(Disclaimer: English version here is provided as a translation of the original Japanese version for the readers' convenience.)

2018.12.13

High Energy Accelerator Research Organization Information Security Regulations

Article 1　(Purpose)

The High Energy Accelerator Research Organization (hereinafter referred to as the "KEK") supports the number of research and education activities both in Japan and overseas, and these activities rely on various Information assets.

It is indispensable for the research and education activities in KEK to utilize information assets. Therefore, it is essential to ensure information security in KEK, keeping with usability, in responding public trust including that from universities and research institutes in and outside of Japan.

These regulations aim at the smooth operation of KEK by establishing rules for information security management and information assets utilization.

Article 2 (Definition of terms)

In these regulations, the following terms are defined as follows;

(1) "Information" means information recorded inside information systems, electromagnetic storages media outside information systems, or any other descriptions on the information systems. Unless otherwise specified it is what KEK owns and manages.

(2) "Information system" means a system used for information processing and communication which consists of hardware, software, networks, and storage media.

(3) "Information assets" means both of "Information" (above (1)) and "Information system" (above (2)).

(4) "Confidentiality" is an attribution of the information that only authorized persons should be able to access.

(5) "Integrity" is an attribution of the information that should not be destroyed, altered or erased.

(6) "Availability" is an attribution of the information that should be ensuring the condition where information and relevant information assets can be accessed by authorized persons without interruption, whenever they are needed to access.

(7) Information security" means maintaining confidentiality, integrity, and availability of information assets.

(8) "Information security incident" means a threatening event against the information

security in KEK.

(9) "Information security-related rules" means the general term for all of the rules outlined in these regulations or derivative regulations.

(10) "Information security measures" means everything to ensure information security.

(11) "Temporary visitors" means persons who are temporarily permitted to use restricted information assets of KEK.

(12) "Information system users" means persons who are permitted to use the information assets of KEK (excluding Temporary visitors).

(13) "Information assets managed by J-PARC Center" means information assets managed in compliance with the information security policy of J-PARC Center.

Article 3 (Scope)

These regulations apply to information assets managed (including leasing and safekeeping) by KEK and apply to Information system users and Temporary visitors.

2 These regulations do not apply to Information assets managed by J-PARC Center.

3 All devices even managed by other than KEK (including Information systems managed by J-PARC Center) connected to the information system of KEK are subjects of these regulations.

(Basic Policy)

Article 4

KEK shall establish the following policy to achieve the purpose of Article 1

(1) Establishment of responsible organizations

KEK shall establish responsible organizations to ensure information security.

(2) Implementation of measures based on risk assessment

KEK shall implement Information security measures after evaluating risk assessment of information security in KEK, establishing plans and Information security related-rules. KEK shall review them in the case that the evaluation is changed.

(3) Education

KEK shall regularly educate Information system users on the Information security to increase the effectiveness of the Information security measures.

(4) Self-check and Audit

KEK shall conduct self-checking and audits on information security to ensure and verify the Information security measures are functioning effectively.

(5) Response to Information security incidents

In the case of the Information security incident, KEK shall response properly in accordance with the pre-defined organization and measures. KEK shall protect internal

and external information assets.

(Chief Information Security Officer)
Article 5
KEK shall appoint the Chief Information Security Officer (hereinafter referred to as the "CISO").
2 Executive Director in charge of information management shall be assigned to be CISO.
3 CISO shall have overall decision-making role and responsibility for the Information security in KEK.
4 CISO may delegate some part of CISO work to others who are assigned separately.

(Information Security Committee)
Article 6
KEK shall establish the Information Security Committee (hereinafter referred to as the "Committee") in KEK.
2 The organization of the Committee shall be specified separately.
3 The Committee shall discuss the following matters as the highest decision-making committee about the Information security in KEK.
(1) Formulation and operation for the Information security regulations and standards for the Information security measures.
(2) Important decisions on the plans, implementation, auditing, and reviewing that are necessary for ensuring information security.
(3) Decisions on any other basic items for the Information security.
4. Other necessary matters with respect to the Committee shall be determined separately.

(Information Security Auditor)
Article 7
KEK shall establish the Information Security Auditor (hereinafter referred to as the "ISA").
2 Director General of KEK shall appoint ISA.
3 ISA shall oversee audits of the Information security of KEK in necessary ways such as verifying the status of compliance with the Information security related-rules and law.

(Head of Information Security Officers)
Article 8
KEK shall establish Head of Information Security Officers (hereinafter referred to as "HISO").
2. CISO shall appoint HISO.

3. HISO shall oversee the implementation of the Information security measures in KEK.

（Information Security Officer） 用語要確認
Article 9
Information Security Officer (hereinafter referred to as "ISO") shall be established in the following departments.
2 ISO of each department shall be assigned as follows;
(1) ISO of Institute of Particle and Nuclear Studies shall be Director of the institute.
ISO of Institute of Materials Structure Science shall be Director of the institute.
(2) ISO of Accelerator Laboratory shall be Directors of the laboratory.
ISO of Applied Research Laboratory shall be Directors of the laboratory.
(3) ISO of Department of Advanced Accelerator Technologies shall be Directors of the department.
(4) ISO of Public Relations Department and that of offices stipulated in Article 7 of KEK organization regulations shall be Director of Public Relations Department.
(5) ISO of Research Administration Department shall be Director of the department.
(6) ISO of Administration Bureau shall be Secretary General of the bureau.
(7) ISO of Others shall be HISO.
3. ISO shall oversee and have responsibility for implementation of the Information security measures for each department under the control of HISO.
4. ISO may delegate some part of her/his work to others who are assigned separately.

(Chief Information Security Advisor)
Article 10
KEK shall establish Chief Information Security Advisor (hereinafter referred to as "CISA").
2 CISA shall be appointed by CISO from persons with expertise and experience on the Information security
3 From her/his professional point of view, CISA may provide advice on Information security measures of KEK to CISO.

(Computer Security Incident Response Team: KEK CSIRT)
Article 11
KEK shall establish Computer Security Incident Response Team (hereinafter referred to as "KEK CSIRT").
2 KEK Computing Research Center shall be engaged for the main work of KEK CSIRT.
3 KEK CSIRT shall serve as an emergency contact from inside and outside of KEK for the

Information security incident. In the case of the Information security incident, KEK CSIRT shall take actions for the prevention of damage enlargement and provide technical supports for the service recovery of the relevant Information systems.

(Risk assessment)
Article 12
According to the result of self-checking and audits described in Article 17 and 18, respectively, CISO shall regularly derive the risk of threat and actual damage for the KEK possessed Information and Information systems.

(Basic Plan for Information Security Measures)
Article 13
CISO shall establish KEK basic plan for the Information security measures (hereinafter referred to as "Basic plan").

(Information Security Standards for Countermeasure)
Article 14
CISO shall establish Information Security Standards for Countermeasure (hereinafter referred to as “Countermeasure Standard”) based on the result of risk assessment by consulting with the Information Security Committee.
The Countermeasure Standards shall uniformly define standards of conduct and judgement criterion for the Information security measures. CISO shall revise Information Security Standards as necessary.

(Implementation of Information Security Measures)
Article 15
HISO and ISO shall implement Information security measures in accordance with the Countermeasure Standards.

(Education)
Article 16
HISO and ISO shall provide training on the Information security to Information system users and Temporary visitors in order to cultivate their better understandings of the Information security-related rules.

(Self-checking)

Article 17
HISO and ISO shall conduct the self-checking performed by the Information system users for the Information security measures in order to understand the status of compliance with the Countermeasure Standards.

(Audit)
Article 18
ISA shall conduct an audit in order to verify the status of compliance with the Information security-related rules and law.

(Response to Information security incidents)
Article 19
In order to deal with the Information security incident, HISO shall establish an appropriate framework and necessary procedures in advance.
2 A person who has recognized the suspicions of the Information security incident shall perform the actions specified by HISO as described in the preceding paragraph of Article 19.

(Monitor of communication)
Article 20
CISO and HISO may monitor any communications through the communication lines of KEK. However, the information obtained by the monitoring is allowed to utilize only for the purposes of the Information security measures or communication failure analysis.
2 ISO of each department may monitor communications related to the department affairs through the communication lines of KEK. However, the information obtained by the monitoring is allowed to utilize only for the purposes of the Information security measures or communication failure analysis.

(Responsibilities of Information system users and Temporary visitors)
Article 21
The Information system users and Temporary visitors shall be aware of the common importance of the Information security and shall comply with the Information security-related rules and law.
2 Staff of KEK shall make an effort for the Information system users other than KEK staff and Temporary visitors to be able to comply with the Information security-related rules and law.

(Exceptions)

Article 22

The Information system users may apply to CISO for an application of exception in accordance with the procedures separately stipulated if it is significantly difficult for the user to comply with the Information security-related rules for accomplishing their work in KEK.

(Miscellaneous provisions)

Article 23

Other necessary matters, which is not provided in these Regulations, for the Information security in KEK may be separately provided.