures for said system as necessary.

(b) The general information security section, divisional information security officers and information security officers shall conduct trainings and reviews of information security measures for emergencies set forth in the preceding paragraph.

Chapter 12. Use of Information Systems

12.1. Procedures for use of information systems

(a) The general information security section 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, the Standards, the Implementation Procedures for Information Security and procedures set forth in the preceding paragraph when using information systems.

12.2. Basic measures for the use of information systems

(a) Users shall not use information systems other than efforts of and permitted by RIKEN.

(b) Users must obtain permission from the information security officer when using the external information system for RIKEN’s efforts or when handling RIKEN's information on the external information system.

(c) Users must obtain permission from the information security officer when an external information system is brought into an areas requiring control measures 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 shall not use any software prohibited to use on information systems by RIKEN or on the external system for business. If it's required to use such prohibited software for the task of RIKEN, an approval from the general information security section shall be granted.

(f) Users shall not take information systems and external electromagnetic media outside of the management areas without approval of information security officers.

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

(h) Users shall not infringe the rights of software and other works.

(i) Users shall protect the information systems from the illegal use and the theft by third parties, by locking the terminal screen and so on.

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

(k) Users s shall comply with the information security measures set forth in the preceding paragraph and requirements defined by information security officers when users take the information systems and electromagnetic storage media outside management areas, in which confidential information are stored.

(l) Information security officers shall formulate the requirements of information security measures in case that users take out confidential information within the jurisdiction from management area and inform them, make all users comply with them.

12.3. Measures against computer viruses

(a) The general information security section shall instruct users to take measures against virus on information systems.

(b) Users shall not use or connect information systems to RIKEN network without virus protection to handle RIKEN information.

(c) If a user becomes aware that an information system could have been infected by malware, follow the procedures in Article 6.3 "Response to information security incidents" after implementing measures like disconnecting the infected information system from the network immediately.

12.4. 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 the IP address of RIKEN (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 IP address to 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 Standards for Information Security.

12.5. Use of external storage media

All users shall comply with the following measures when handling confidential information in external storage media such as USB memories, 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 according to the procedures that make electromagnetic media non-restorable.

12.6. Management of accounts and the entity authentication information

(a) Users shall not use the information system with account other than the ones information system administrator assigned to them.

(b) Users shall take information security measures for the assigned account and entity authentication information such as passwords.

(c) Users shall use administrator accounts only for management work of information systems.

(d) Information security officers shall formulate the requirements for information security measures for administrator accounts and implement said measures.

12.7. Measures for use of digital signatures

(a) The general information security section shall formulate procedures for encryption and cryptographic key management that are required to handle credential information and critical information.

(b) Users shall follow the procedures set forth in the preceding paragraph as necessary when encrypting information or granting digital signatures to information.

(c) Users shall follow the procedures of cryptographic key management set forth in paragraph (a) as necessary to manage keys for decryption of encrypted information and for granting digital signatures.

12.8. Procedures for the use of external information systems

(a) When a user of the division uses the external information system for RIKEN efforts, or handles RIKEN's information using the external information system, the information security officer shall grant permission and register the application with the general information security section after confirming the contents of the application form provided separately.

(b) Users shall not, in principle, store any confidential information of RIKEN in the external information system when using the external information system 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.

12.9. Authentication data management

(a) The general information security section shall establish a policy for the management and operation of the authentication data in the infrastructure service for information and human management to verify (“authenticate”) the identity of RIKEN officers and employees and those who have a certain relationship with RIKEN when they use the information service provided by the institute. The policy shall be presented to the administrator of the information system pertaining to the information services provided by RIKEN.

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 x 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”