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

Kyoto University Regulations for Information Security Programs

October 21, 2003
Notification No.43

Chapter 1 General Provisions

Article 1 (Purpose)

The purpose of these Regulations is to set forth rules for maintaining and improving the information security of the information system in Kyoto University (hereinafter the "University") to ensure protection and proper utilization of the University's information assets.

Article 2 (Definition)

In these Standards, the following terms are defined as follows:

(1) “Information security” means ensuring confidentiality, integrity and availability of information assets.
(2) “Information system” means a system designed to create, use and manage information and perform other similar operations (information devices composed of hardware and software, and wired and/or wireless network).
(3) “Information assets” means information systems, information recorded on such information systems and information related to development and operation of such information systems, all of which shall be recorded in electromagnetic means as specified in Item (11) below unless otherwise specified.
(4) “Information Security Policies” refers to the Kyoto University Basic Policy for Information Security (determined by the Board of Executive Directors on March 25, 2015) and the Kyoto University Regulations for Information Security Programs (this document).
(5) “Implementation regulations” refers to the Kyoto University Information Security Program Standards (hereinafter the “Standards”), the Kyoto University Information Classification Standards (hereinafter the “Classification Standards”), and other regulations, standards and plans, established by the Trustee in charge of information management (hereinafter “Trustee in Charge”) in accordance with the Information Security Policies.
(6) “Incident” means an accident or event relating to information security, occurring either

intentionally or accidentally, that results in a breach of any of the University's regulations or statutory provisions.

(7) "Personal information" means personal information as defined in Article 2.1 of the Kyoto University Regulations for Protecting Personal Information (Notification No.1 2005), specific personal information as defined in Article 2.4 of the Regulations for Protecting Personal Number and Specific Personal Information (Notification No.49 2015) and other similar information.

(8) "Departments" means graduate schools, laboratories, libraries, university hospitals and centers (facilities defined in Sections 7, 8, 10 and 11, Chapter 3 of Regulations Regarding Organization of Kyoto University (Notification No.1 2004, referred to as "Organization Regulations" in this Item (8)), administrative organizations of headquarters (a unit defined in Article 56.1 of the Organization Regulations shall be treated as one department; the same definition applies to Article 5.1 below), the administrative office in Uji Campus and the common administrative office for three graduate schools.

(9) "Faculty members and office personnel" means officers and faculty members and office personnel employed in accordance with the office regulations of the University.

(10) "Students" means graduate and undergraduate students, foreign students, trusted students, non-degree students, auditing students, special auditing students, special research students, special exchange students and other similar students (as defined in Chapter 5 of the Kyoto University General Rules (Notification No. 3, 1953)), research students, trainees and other similar students (as defined in the Kyoto University Training Regulations (Notification No. 3, 1949)) and researchers and other persons engaged in academic activities accepted by the University in accordance with other regulations of the University.

(11) "Electromagnetic records" means records created by electronic or magnetic means or any other means that cannot be perceived by human senses, which are provided for the purpose of data processing by computers.

Article 3 (Scope)

1. Information Securities Policies shall apply to the following information assets:
   (1) Information systems owned or managed by the University,
   (2) Information devices connected to information systems referred to in Item (1) above and not falling under the definition in Item (1),
   (3) Information systems provided by other parties in accordance with contract or other arrangement with the University,
   (4) Information created or collected by users of information systems as defined in Items (1)

and (2) above or information devices as defined in Item (2) above (including other users than faculty members and office personnel and students; the same definition shall apply hereinafter) for the purpose of educational activities, studies and other activities of the University, which is stored on such information systems or information devices,

(5) Information regarding planning, structuring, operation and other data processing activities related to information systems as defined in Items (1) or (3), which is recorded in writing, and

(6) Information created or collected by faculty members, office personnel and students for the purpose of educational activities, studies and other activities of the University and not falling under the definition in Item (2) above.

2. Persons who operate, manage or use information assets referred to in each Item in Paragraph 1 above shall observe the Information Security Policies.

Chapter 2 Responsible Organizations

Article 4 (Chief Information Security Officer)

1. The University shall appoint the officer in charge of information management as the Chief Information Security Officer of the University.
2. The Chief Information Security Officer shall have general power and responsibility for information security of the University.

Article 4-2 (Information Security General Manager)

1. The President of the University shall appoint the Information Security General Manager from among faculty members and office personnel of the University.
2. The Information Security General Manager shall exercise general supervision of implementation of information security measures in the University.

Article 4-3 (Information Security Auditing Manager)

1. The Chief Information Security Officer of the University shall appoint the Information Security Auditing Manager from among faculty members and office personnel of the University.
2. The Information Security Auditing Manager shall exercise supervision of the audit specified in Article 15, in accordance with instructions given the Chief Information Security Officer.

Article 4-4 (Information Security Auditor)

1. The Information Security Audit Manager shall appoint the Information Security Auditor, from among faculty members and office personnel of the University.

2. The Information Security Auditor shall carry out the audit specified in Article 15, in accordance with instructions given by the Information Security Auditing Manager.

Article 4-5 (Information Security Advisor)

1. The University may appoint an Information Security Advisor as necessary.
2. The Information Security Adviser shall be appointed by the Chief Information Security Officer from persons outside of the University who have professional expertise and experience on information security.
3. The Information Security Advisor shall provide technical advice on information security to the Chief Information Security Officer.

Article 5 (Department Information Security Manager)

1. Each department shall have a position of department information security manager, which shall be served by the chief of such department (or by a person designated by the Chief Information Security Officer in the case of the administrative office of the headquarters).
2. The information security manager of each department shall have power and responsibility for information security of the department.

Article 5-2 (Department Information Security Technical Manager, etc.)

1. The information security manager of each department shall appoint the department information security technical manager from among faculty members and office personnel of the department.
2. The information security technical manager of each department shall supervise implementation of information security measures for the departments' information system.
3. Each department may have a position of deputy information security technical manager as necessary to assist the information security technical manager of such department.

Article 5-3 (Department Information System Technical Staff Member)

1. In each department that has its own information system, the information security manager shall appoint a staff member in charge of technical matters for each such information system.
2. The information system technical staff member shall implement information security measures for the information system that he/she manages.

Article 5-4 (Department Information Security Communications Manager)

Each department shall have a position of information security communications manager with responsibility for exercising general supervision of work related to communications and

coordination associated with any incidents which may occur in such department.

Article 6 (University Information Security Committee and Other Committees)

1. The University shall appoint the University Information Security Committee (hereinafter the "University Committee") that discusses the following matters relating to information security of the University:
   (1) Revision or abolition of these Regulations,
   (2) Establishment, revision or abolition of implementation regulations that is necessary for ensuring information security,
   (3) Any matter relating to measures taken or to be taken for maintenance and improvement of information security, and
   (4) Any other matter that is important for information security.
2. The University Committee shall be comprised of the following members:
   (1) Chief Information Security Officer,
   (2) Information Security General Manager,
   (3) Department information security managers, and
   (4) Other persons designated by the Chief Information Security Officer (several persons)
3. The University Committee shall appoint the Chief Information Security Officer as its chairperson.
4. The chairperson shall call a meeting of the Committee and chair such meetings.
5. To coordinate technical matters related to information security between the University system and department systems, the University Information Security Technical Coordination Committee (hereinafter the “Coordination Committee”) shall be established under the University Committee.
6. The Coordination Committee shall be comprised of the following members, and chaired by the Information Security General Manager or any person designated by the Information Security General Manager.
   (1) Information Security General Manager,
   (2) Either the information security technical manager or the deputy information security technical manager from each department, as appointed by the department’s information security manager (one person from each department), and
   (3) Other persons designated by the Information Security General Manager (several persons)
7. Other businesses of and other necessary matters relating to the University Committee shall be determined by the University Committee.

Article 7 (Information Security Incident Response Team)

1. The Information Security Incident Response Team (hereinafter “CSIRT”) shall be established under the Chief Information Security Officer in order to respond promptly and smoothly when incidents occur.
2. Matters necessary for the CSIRT shall be determined by the Trustee in charge of information infrastructure.

Article 7-2 (Information Network Risk Management Committee)

1. The Information Network Risk Management Committee shall be established under the Chief Information Security Officer that is responsible for risk management of the information network.
2. Matters necessary for the Information Network Risk Management Committee shall be determined by the Trustee in charge of information infrastructure.

Article 7-3 (Information Network Ethics Committee)

1. The Information Network Ethics Committee shall be established under the Chief Information Security Officer to ensure prevention of transmission of information that infringes or may infringe human rights, copyrights and other rights of other persons.
2. Matters necessary for the Information Network Ethics Committee shall be determined by the Trustee in charge of information infrastructure.

Article 8 (Department Information Security Committee)

1. Each department shall establish an information security committee (hereinafter the "department committee").
2. Notwithstanding the provision in the preceding Paragraph, if deemed necessary by relevant departments, more than one department may form one department committee jointly.
3. The department committee shall be comprised of persons appointed by the information security manager of the department. For the department committee jointly formed by more than one department as stipulated in Paragraph 2 above, members of the department committee shall be appointed upon mutual consultation among information security managers of relevant departments.
4. The department committee shall appoint the information security manager of the department as its chairperson. For the department committee formed in accordance with Paragraph 2 above, relevant departments shall consult with each other to appoint a chairperson from among information security managers of those departments.
5. Each department committee shall assist the information security manager of the department and handles matters relating to information security of the department.

6. Matters necessary for the department committee shall be decided by such department. For the department committee formed in accordance with Paragraph 2 above, such matters shall be decided by mutual consultation among relevant departments.

Article 9 (Segregation of Duties)

In implementing information security measures, the following duties shall not be performed by the same person:

(1) The person requesting approval or permission, and the person giving approval or permission to such request; and

(2) The person who is audited and the person who conducts the audit.

Chapter 3 Protection of Information Assets

Article 10 (Classification and Management of Information Assets)

1. The information security manager of each department shall assign an appropriate classification to each information asset managed by such department and shall conduct management thereof based on the Classification Standards.
2. Specific rules and procedures necessary for following the provision in Paragraph 1 above shall be set forth in the Standards.

Chapter 4 Maintenance and Improvement of Information Systems Security

Article 11 (Information System Life Cycle)

Matters necessary for the installation, operation, and disposal of information systems owned or managed by the University shall be set forth in the Standards.

Chapter 5 Measures Against Incidents

Article 12 (Measures Against Incidents)

Specific rules and procedures necessary for taking measures against incidents shall be set forth in the Standards.

Chapter 6 Monitoring of Network and Collection of Use Information

Article 13 (Monitoring of Network)

1. Persons who manage, operate or use the information systems as defined in Article 3.1 or 3.3 or information devices as defined in Article 3.2 shall not monitor communications

transmitted on the network. However, the Chief Information Security Officer or the information security manager of the department that manages such information system may direct a person designated in advance to monitor communications transmitted on the network (hereinafter "monitoring") if such monitoring is necessary to ensure security of the information system. The scope and procedures for monitoring shall be set forth in the Standards.

2. The person designated in Paragraph 1 above shall not disclose to any other party the contents of communications or personal information that he/she may come to know in the course of such monitoring; provided, however, that, if it is deemed necessary to prevent serious invasion of security of other parties within or outside the University, information collected in such monitoring may be disclosed to the person who has directed such monitoring and other parties that need to know such information as designated in the Standards.
3. Rules for handling monitoring records and other necessary matters relating to monitoring shall be set forth in the Standards.

Article 14 (Use Records)
Matters related to collection and handling of use records of information systems shall be set forth in the Standards.

Chapter 7 Auditing, Inspection, Revision of Information Security Policies

Article 15 (Auditing)
The Information Security Auditing Manager and the Information Security Auditor shall conduct an audit of the implementation status of the Information Security Policies and implementation regulations, and the Information Security Auditing Manager shall report the results of the audit to the Chief Information Security Officer.

Article 16 (Inspection)
The information security manager of each department shall inspect the implementation status of the Information Security Policies and implementation regulations, and report the results of the inspection to the Chief Information Security Officer.

Article 17 (Revision of Policies and Implementation Regulations)
The University Committee shall, taking into account the results of the auditing in Article 15 and the results of the inspection in Article 16 and incident experiences in the University, consider revision of Information Security Policies and implementation regulations.

Article 18 (Other Matters)
Other matters not provided for in these Regulations but necessary for information security in the University shall be set forth in the Standards.

Supplementary Provisions
These Regulations shall take effect on October 21, 2003.
Supplementary Provisions (Notification No. 117, 2004)
These Regulations shall take effect on June 2, 2004 and shall apply retroactively from April 1, 2004.
Supplementary Provisions (Notification No. 143, 2005)
These Regulations shall take effect on February 16, 2005 and shall apply retroactively from April 1, 2004.
Supplementary Provisions (Notification No. 76, 2005)
These Regulations shall take effect on November 29, 2005 and shall apply retroactively from November 1, 2005.
[Description of subsequent supplementary provisions related to revision of the Regulations is omitted.]
Supplementary Provisions (Notification No. 71, 2006)
1. These Regulations shall take effect on December 25, 2006.
2. The Kyoto University Rules for Information Network Risk Management Committee (established by the President of the University, March 31, 2004) are abolished.

[Description of subsequent supplementary provisions related to revision of the Regulations is omitted.]
Supplementary Provisions (Notification No. 67, 2009)
1. These Regulations shall take effect on April 1,2009.
2. The Kyoto University Standards for Information Security Programs (approved by the President of the University, October 21, 2003) are abolished.

[Description of subsequent supplementary provisions related to revision of the Regulations is omitted.]
Supplementary Provisions (Notification No. 40, 2014)
These Regulations shall take effect on October 1, 2014.
Supplementary Provisions
These Regulations shall take effect on April 1, 2015.
Supplementary Provisions
These Regulations shall take effect on April 1, 2016.
Supplementary Provisions

These Regulations shall take effect on April 1, 2017.