Basic Regulations Concerning Information Security Measures of the Public University Corporation, the University of Aizu

(Apirl 1, 2021, Regulation No. 1)

Article One

(Purpose)

1.1 The purpose of these regulations shall be to provide for basic matters concerning information security measures for information and information systems at the Public University Corporation, the University of Aizu (hereinafter, the UoA) in order to facilitate the protection and utilization of the information owned by the UoA as well as the maintainance and improvement of the information security standards provided for in the Basic Policy on Information Security Measures of the University.

Article Two

(Scope of Application)

2.1 These regulations shall apply to individuals who operate and manage the information systems of the UoA as well as regular and temporary users of the systems.

2.2 Information subject to these regulations shall be as follows.

1) Information recorded in information / telecommunication systems or in external electromagnetic recording media (including information in documents output from said information systems and information input from documents into said information systems) procured or developed by the UoA for faculty, administrative staff, etc. to use in their work

2) Other information recorded in information systems or external electromagnetic recording media (including information in documents output from said information systems and information input from documents into said information systems) and handled by faculty, administrative staff, etc. in their work

3) Information concerning the design and operational management of information systems procured or developed by the UoA

2.3 The information systems subject to these regulations shall be all of those that handle information subject to these regulations.

2.4 Regardless of the provisions of the preceding paragraphs 1 to 3, information and information systems subject to the UoA Revitalization Center infomraiton security policies such as the UoA Revitaliation Center ISMS shall not be subject to these regulations.

However, information and information systems that are subject to the UoA Revitalization Center ISMS and connected to the University of Aizu Information Network System provided for in the University Regulation on the Use of the Information Processing Center (the University of Aizu Information Systems and Technology Center) shall be subject to the regulations.

Article Three

(Definition)

3.1 For the purpose of this regulation, the terms set forth below shall be defined as follows:

1) Information

This refers to information provided for in Article 2.2 of the regulations.

2) Information System

This refers to information systems that are comprised of hardware and software and are used for information processing and/or telecommunication procured, developed, or used by the UoA (including those managed by contractors) or connected to the information network of the UoA unless otherwise noted.

3) Important Information System

This refers to the information systems of the UoA that serves as part of its informationinfrastructure for which it is considered an information security breach would have a major impact.

4) Information Security Policies

This refers to both the Basic Policy on Information Security Measures of the Public University Corporation, the University of Aizu and these regulations established by the UoA.

5) Regulations Related to Information Security.

This is a general term for regulations, standards, and plans formulated based on the information security policies.

6) Security Standards

This refers to the Information Security Standards of the Public University Corporation, the University of Aizu formulated by the UoA and any related standards to which said security standards refer.

7) Implementation Procedure

This refers to the detailed procedures that must be specified in advance in order to apply measures provided for in the security standards to individual information systems and tasks.

8) Device, etc.

This is a general term for information system components (servers, terminals, telecommunication circuit devices, multifunctional printers, devices and equipment with a specific use, software and other devices), external electromagnetic recording media, etc.

9) Recording Medium

This refers to tangible objects within which information is recorded and entered which include:

-Paper and other tangible objects which include information that can be perceived by humans such as letters and shapes (hereinafter, Documents)

-Recording devices for records created in electronic, magnetic, or other forms that cannot be percepted by humans used for processing information through information systems (hereinafter, Electromagnetic Records and Electromagnetic Recording Media)

Electromagnetic Recording Media include internal Electromagnetic Recording Media built in servers, terminals, telecommunications circuit devices, etc. and external Electromagnetic Recording Media such as USB flash drives, portable hard drives, and DVD recorders

10) Server

This refers to information system component devices that retain services and provide said services to terminals connected to thereto via telecommunication circuits, etc. (including software

installed on said devices and those directly connected to and considered to be an integral part of said devices such as keyboards and mice) that are, unless otherwise noted, procured, developed, or used by the UoA (including systems managed by vendors).

11) Terminal

This refers to information system component devices directly used by users for processing information (including software installed on said devices and those directly connected to and considered to be an integral part of said devices such as keyboards and mice) that are, unless otherwise noted, procured or developed by the UoA or those not provided by the UoA. They also include mobile terminals.

12) Mobile Terminals

This refers to any form of devices designed to be used on the move as needed.

13) Telecommunications Circuit

This refers to systems for sending and receiving information between the UoA's information systems or devices, etc. (including those not procured, etc. by the UoA) and, unless otherwise noted, is a general term for telecommunication circuits regardless of types (including wired, wireless, physical and virtual telecommunications circuits) including those not directly managed by the UoA.

14) Telecommunications Circuit Device

This refers to devices installed for the purpose of connecting telecommunications circuits or connecting telecommunications circuits to information systems in order to, among other things, control information to be sent and received via the telecommunications circuits. It includes hubs, switches, routers, and firewalls.

15) Information Networks

This refers to any network comprised of the UoA's information systems, devices, and telecommunications circuits.

16) Department, Division, and Center

The definition of these terms within the UoA shall be defined as follows.

a. The University of Aizu (Administration)
b. The University of Aizu (Education)
c. The University of Aizu (Research)
d. University-Business Innovation Center (UBIC)
e. Revitalization Center (LICTiA)
f. The University of Aizu Junior College Division (JCD)

17) Department, Division, or Center Executive Administrator

This refers to the individual who supervises administrative affairs related to information security measures in each Department, Division, or Center.

18) Information Security Measure Promotion System

This refers to the system established to perform duties related to the promotion of the information security measures of the UoA.

19) Students, Etc.

This refers to undergraduate students, graduate students, non-degree students, research

students, special audit students, exchange students provided for in the UoA's regulations, etc., and other individuals recognized by Departments, Divisions, and Centers executive administrators.

20) Faculty, Administrative Staff, Etc.

This refers to the UoA's executives, full-time or part-time faculty and administrative staff working for the UoA (including temporary staff, etc.), and other individuals approved by Departments, Divisions, and Centers executive administrators.

21) User

This refers to faculty, administrative staff, etc. and students, etc. authorized to use the UoA's information systems.

22) Temporary User

This refers to individuals other than faculty, administrative staff, etc. and students, etc. authorized to temporarily use the UoA's information systems.

23) Outsourcing

This refers to contracting an external personnel with conducting the partial or entire duties related to information processing of the UoA. It includes all types of outsourcing contracts including delegation, semi-delegation, and service conracts.

24) Information Security Incident

This refers to information security incidents defined in JIS Q 27000:2014

25) CSIRT (Computer Security Incident Response Team)

This refers to the organization established in the University in order to handle information security incidents occurring within the UoA.

26) Information Levels and Handling Restrictions

This refers to standards for defining protection levels for information, which serves to clarify information security measures the UoA needs to take according to its confidentiality, integrity, and availability.

The details shall be provided for separately.

27) Secure Area

This refers to areas managed by the UoA (including areas in the facilities, etc. rented from external organization) requiring measures concerning facilities and work environment in order to protect information handled by the UoA.

Article Four

(Chief Information Security Officer)

4.1 The position of Chief Information Security Officer, which is in charge of supervising administrative affairs related to the information security of the UoA, shall be established. The Chairperson of the Board of Executives shall appoint an individual for the position.

4.2 The term of office of the Chief Information Security Officer shall be two years.

4.3 The Chief Information Security Officer shall be able to appoint a Deputy Chief Information Security Officer to assist the Chief Information Security Officer, organize administrative affairs related to the information security of the UoA on the orders of Chief nformation Security Officer,

and supervise administrative affairs related to the UoA's information security if needed.

4.4 The Chief Information Security Officer shall supervise the following administrative affairs.

1) Establishment of organizations and systems for promoting information security measures

2) Decisions on and reviews of revisions of items of the information security policy and regulations related to information security

3) Instructions and other measures necessary to handle information security incidents

4) Decisions on and reviews of revisions of important items related to information security other than those provided for in the preceding items

4.5 The Chief Information Security Officer shall be able to designate the information systems of the UoA considered to have a major impact if an information security breach occurs as important information systems

Article Five

(Establishment of the Information Security Committee of the Public University Corporation of the University of Aizu)

5.1 The Chief Information Security Officer shall establish the Information Security Committee of the Public University Corporation of the University of Aizu (hereinafter, Information Security Committee) comprised of representatives, etc. of Departments, Divisions, and Centers that perform duties related to the information security measure promotion system and other related duties, which serves as an organization to deliberate on the information security policy and regulations related to information security.

5.2 The chairperson and members of the Information Security Committee shall be appointed from amongst representatives, etc. of Departments, Divisions, and Centers that perform duties related to the information security measure promotion system and other related duties by the Chairperson of the Board of Executives.

5.3 The Information Security Committee shall deliberate on the following items.

1) Items related to the implementation, revision, and abolition of the information security policy and regulations related to information security

2) Items related to information security awareness, education, and training

3) Items related to information security audits

4) Items related to the operation of the information security system

5) Items related to recurrence prevention measures for information security incidents

6) Other necessary items related to information security not provided for in the preceeding items

Article 6

(Chief Information Security Audit Officer)

6.1 The Chief Information Security Officer shall appoint Chief Information Security Audit Officer who will supervise affairs related to audits orderd by the Chief Information Security Officer.

Article 7

(Information Security Administrative Office)

7.1 The Information Security Committee shall establish the Information Security Administrative Office, the duties of which shall be performed primarily by the General Affairs and Budget Division.

Article 8

(Administrative Affairs Performed by the Information Security Administrative Office)

8.1 The Information Security Administrative Office shall perform the following administrative affairs based on the instructions from Chief Information Security Officer.

1) Administrative affairs related to the operation of the Information Security Committee

2) Monitoring the implementation of the policy in the operation and the use of the University's information systems

3) Monitoring the implementation of the lecture plans, risk management, emergency action plans, etc.

4) Announcements and reports related to the University's information security

Article Nine

(Position of Department, Division, or Center Executive Administrator)

9.1 The Chief Information Security Officer shall appoint an executive administrator in each department, division, and center as the individual responsible for supervising administrative affairs related to information security measures of their organization. The executive administrator of the Information Security Administrative Office shall supervise the other executive administrators.

9.2 The executive administrator of the Information Security Administrative Office shall supervise the following administrative affairs on the orders of the Chief Information Security Officer.

1) Designation of secure areas and decisions on measures related to facilities and environments in said areas

2) Coordination of the establishment and revision of the information security measure implementation procedures and administrative affairs related to said implementation procedures

3) Formulation of information security education implementation plans and establishment of systems for implementing said plans

4) Recording of processes and results of examinations of application of exceptional measures

5) Establishment of emergency contacts, etc. to handle information security incidents

6) Other administrative affairs related to information security measures not provided for in the preceeding items

9.3 Executive Administrators of Department, Division, and Center shall, on the orders of the Chief Information Security Officer, supervise the following administrative affairs in order to promote information securities in the organization they manage.

1) Appointment of Information Security Officer of their Department, Division, and Center

2) Appointment of Infomration Security Technical Officer of their Department, Division, and Center for each system

3) Implementation of investigations of the causes of information security incidents, recurrence

prevention measures, and other items related to information security incidents

4) Formulation of self-inspection plans and establishment of implementation procedures

5) Other administrative affairs related to information security measures in the organization they manage not provided for in the preceeding items.

Article Ten

(Position of Information Security Officers)

10.1 Department, Division, and Center Executive Administrators shall appoint an Information Security Officer responsible for supervising administrative affairs related to information security measures in each organization defined in the List of the University of Aizu Management Organization for Information Security Measures.

The Information Security Officer of a department, division, or center shall be an individual from/who belong to said department, division, or center.

10.2 Information Security Officers shall supervise administrative affairs related to handling of information and other information security measures in each organization on the orders of Department, Division, and Center Executive Administrators.

Article Eleven

(Department, Division, and Center Information Security Committees)

11.1 Department, Division, and Center Executive Administrators shall be able to establish Department, Division, or Center Information Security Committees as needed.

11.2 Department, Division, and Center Information Security Committees shall perform the following duties.

1) Investigation of and dissemination of information on the state of policy compliance at their department, division, or center

2) Risk management and formulation and implementation of emergency action plans at their department, division, or center

3) Formulation and implementation of recurrence prevention measures for information security incidents at their department, division, or center

4) Planning, proposing and implementation of education of information security technical staff at their department, division, or center

Article Twelve

(Members of Departments, Division, and Center Information Security Committees)

12.1 The Departments, Division, and Center Information Security Committees shall be comprised of a chairperson and the following individuals as committee members.

1) Department, Division, and Center Information Security Technical Officer

2) Department, Division, and Center Information Security Technical Staff

3) Other individuals recognized as necessary by Departments, Division, and Center Executive Administrators

Article Thirteen

(Chairperson of Departments, Division, and Center Information Security Committees)

13.1 The role of Chairperson of Department, Division, and Center Information Security Committee shall be performed by the Department, Division, and Center Executive Administrators.

Article Fourteen

(Position of Department, Division, and Center Technology Officers)

14.1 Department, Division, and Center Executive Administrators shall select Department, Division, and Center Technology Officers, who will be the individual responsible for administrative affairs related to information security measures for information systems under the jurisdiction of their own department, division, or center before the beginning of work on the planning for the information systems.

14.2 Department, Division, and Center Technology Officers shall be in charge of administrative affairs related to information security measures within information systems on the orders of Department, Division, and Center Executive Administrators.

14.3 Department, Division, and Center Technology Officers shall be able to appoint Department, Division, and Center Technical Staff, who will be in charge of management tasks for information systems under the jurisdiction of their own department, division, or center within each management organization, as needed.

Article Fifteen

(Position of Information Security Advisor)

15.1 The Chief Information Security Officer shall appoint an individual with a high level of expertise and experience concerning information security as Information Security Advisor.

15.2 The term of office of the Information Security Advisor shall be two years.

15.3 The Information Security Advisor shall perform the following duties.

1) Advising the Chief Information Security Officer concerning the promotion of information security measures at the UoA

2) Giving advice on establishment of the Information Security Policy and other related regulations

3) Giving advice on the formulation of plans for promoting information security measures

4) Giving advice on the designing of education implementation plans, supporting the development of educational materials and the implementation of education

5) Giving technical advice concerning information systems

6) Giving advice on the formulation of requirement specifications related to information security included with the procurement specifications submitted to vendors in cases where the design and/or development of information systems is outsourced

7) Supporting the handling of information security incidents

8) Giving other advice or support regarding information security measures other than that provided for in the preceeding items

Article Sixteen

(Establishment of the Information Security Measure Promotion System of the UoA)

16.1 The Chief Information Security Officer shall establish the UoA Information Security Measure Promotion System and stipulate the roles within it.

16.2 The Chief Information Security Officer shall appoint individuals responsible for the Information Security Measure Promotion System.

16.3 The Chief Information Security Officer shall stipulate the roles within the system including the following:

1) Administrative affairs related to the formulation of information security-related regulations and plans for promoting the measures

2) Administrative affairs related to the implementation of information security-related regulations

3) Administrative affairs related to exceptional measures

4) Administrative affairs related to the implementation of education and training sessions regarding information security measures

5) Administrative affairs related to self-inspection of information security measures

6) Administrative affairs related to the review of information security-related regulations and plans for promoting the measures

Article Seventeen

(Establishment of Systems for Prepareing for Information Security Incidents)

17.1 The Chief Information Security Officer shall establish CSIRT and clarify the roles within it.

17.2 The Chief Information Security Officer shall select individuals recognized as having a high level of expertise and qualification as CSIRT members from amongst the faculty and administrative staff members. The CSIRT Officer respsible for handling information security incidents at the UoA shall be selected from these individuals. In addition, faculty or administrative staff members, etc. in charge of task management within CSIRT, collaboration with external entities, etc. shall be appointed.

17.3 The Chief Information Security Officer shall establish a system that will allow immediate reporting of information security incidents to himself or helself when it occurs.

17.4 The Chief Information Security Officer shall stipulate the roles within CSIRT including the following task.

1) Centralized management of handling information security incidents involving the UoA when it occurs

- Management of handling of information security incidents at the UoA
- Receiving reports on possible information security incidents
- Aggregating information concerning information security incidents at the UoA
- Reporting information security incidents to the Chief Information Security Officer, etc.
- Establishment of a vertical chain of command concerning handling of information security incidents

2) Prompt and appropriate handling of information security incidents

- Determining whether a case is an information security incident or not
- Orders, recommendations, or advice regarding the whole of handling of information security

incidents including orders or recommendations to take emergency measures to minimize damage

- Contacting MEXT and the prefectural government
- Collecting information regarding information security incidents from external specialized institutions, etc.
- Sharing information related to information security incidents with other institutions, etc.
- Providing expertise related to and handling of information security incidents

17.5 The Chief Information Security Officer shall establish an effective system for CSIRT including staff members in charge of performing its actual business.

17.6 The Chief Information Security Officer shall establish a system that allows the necessary support from external specialists, etc. who have a high level of expertise regarding the handling of information security incidents to be received immediately in the event an information security incident occurs.

17.7 The Chief Information Security Officer shall, in the event of an information security incident at the UoA, stipulate the division of roles of the CSIRT, the department, division or center involved, and other related department, division or center regarding the handling of said information security incident.

Article Eighteen

(Roles Which May Not Be Performed Concurrently)

18.1 No faculty or administrative staff member, etc. shall concurrently perform the following pairs of roles concerning the operation of information security measures.

1) Applying for and granting approval / certificiation
2) Undergoing and conducting audits

Article Nineteen

(Establishment of Security Standards)

19.1 The Chief Information Security Officer shall establish the security standards in line with the “Common Standard on Information Security Measures of Government Entities” established by the Cybersecurity Strategic Headquarters after the discussion at the UoA Information Security Committee meeting. In addition, the security standards shall be established based on the results of risk evaluations concerning the work of, the information handled by, and the information systems possessed by the UoA.

Additional Provisions

This regulation shall be enforced as of April 1, 2021.