(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.)

Security Standards (Network Guidelines) for Public Experiment Networks at SPring–8/SACLA

1st edition
October 30, 2020
SPring–8 Data and Network Committee

1. Purpose

These guidelines 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 principles to be strictly followed while using Public Experiment Networks at SPring-8/SACLA.

(Principles to be followed by the Operation Supervisor)

2. System of Operation

The Operation Supervisor must establish a management organization for Public Experiment Networks and appropriately direct and supervise the Operation Managers.

3. Response to Cyber Security Incidents

The Operation Supervisor must establish a cyber security incident response team.

4. Instructions to Users

The Operation Supervisor must give appropriate instructions to Users and System Administrators so that cyber security in Public Experiment Networks can be properly maintained.

5. Auditing Computers

1)
The Operation Supervisor can audit devices connected to Public Experiment Networks.
2)
The timing and items to be audited are determined in consultation with the System Administrator, taking into consideration the importance (confidentiality, integrity, availability) of the relevant device(s).

6. Establishment and Revision of Detailed Rules

1)
The Operation Supervisor must establish detailed rules that Users must comply with while using Public Experiment Networks.
2)
The Operation Supervisor must periodically review the detailed rules and make rational amendments according to the needs of Public Experiment Networks when necessary.
3)
Any revision or amendment of the detailed rules must be reported to the Committee.
4)
The detailed regulations will be released after a certain period of time to inform the Users and System Administrators.

(Principles to be followed by Users)

7. Purpose of Use

1)
Users can use Public Experiment Networks for research and related purposes.
2)
Services that can be used on Public Experiment Networks will be individually determined from a security point of view. Details are defined in the detailed rules established by the Operation Supervisor.

8. Authority of the Operation Supervisor

1)
When using Public Experiment Networks, the User must follow the instructions of the Operation Supervisor.
2)
If the User violates the instructions of the Operation Supervisor, the Operation Supervisor can revoke the permission to use Public Experiment Networks.

9. Cyber Security

1)
The User must follow standard security protocols when using Public Experiment Networks.
2)
Operating systems and other software on the computers must use versions which are currently supported by the manufacturer/developer.
3)
If it is unavoidable that the above items cannot be followed, the instructions of the Operation Supervisor must be followed.

10. Password Management

The User must not use the same authentication credentials (password, etc.) on multiple systems or services for Public Experiment Networks.

11. Continuously Connected Server Computers

For the purpose of research activities, the User can connect a server computer to Public Experiment Networks.

12. Establishing the System Administrator

The User must have a System Administrator for the server computer that connects to Public Experiment Networks.

(Principles to be followed by the System Administrators)

13. Notifications

1)
System Administrators must pay special attention to the cyber security of computer systems.
2)
System Administrators must take appropriate measures against unauthorized use of computer systems, including the specific measures described in the detailed rules.

14. Account Management

1)
System Administrators must appropriately set up and manage accounts such as authentication and authorization on computer systems.
2)
User accounts and System Administrator accounts must be separate.
3)
System Administrators must consider employing multi-factor authentication on computer systems, depending on the importance of services.

15. Logging

1)
According to the importance both of functions and of services, System Administrators must record operation history (logs), which are necessary for investigating the cause of security incidents.
2)
System Administrators must check the logs on the computer system on a daily basis to confirm that there have been no problems or suspicious behavior.
3)
System Administrators must retain computer system logs for at least six months.