

(Note: the Japanese version is the original. The English version is provided as a translation of the content of the Japanese version for the user's convenience.)

## Rules of Use for the SPring-8 and SACLA Data Centers

1<sup>st</sup> edition

January 14, 2022

SPring-8 Data and Network Committee

### 1. Purpose

These rules have been compiled by the SPring-8 Data and Network Committee (hereinafter the “Committee”), based on the “Management Regulations for Public Experiment Data Systems and Public Experiment Networks at SPring-8/SACLA” (hereinafter the “Regulations”), and provide the necessary conditions concerning the use of the SPring-8 Data Center and the SACLA Data Center. These Data Centers are part of Public Experiment Data Systems described in the “Basic policy for Public Experiment Data System and Public Experiment Networks at SPring-8/SACLA”.

### 2. Applicability

These rules are applicable to all persons connected to the use of the Data Centers (hereinafter “Users”), operation supervisors defined in Item 3 of the Regulations (hereinafter “Operation Supervisor”), and operation managers defined in Item 4 of the Regulations (hereinafter “Operation Managers”).

### 3. Users

A User is defined in Item 5 of the Regulations and has the qualifications specified in Item 4 to use the Data Centers.

### 4. Usage Qualifications

A person is permitted to use the Data Centers if they are any of the following:

1. A project member of an approved proposal at SPring-8/SACLA.
2. A collaborator of 1., and someone who partakes in research data analysis.
3. A person specially approved by the Operation Supervisor.
4. Facility staff assigned to maintain or improve the functionality of the Data Centers.

#### 5. Usage Approval

In order for a person to use the Data Centers, they must file an application to the Operation Supervisor and receive approval. The format of the application is decided by the Operation Supervisor. However, Users that fall under Case 4 in Item 4 are exempt from this rule.

#### 6. Period of Validity of the User's Account

The period of validity of the User's account is 3 years. Users who are qualified as described in Rule 4 can submit an extension application. If the Operation Supervisor approves the extension, the User's period of validity will be extended by 3 years.

#### 7. Account and Password Management

1)

Users are solely responsible for properly managing their accounts, as well as the passwords to the accounts. They must also be cautious with and prevent misuse of their accounts.

2)

Users shall not, under any circumstances, transfer or lend their account or password to anyone else.

3)

The Operation Supervisor and the Operation Manager will regard any activity of a user account, which has been logged in through normal authentication procedures, as an act by the User who owns that relevant user account.

#### 8. Usage Fee

Usage fee amounts are established in the separate detailed rules.

## 9. Data Retention

Users who have stored data in the Data Centers must abide by the “Experimental Data Retention Policy of Public Experiment Data Systems at SPring-8/SACLA”.

## 10. Data Backups

The Operation Manager will not create any backups of Users’ data. The creation of data backups is the responsibility of the User.

## 11. Prohibited Activity

Users shall not commit any of the following:

1. Actions that hinder the operation of the Data Centers or other equipment at SPring-8/SACLA.
2. Actions that store data irrelevant to the experiments pertaining to SPring-8/SACLA.
3. Actions that violate intellectual property rights (copyrights, trademark rights, etc.) of another person or entity.
4. Actions that damage material assets or compromise the reputation of another person or entity.
5. Actions that allow other individuals, whether approved Users or not, to access and use the Data Centers using the User’s connection credentials.
6. Actions that concern faking the identity of another User in order to access and use the Data Centers.
7. Any form of scam or illicit activity.
8. Sending or storing any harmful program or virus.
9. Any activity that is against public policy.
10. Any other illegal activity.

## 12. User’s responsibilities

1)

Users connecting to the Data Centers must obey these Rules.

2)

Users who become aware of any prohibited activity as described in Item 11 conducted by other User, or who have suspicions about other Users being engaged in such activities, must immediately notify the Operation Manager via the contact desk.

#### 13. Notifiable issues

Users must immediately notify the Operation Manager of any change in the notice issued at the time of account creation, as well as in the case of account suspension or closure.

#### 14. Revocation of Usage Approval

1)

If there is deemed to be an issue in the use of the Data Centers by a User, the Operation Manager may give instructions to the User for correcting the issue.

2)

If the User does not follow the instructions, or if the User falls under any of the cases below, the Operation Managers may at any point suspend the User's account or carry out any appropriate measures. This may be done without notifying the User.

1. If the User has lost the qualifications described in Item 4.
2. If it is found that the User committed a prohibited activity described in Item 11, or if the Operation Manager suspects the possibility of such activity.
3. If the Operation Manager suspects that the User neglected the responsibilities stated in Item 12.
4. If the User has failed to notify the Operation Manager as described in Item 13.

#### 15. Exemption from Responsibility

1)

The Operation Manager works to maintain stable operations for the Data Centers, but there may be instances of downtime or delay, as well as destruction or partial damage to data, caused by malfunctioning or damage to networking cables or devices, computers, storage devices etc., which the Operation Manager cannot predict or prevent. The Operation Manager and the Operation Supervisor shall be exempt from taking responsibility and not liable for damage or losses incurred by damage to the Data Centers, damages or data loss associated with a User's own negligence, or as a result of the User being involved in any of the prohibited actions listed in Item 11, or any other kind of damages in relation to the Data Centers; from default on a

debt; from criminal liability and/or compensation, regardless of the claimed reason; and from any related dispute.

2)

While providing the services of the Data Centers, the Operation Manager and the Operation Supervisor shall provide means to encrypt the communication path between the system and the User and establish an authentication mechanism to ensure that data is protected within reasonable expectations; although they strive to prevent data leaks and falsification, they do not bear any responsibility or burden for loss or damage related to compromised data, data leakage, data falsification, etc., due to unauthorized access or hacking by a third party.

#### 16. Notifications

Notifications from the Operation Manager to the User will be posted on the official website or sent by e-mail, at which point the notification process is finalized.

#### 17. Contact Desk

A contact desk will be in operation for any inquiries or notifications from the User to the Operation Manager.

#### 18. Revision of the Rules

The Committee holds the right to revise the current guidelines, in response to any changes in the administrative oversight of SPring-8/SACLA.