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

Kyoto University Information Security Program Standards

(Approved by Trustee in charge of Information Infrastructure on March 2 , 2009)

Chapter 1 General Provisions

Article 1 (Purpose)

The purpose of these Standards is to set forth rules for maintaining and improving the information security of the information system at Kyoto University (hereinafter the "University") in accordance with Article 2.5 of the Kyoto University Regulations for Information Security Programs, in order to ensure the protection and proper utilization of the University's information assets and to improve the reliability, safety, and efficiency of the information system.

Article 2 (Definitions)

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

(1) “Basic Policy**”** refers to the Kyoto University Basic Policy for Information Security (determined by the Board of Executive Directors on March 25, 2015).

(2) “Regulations” refers to the Kyoto University Regulations for Information Security Programs (Notification No. 43, 2003).

(3) "Information network devices" means devices installed for connecting to information networks and for controlling information sent and received by servers and terminals via information networks (including firewalls, routers, hubs, information wall sockets, and wireless network access points).

(4) “Servers” means components of information systems (including installed software and directly connected keyboards, mouse devices, and other peripherals fully integrated therewith) that provide their own services to terminals and the like connected via information lines, and which, except where expressly stated otherwise, are procured or developed by the University.

(5) “Terminals” means components of information systems (including installed software and directly connected keyboards, mouse devices, and other peripherals fully integrated therewith) that are operated directly by users and the like for the purpose of information processing, and which are procured or developed by the University, or sourced from external providers, and are connected to on-campus communication lines. Mobile terminals are included in this definition.

(6) “University Information System” means the information system as defined in Article 3.1.(1) and 3.1.(3) of the Regulations.

(7) “Campus-wide Information System” refers to a part of the University Information System as defined in Article 4.1.

(8) “Department information systems” refers to other parts of the University Information System that are not part of the Campus-wide Information System.

(9) "Secure area" means an area within an office, laboratory, classroom, server room or other room (including off-campus server room or data center) where servers and terminals and/or information network devices are installed and where security measures are taken, on its facilities and in its environment, to prevent intrusion by any persons other than users and the like, the invasion of information security caused by natural disaster or other causes.

(10) “Users” means faculty members, office personnel and students of the University who are authorized to use the University Information System.

(11) “Temporary users” means persons other than faculty members, office personnel and students of the University who are authorized to use the University Information System.

(12) “Users and the like” means users, temporary users and persons who manage the University

Information System.

(13) “Entity” means a person who attempts to access the information system, or a server, terminal or the like that accesses another information system. The term “entity” primarily envisages human subjects but, in the event that two or more information systems or devices function in tandem, it also includes other information systems or devices as entities attempting to access the information system.

(14) “Entity authentication” means the process of verifying whether an entity presenting an identification code (as defined in Item 16) is an authentic entity that has been assigned with that identification code. When entity authentication information is presented in the correct manner, together with an identification code, the information system verifies that the entity presenting the information is an authentic entity. For the purposes of these Standards, "authentication" includes both authentication by the University’s integrated authentication system and authentication by department information systems.

(15) “Identification” means identification by an information system of an entity attempting to access that system.

(16) An "identification code" is a code recognized by the information system to identify an entity. A user ID can be cited as a typical identification code.

(17) “Entity authenticating information” is information presented by entities to the information system for entity authentication. A password is a typical form of entity authenticating information.

(18) An "account" is the rightful authority assigned to an entity to access the information system requiring entity authentication.

(19) The university’s Computer Security Incident Response Team (CSIRT) is established in accordance with Paragraph 1 of Article 7 of the Regulations for the CSIRT.

(20) Other terms used in these Standards have meanings as defined in the Exhibit attached to these Standards and the Regulations.

Article 3 (Scope)

1. These Standards shall apply to faculty members, office personnel, and users and the like who use and manage information assets of the University.
2. If special rules are stipulated by law and/or directives issued in accordance with such law regarding matters about use and management of information assets, such matters shall be handled in accordance with such rules stipulated by law and/or directives.

Article 4 (Operational and Management Organization)

1. The Chief Information Security Officer shall designate the information system implemented as an intelligence infrastructure for the entire organization of the University that would be significantly affected by infringement of information security (hereinafter the "Campus-wide Information System").
2. An organization responsible for operation and management of the Campus-wide Information System (hereinafter the "Operational and Management Organization") shall be established, whose functions shall be served by the Institute for Information Management and Communication of the University.
3. In addition to the responsibilities referred to in Paragraph 2 above, the Operational and Management Organization shall conduct the following activities, in accordance with directions from the Information Security General Manager (see Article 7):
   (1) Administrative activities relating to the operation of the University Information Security Committee;
   (2) Collection of information on the observation status of the Information Security Policy in the operation and use of the University Information System;
   (3) Collection of information on the progress of training programs, risk management, the emergency action plan, and other programs;
   (4) Notification and communication of matters relating to information security of the University Information System;
   (5) Coordination of connections between the Campus-wide Information System and department information systems, and connection with external networks; and

(6) Provision of documentation to aid compliance with these Standards.

Article 5 (Responsible Organizations)

1. The Information Security General Manager shall represent the Campus-Wide Information System in communications and notifications related to information security of the Campus-Wide Information System.
2. The Information Security Committees of each department under the Operational and Management Organization shall implement information security measures for the Campus-wide Information System, in accordance with the Basic Policy and the Regulations and under the direction of the Information Security General Manager.
3. The Information Security Committee of each department shall implement information security measures for its department information system, in accordance with the Basic Policy and the Regulations and the operation policy of the department, under the direction of the department information security manager, who is responsible for managing such information system of the department.
4. Technical coordination between the University system and department systems of matters regarding information security shall be made by the University Information Security Technical Coordination Committee.
5. Directions or recommendations for emergency measures for the purposes of University-wide and inter-departmental coordination and damage mitigation in relation to information security incidents shall be issued by the Information Security Management Office, IT Services Division, Planning and Information Management Department.
6. The Information Network Risk Management Committee shall conduct risk management of the information network.
7. The Information Network Ethics Committee shall be responsible for handling matters relating to prevention of transmission of information that infringes or may infringe human rights, copyrights or other rights of any person.

Article 6 (Contact Network)

1. The Information Security General Manager (see Article 7) shall establish the following contact networks for matters regarding information security:
   (1) A contact network among all department information security managers; and
   (2) A contact network among all department information security technical managers.
   (3) A contact network for the implementation of university-wide information security measures.
2. Each department information security technical manager shall establish a contact network among information system technical staff members of the department.

Article 7 (Prohibitions)

The department information security technical manager and information system technical staff members of the department shall not conduct or cause other persons to conduct the following acts:

(1) Use information assets to other purposes than the intended purposes;
(2) Provide information that breaches obligations of confidentiality;
(3) Conduct unauthorized monitoring of communications on the information network or collect usage records from information network devices, servers, or terminals, without permission from the information security manager of the department;
(4) Conduct unauthorized detection of security vulnerabilities of systems without directions from the department information security manager;
(5) Provide information that breaches statutory provisions or the University's regulations;
(6) Abuse any administrator authority; and
(7) Conduct any act that encourages any of the above-mentioned acts.

Article 8 (Connection to Off-Campus Communication Lines)

1. The Information Security General Manager shall obtain approval from the Chief Information Security Officer before connecting an on-campus communication line with a communication line

outside the university ("off-campus communication line"). Users and the like are not authorized to make connection between an on-campus and an off-campus communication line.
2. If the Information Security General Manager determines that connection between an on-campus communication line and an off-campus communication line may jeopardize the security of the information system, such on-campus communication line shall be structured as a communication line that is segregated from any other on-campus communication lines shared with other information systems or from any off-campus communication lines.
3. If any situation arises where it is difficult to secure the information system regarding the connection between an on-campus communication line and an off-campus communication line, the Information Security General Manager shall change the configuration of the on-campus communication line so that it is segregated from any other on-campus communication line shared with other information systems or off-campus communication lines.
4. On a periodic basis and whenever a change is made to the communication line, the Information Security General Manager shall review the configuration of access control.
5. The Information Security General Manager shall periodically check for security holes on on-campus communication lines and information network devices that can be accessed from an off-campus communication line.
6. The Chief Information Security Officer shall monitor the contents of transmissions between on-campus communication lines and off-campus communication lines.

Article 9 (Relationship with Upstream Networks)
In structuring and operating the University Information Network, the Information Security General Manager shall ensure to maintain consistency with the upstream networks with which the University Information Network is connected.

Chapter 2 Lifecycle of Information System
Section 1 Lifecycle Concepts

Article 10 (Planning and Design of the Information System)
1. The information security technical manager of each department shall require the person in charge of controlling the information system to maintain a system that ensures the security of the information system over its lifecycle.
2. The information security technical manager of each department shall determine security requirements for the information system of the department.
3. The information security technical manager of each department shall determine the purchase of devices and other materials (including leases equivalent to purchases), countermeasures to be considered during software development, configuration of information security functions, measures against threats on information security, and measures necessary for components in the information system, in order to satisfy the security requirements of the information system.
4. In implementing the developed information system, the information security technical manager of each department shall determine procedures and environments for the implementation from the viewpoint of information security.

Article 11 (Development, Operation, and Monitoring of the Information System)
In development, operation, and monitoring of the information system, the information security technical manager of each department shall implement information security measures determined in accordance with security requirements.

Article 12 (Review of the Information System)
The information security technical manager of each department shall from time to time consider whether information security measures currently implemented for the information system must be reviewed. He/she shall conduct such reviews as necessary, and take necessary actions.

Article 13 (Switching or Abandonment of the Information System)

If the department shifts to a new information system and abandons the old system, the information security technical manager of each department shall consider the necessity of, and take proper actions for, deletion and retention of data stored on the old system, and abandonment and reuse of components of the old system.

Article 14 (Planning for Operational Continuity of the Information System)

1. The information security manager of each department shall consider measures pertaining to information security in emergency situations in the course of planning for operational continuity of the information system to support emergency priority work in the department.
2. The information security manager of each department shall verify the operability of information security measures for use in emergency situations when conducting education/training on and maintenance/improvement of plans for operational continuity of the information system.

Section 2 Structuring

Article 15 (Procurement and Structuring)

When selecting devices and the like, the information security technical manager of each department shall ensure that:

(1) Reliable systems have been established for quality assurance in the development process.
(2) Support systems have been established for installation and maintenance.
(3) Appropriate user manuals/guidelines have been prepared.
(4) Implementation of vulnerability diagnoses and other tests can be confirmed.
(5) Third-party validation in accordance with international standards such as ISO is used where possible.
(6) Security functions satisfy the security requirements for the device and the like in question.
(7) The following conditions are satisfied in cases where devices and the like require application of security modifications in order to maintain information security:
  (a) The necessary security modifications have been applied at the time of delivery.
  (b) The necessary security modifications are provided and applied on an ongoing basis after delivery.
(8) It is possible to apply any of the following maintenance and inspection works that the department information security technical manager considers necessary to ensure information security.
  (a) Maintenance, checks, etc. of hardware
  (b) Provision of software and software modifications and updates
  (c) Vulnerability diagnoses and other forms of maintenance and checks of devices and the like considered necessary by the department information security technical manager.

Article 16

When conducting verifications and inspections upon delivery of devices and the like or introduction of information systems, the information security technical manager of each department shall confirm that requirements regarding information security measures are satisfied in accordance with the inspection procedures prescribed in specification documents, etc.

Article 17 (Measures Against Security Holes)

1. The information system technical manager of each department shall collect device information necessary for taking measures against security holes for servers, terminals, and information network devices maintained by the department, and document the collected information.
2. When installing or before commencing the use of servers, terminals, and information network devices maintained by the department, information system technical staff members shall implement countermeasures against publicly released security holes on software to be used on such devices.

Article 18 (Measures Against Malware)

1. The information security manager of each department shall set forth security guidelines for daily

operations to be followed by users and the like in order to avoid infection with malware.
2. The information security technical manager of each department shall install antivirus software on servers and terminals and take other appropriate measures to protect servers and terminals from malware (unless no antivirus software that can be run on such servers and terminals is available; the same condition applies hereinafter).
3. The information security technical manager of each department shall implement measures against malware, including installing antivirus software, on all possible infection routes for malware.

Article 19 (Measures Against Denial-of-Service Attacks)

For an information system that handles information requiring stability, the information security technical manager of each department shall, as countermeasures against denial-of-service attacks, utilize the applicable functions provided by servers, terminals, and information network devices used for providing services.

Article 20 (Measures Against Targeted Attacks)

1. The information security technical manager of each department shall institute measures (entry point measures) in the information system to minimize incursions into the organization by targeted attacks.
2. The information security technical manager of each department shall institute measures (internal measures) in the information system to enable early detection and response to attacks constituting an internal incursion, to increase the difficulty of expanding the scope of the incursion, and to detect and respond to unauthorized external communication.

Article 21 (Secure Areas)

1. The information security technical manager of each department shall implement the following security measures on facilities and environment in regard to on-campus secure areas, considering the risks associated with information systems (including risks of physical destruction, leakage, or unauthorized alteration of information).
   (1) Clearly separate secure areas from their surrounds using walls, lockable doors, partitions, and other demarcations in order to prevent easy access by unauthorized personnel. For classrooms, laboratories, offices and other spaces with service counters which cannot easily be separated, institute measures enabling faculty members or office personnel to monitor the counters constantly at times when the area is accessible by persons who cannot be identified.
   (2) Lock the area when all faculty members and office personnel are absent, in order to prevent easy access by unauthorized personnel.
2. The information security technical manager of each department shall consider the risks associated with information systems and, if using an off-campus server room or data center as a secure area, shall confirm that the measures stated in the preceding paragraph are implemented.

Article 22 (Establishment of Rules and Documents)

1. The information security technical manager of each department shall establish rules for ensuring the security of servers and terminals.
2. The information security technical manager of each department shall establish rules for ensuring the provision of secure services via communication lines.
3. The information security technical manager of each department shall create and maintain a document to identify the user or the like who is responsible for controlling each server and terminal used in the department.
4. The information security technical manager of each department shall create and maintain documents related to servers and terminals.
5. The information security technical manager of each department shall create and maintain documents related to communication lines and information network devices.

Article 23 (Entity Authentication and Authority Management)

1. The information security technical manager of each department shall set up each server and terminal so that it performs entity authentication when a user or the like attempts to log-in to the server or terminal.
2. The information security technical manager of each department shall perform authority management of a user or the like who has been logged-on to the server or terminal, based on the identification code presented by such user or the like.

Article 24 (Security Measures on Terminals)

1. The information security technical manager of each department shall list specific names of software that are not allowed to be installed or used on terminals in the department. 2. For mobile terminals handling information that needs to be protected, the information security technical manager of each department shall set up the terminals so that protection means equivalent to those used on campus will effectively work when they are used off campus.

Article 25 (Security Measures for Servers)

1. When maintenance of a server is performed via a communication line, the information security technical manager of each department shall ensure that the information to be transmitted is encrypted.
2. The information security technical manager of each department shall designate the software used for provision of services and operation and management of the server.
3. If any other server application than that designated is running, the information security technical manager of each department shall stop the use of such server application. Moreover, all unnecessary functions must be disabled when such a designated server application is used.

Article 26 (Measures for Hybrid Devices)

1. When procuring a hybrid device, the information security technical manager of each department shall establish appropriate security requirements in light of the functions of the device, the environment in which it is to be installed, and the classification and handling restrictions for the information it is to handle. 2. The information security technical manager of each department shall institute measures against information security incidents involving hybrid devices in operation, by applying appropriate settings for the functions of such devices.

Article 27 (Special Purpose Devices)

In the event that there is a threat to a special purpose device due to the information it handles, its methods of use, or its mode of connection to communication lines, etc., the information security technical manager of each department shall institute measures in accordance with the characteristics of the device.

Article 28 (Connection Management)

If the information security manager of the department receives a request for connection to the information network, he/she shall notify the requesting person of acceptance or refusal of such request for connection, and shall give necessary instructions to the requesting person, in accordance with pre-determined information network connection procedures.

Article 29 (Measures for Communication Lines)

1. The information security technical manager of each department shall structure communication lines, considering the risks associated with structuring communication lines (including risks of physical destruction, leakage, or unauthorized alteration of information).
2. For computers that handle information that requires stability, the information security technical manager of each department shall make sure that the communication performance of communication lines and information network devices is high enough to be able to ensure the stability of information, taking into account the possibility that requirements may become stricter in the future.
3. The information security technical manager of each department shall divide servers and

terminals into separate groups, according to security levels and responsible units, etc., and shall separately control these groups of servers and terminals on logically or physically separate communication lines.

4. The information security technical manager of each department shall examine the communication requirements for each group of servers and terminals, and perform access control and path control in accordance with such requirements, by using information network devices.
5. For information systems that handle confidential information, the information security technical manager of each department shall consider whether or not encryption is necessary for transmission of such information via communication lines. If he/she deems it necessary, the information transmitted must be encrypted.
6. For information systems that handle information that needs to be protected, the information security technical manager of each department shall examine and select proper physical security measures used for communication lines.
7. The information security technical manager of each department shall ensure secure connections by services used for remote maintenance or diagnosis of information network devices.
8. If a leased-line service of a telecommunications service operator is used, the information security technical manager of each department shall agree with such operator on the security level and service level required and other requirements at the time the contract is concluded.
9. The information security technical manager of each department shall examine whether log management is necessary on information network devices. If he/she deems it necessary, log management shall be implemented.

Article 30 (Information Wall Sockets)

Before installing information wall sockets, the information security technical manager of each department shall examine whether the following measures, among other things, are necessary to ensure information security. If he/she deems it necessary, he/she shall implement any or all of such measures:

(1) Identification of servers and terminals or entity authentication of users and the like attempting to connect to the network;
(2) Acquisition and management of entity authentication records;
(3) Restriction of the range of communication lines accessible via the information wall socket;
(4) Blocking connection to other communication lines while a device is using the information wall socket connection;
(5) Securing confidentiality of the connection method via the information wall socket; and
(6) Management of servers and terminals that use the information wall socket for network connection.

Article 31 (VPN, Wireless LANs, and Remote Access)

1. Before structuring a VPN environment, the information security technical manager of each department shall examine whether the following measures, among other things, are necessary to ensure information security. If he/she deems it necessary, he/she shall implement any or all of such measures:
   (1) Establishment of procedures for request for use or discontinuation of use;
   (2) Encryption of transmitted data;
   (3) Identification of servers and terminals or entity authentication of users and the like attempting to connect to the network;
   (4) Acquisition and management of entity authentication records;
   (5) Restriction of the range of communication lines accessible via VPN;
   (6) Securing confidentiality of the connection method via VPN; and
   (7) Management of servers and terminals that use VPN.
2. Before structuring a wireless LAN environment, the information security technical manager of each department shall examine whether the following measures, among other things, are necessary to ensure information security. If he/she deems it necessary, he/she shall implement

any or all of such measures:
(1) Establishment of procedures for request for use or discontinuation of use;
(2) Encryption of transmitted data;
(3) Identification of servers and terminals or entity authentication of users and the like attempting to connect to the network;
(4) Acquisition and management of entity authentication records;
(5) Restriction of the range of communication lines accessible via wireless LAN;
(6) Blocking connection to other communication lines while a device is using a wireless LAN connection;
(7) Securing confidentiality of the connection method via wireless LAN; and
(8) Management of servers and terminals that use wireless LAN connection.

3. Before structuring a remote access environment via a public telephone network, the information security technical manager of each department shall examine whether the following measures, among other things, are necessary to ensure information security. If he/she deems it necessary, he/she shall implement any or all of such measures:
(1) Establishment of procedures for request for use or discontinuation of use;
(2) Identification and entity authentication of the user or the caller's phone number;
(3) Acquisition and management of entity authentication records;
(4) Restriction of the range of communication lines accessible via remote access;
(5) Blocking connection to other communication lines while a device is using the remote access connection;
(6) Securing confidentiality of the connection method via remote access; and
(7) Management of computers that use remote access connection.

Article 32 (Measures for E-mail Servers)

1. The information security technical manager of each department shall institute measures to prevent the e-mail server from performing unauthorized relaying of e-mail.
2. The information security technical manager of each department shall structure the e-mail server so as to ensure that entity authentication is conducted when users and the like send and receive e-mail.
3. The information security technical manager of each department shall institute measures to prevent e-mail impersonation.

Article 33 (Measures for Web Servers)

In the management and configuration of web servers, the information security technical manager of each department shall investigate whether or not the following measures are necessary, and institute those considered necessary.

(1) Suspension or restriction of unnecessary web server functions;
(2) Restriction of entities responsible for editing website content;
(3) Management to prevent publication of website content that is irrelevant or disallowed for publication;
(4) Restriction of the terminals used for website content editing, and appropriate management of identification codes and entity authentication information;
(5) Configuration of encryption functions and digital certificate authentication functions in the event that it is necessary to prevent information leakage due to theft during transmission, etc., such as where information concerning individual users of services is transmitted;
(6) Specification of information stored on web servers and confirmation that servers do not store information that is unnecessary for service provision.

Section 3 Operation

Chapter 1 Duties of Department Information Security Technical Managers

Article 34 (Measures Against Security Holes)

1. The information security technical manager of each department shall promptly implement measures as necessary for servers, terminals, and information network devices in such department, based on information concerning security holes received from the Institute for Information Management and Communication, etc.
2. The information security technical manager of each department shall share information with information security technical managers of other departments as necessary in connection with the preceding paragraph.

Article 35 (Measures Against Malware)

The information security manager of the department shall check and review the status of measures implemented against malware, as necessary.

Article 36 (Vulnerability Diagnosis)

The information security technical manager of each department shall conduct vulnerability diagnosis of the information system to maintain the proper security of the system at least once a year in accordance with the directions of the information security manager of the department.

Article 37 (Review and Revision of Rules and Documents)

1. The information security technical manager of each department shall review the rules for ensuring security of servers and terminals, as necessary. Written records of revisions must be maintained to record all revisions made as a result of such review.
2. The information security technical manager of each department shall review the rules for ensuring provision of secure services via communication lines, as necessary. Written records of revisions must be maintained to record all revisions made as a result of such review.
3. If any user or the like who is engaged in the management of servers and terminals is added or removed, the information security technical manager of each department shall reflect such change in the document in which users and the like engaged in management of servers and terminals are identified. A record of such changes shall be maintained.

Article 38 (Resource Management)

To promote comprehensive and systematic utilization of server, terminal, and information device CPUs, disks, information network bandwidth, and other resources within the department, the information security technical manager of each department shall allot these resources adequately to users and the like, considering their respective use status.

Article 39 (Management of Network Information)

The information security technical manager of each department shall receive the domain name(s) and IP addresses used in the information network of the department and other network information from the Institute for Information Management and Communication. He/she shall manage and assign this network information adequately for users and the like, considering their use status.

Article 40 (Security Measures for Servers)

1. The information security technical manager of each department shall periodically check if any changes have been made to the configurations of servers and shall also check the status of software. He/she shall identify what impacts have been or are caused by such changes on the security of the server and take necessary measures to eliminate any negative impacts.
2. The information security technical manager of each department shall examine whether log management is necessary on servers. If he/she deems it necessary, log management shall be implemented.

Article 41 (Measures for Terminals)

The information security technical manager of each department shall periodically investigate the status of software used on terminals within the department, and shall effect improvements if an improper status is found on any terminal.

Article 42 (Security Measures on Communication Lines)

1. The information security technical manager of each department shall periodically check if any changes have been made to the constitution of the communication line, configuration of information network devices, configuration of access control, identification codes, and other relevant matters. He/she shall identify what impacts have been or are caused by such changes on the security of the communication line and take necessary measures to eliminate any negative impacts.
2. If any situation arises where it is difficult to maintain the security of the information system, the information security technical manager of each department shall change the configuration of the communication line to a closed configuration that is independent from communication lines shared by other information systems.

Chapter 2 Duties of Department Information System Technical Staff Members

Article 43 (Measures Against Security Holes)

1. The information system technical staff members of each department shall update the documentation created in accordance with Paragraph 1 of Article 17 for any change in the constitution or set-up of servers and terminals and information network devices.
2. The information system technical staff members of each department shall collect publicly available information on security holes found in software used on servers and terminals and information network devices managed by the department, as necessary.
3. The information system technical staff members of each department shall implement measures against security holes based on the plan for security hole countermeasures.
4. The information system technical staff members of each department shall record implementation dates, specific measures taken, persons who took the measures and other details of measures taken for security holes.
5. The information system technical staff members of each department shall obtain files designed to fix security holes from reliable sources. If the department has a method to verify the integrity of such files, it shall perform verification of the files.
6. The information system technical staff members of each department shall perform periodic checking and analysis of the status of security hole countermeasures and software installed on servers, terminals, and information network devices and, if an improper status is found on any server, terminal or information network device, appropriate measures shall be taken.

Article 44 (Measures Against Malware)

The information system technical staff members of each department shall strive to collect information on malware and decide whether countermeasures are necessary against any malicious program referred to in such information. If specific measures are necessary for such malware, he/she shall give necessary instructions to users and the like regarding implementation of such measures.

Article 45 (Review and Revision of Rules and Documents)

1. If the configuration of any server or terminal is changed, the information system technical staff members of each department shall reflect such change in the documentation relating to such server or terminal. A record of such changes shall be maintained.
2. If the constitution of communication lines, configuration of information network devices, configuration of access control, or matters involving identification codes is changed, the information system technical staff members of each department shall reflect such changes in the documents related to communication lines and information network devices. A record of such changes shall be maintained.

Article 46 (Operation Management)

1. The information system technical staff members of each department shall conduct operation

management of servers and terminals based on the rules for their security maintenance.
2. The information system technical staff members of each department shall conduct daily and periodic operation management based on the rules for ensuring provision of secure services via communication lines.

Article 47 (Security Measures for Servers)
1. The information system technical staff members of each department shall periodically create a backup of information that is stored on the server that handles information requiring stability. The media on which the backup is recorded shall be maintained in a secure way.
2. The information system technical staff members of each department shall record maintenance dates, servers for which maintenance were performed, details of the maintenance work, persons who performed the maintenance, and other details regarding the maintenance of servers.
3. The information system technical staff members of each department shall synchronize the server time with the standard time used in the information system.

Article 48 (Security Measures on Communication Lines)
1. The information system technical staff members of each department shall manage identification codes of servers and terminals that use the communication line, the users and the like of servers and terminals, the identification codes of such users and the like, the departments that use the communication line, and other relevant information.
2. The information system technical staff members of each department shall not allow any server, terminal, or information network device that has not been approved by the information security technical manager to connect to the communication line.
3. For information systems that handle information requiring stability, the information system technical staff members of each department shall routinely check and analyze the use condition and status of the communication line, and infer or detect performance degradation or troubles on the communication line based on such analysis.
4. The information system technical staff members of each department shall synchronize the time of information network devices with the standard time used in the information system.

Section 4 Discontinuation of Use

Article 49 (Security Measures on Devices, etc.)
When use of a device or the like is discontinued, the information security technical manager of each department shall convert all data stored on such device or the like to a non-restorable condition, by means of data elimination software or a data elimination device, physical destruction, magnetic destruction, or any other appropriate method.

Section 5 Use of Information Systems

Article 50 (Basic Measures)
1. Users and the like shall not use information systems for purposes other than education, research, and other activities of the University.
2. Users and the like shall not connect on-campus information systems to communication lines other than those for which connection permission has been granted by the department information security technical manager.
3. Users and the like shall not connect to any on-campus information systems for which connection permission has not been granted by the department information security technical manager.
4. Users and the like shall not use any software that is prohibited for use on information systems. Authorization of the department information security technical manager shall be obtained in the event that it is necessary for work purposes to use software other than that permitted for use on

information systems.

5. Users and the like shall institute measures to protect information systems from unauthorized operation in the event that there is a risk of unauthorized operation by a third party, such as when the user or the like is absent from the place of installation of the information system.
6. When processing information on terminals which handle information that needs to be protected, users and the like shall institute appropriate measures in accordance with the handling restrictions for such information.
7. When removing from secure areas information systems installed in secure areas which handle information that needs to be protected, users and the like shall institute appropriate measures in accordance with the handling restrictions for such information.
8. When discontinuing use of a terminal, users and the like shall, in accordance with Article 49, convert to a non-restorable condition all information stored on the terminal that needs to be protected.

Article 51 (Measures Against Malware)

1. Users and the like shall work on measures related to prevention of infection by malware.
2. In the event that users and the like become aware that an information system may be infected by malware, they shall institute necessary measures such as promptly disconnecting the infected information system from communication lines.

Article 52 (Measures Regarding Use of E-mail and Websites)

1. When sending and receiving e-mail containing information that needs to be protected, users and the like shall use e-mail services provided via e-mail servers managed or outsourced by the University.
2. When sending information by e-mail to a party outside the University, users and the like shall use the University's domain name as the domain name for such e-mail transmission. However, this shall not apply in cases where the user or the like is already known to the external party.
3. When receiving suspect e-mail, users and the like shall deal with them in accordance with predetermined procedures.
4. When it is necessary to review Web client configurations, users and the like shall not make changes to such configurations that could affect information security.
5. When downloading software to servers or terminals operated by Web clients, users and the like shall use electronic signatures, etc. to confirm the legitimacy of the software distributors.
6. Users and the like shall confirm the following when inputting and sending confidential information in forms displayed on websites that they are viewing.
   (1) The information being sent is encrypted.
   (2) The website belongs to the organization to which the information is intended to be sent.

Article 53 (External Electromagnetic Recording Media)

Users and the like shall observe the following in regard to handling of information using external electromagnetic recording media.

(1) External electromagnetic recording media supplied by the University shall be used when information classification or handling restrictions are specified.
(2) Security functions such as entity authentication and encryption shall be used in cases where the external electromagnetic recording media offer such functions.
(3) Confidential information shall be deleted promptly when storage thereof is no longer necessary.
(4) Anti-malware software shall be used for quarantining and eradication before external electromagnetic recording media are used.

Article 54 (Handling of Identification Codes and Entity Authentication Information)

1. Users and the like shall not use information systems using identification codes other than those assigned to them upon entity authentication.
2. Users and the like shall appropriately manage identification codes assigned to them.
3. When identification codes with attached administrator authorities are assigned to them, users

and the like shall use such codes only to the extent necessary for performing their duties as administrators.

4. Users and the like shall manage their own entity authentication information with the utmost care.

Chapter 3 Outsourcing

Article 55 (Scope of Outsourcing)

The information security technical manager of each department may outsource the following work if permitted to do so under the classification and handling restrictions for the information being handled.

(1) Information system design and development
(2) Information system operation, maintenance, and checking
(3) Information production and processing
(4) Information storage and transportation

Article 56 (Outsourcing Contracts)

1. When outsourcing work, the department information security technical manager shall select a contractor in accordance with the following standards:
   (1) Capacity to comply with the provisions of these Standards;
   (2) Provision of information security management systems equivalent to these Standards;
   (3) Implementation of education for the contractor's employees on information security measures equivalent to these Standards.
2. The department information security technical manager shall include implementation of the following information security measures as conditions for selection of a contractor and as part of the contractor's specifications.
   (1) Prohibition of use of information provided to the contractor for purposes other than the intended purposes;
   (2) Preparation of implementation details and management systems for information security measures by the contractor;
   (3) Preparation of management systems to ensure that no unintended changes are made by the contractor, its employees, its subcontractors, or any other parties in the course of implementing the outsourced work;
   (4) Provision of information on the contractor's capital relationship, officers, etc., the places of implementation of the outsourced work, and the affiliations, expertise (information security qualifications, training, etc.), experience, and nationalities of the persons engaged in the outsourced work;
   (5) Measures for responding to information security incidents;
   (6) Methods for confirming the performance of information security measures and other contractual provisions;
   (7) Methods for dealing with inadequate performance of information security measures.
3. The department information security technical manager shall include the following in the contractor's specifications as necessary in light of the classification, etc. of information handled in the outsourced work.
   (1) Submission to information security auditing;
   (2) Service level guarantees; and
   (3) In the event that the contractor handles information that needs to be protected, implementation of measures equal or greater to those listed in paragraph 1 of Article 21 in the area where the information system is installed.
4. In the event that a contractor entrusts a subcontractor to perform some of its services, the department information security technical manager shall require such subcontractor to guarantee that the measures in the preceding two paragraphs are implemented in order to ensure that adequate information security is maintained against threats that could arise through such subcontracting.

Article 57 (Implementation of Measures in Outsourcing)

1. The department information security technical manager shall confirm the contractor's performance of information security measures in accordance with the contract.
2. In the event that the department information security technical manager becomes aware of the occurrence of an information security incident or use of information for a purpose other than the purpose intended in the course of a contractor's work, or receives a report of such occurrence or use from faculty members or office personnel, the department information security technical manager shall institute the necessary measures, such as suspending use of the service in question, and shall require the contractor to institute the necessary measures in accordance with the contract.
3. The department information security technical manager shall confirm that information handled by the contractor has been fully returned or erased upon completion of the outsourced work.

Article 58 (Handling of Information in Outsourcing)

Faculty members and office personnel shall comply with the following when providing information to contractors.

(1) When providing contractors with information that needs to be protected, the provided information shall be limited to the minimum necessary, and safe handover methods shall be used in accordance with Article 68;

(2) When contractors no longer require provided information that needs to be protected, they shall be required to return or delete such information, without fail;

(3) Upon becoming aware of the occurrence of an information security incident or use of information for a purpose other than the purpose intended in the course of a contractor's work, such occurrence or use shall be promptly reported to the information security technical manager of the department concerned.

Article 59 (Use of External Services Subject to Terms and Conditions)

1. Faculty members and office personnel may use external services subject to terms and conditions when permitted to do so under the classification and handling restrictions for the information being handled and after instituting appropriate measures pursuant to confirmation that use-related risks can be accepted in light of the terms and conditions of the service used and other conditions of provision of such services. However, the information security manager of the department shall be notified of such use in advance if it involves handing of information that needs to be protected.
2. When using external services subject to terms and conditions faculty members and office personnel shall specify a responsible person for each use. However, the information security manager of the department shall specify a responsible person if such use involves handing of information that needs to be protected.
3. Responsible persons under the preceding paragraph shall conduct such use paying attention to the following matters:

(1) Periodic checks of service function settings;

(2) Institution of backups to provide against information loss, damage, etc.;

(3) Raising awareness among users.

Article 60 (Measures for Transmission of Information Using Social Media Services)

1. When social media services are used by a department for transmission of official information, the information security technical manager of the department shall specify a responsible person for each social media service used.
2. Responsible persons under the preceding paragraph shall take the following measures against impersonation in order to make it possible to ascertain that the transmission of information via the account used is actually performed by the University.

(1) In order to clarify that the information is being transmitted by the University, account names, account descriptions, etc., shall be used to indicate that the account is operated by the University.

(2) In order to clarify that the information is being transmitted by the University, a Web page shall be established, within a website managed by the University and using the University's domain

name, that specifies the names of social media services used and the account names used in those services, and/or provides hyperlinks to said account pages.

(3) The account description section of the social media account to be operated shall include the URL of a page on the University website that states that the account concerned is operated by the University.

(4) Wherever possible, a so-called “verified account” (or “official account”) in which the social media service provider verifies and publishes the name of the account administrator shall be used.

(5) URL shortening services shall not be used except where such use cannot be avoided, such as where the social media used has an automatic URL shortening function.

3. In order to avoid so-called “account hijacking” whereby a third party engages in unauthorized conduct such as transmission of false information following unauthorized log-in to an account by some means, responsible persons under Paragraph 1 shall take the following measures in regard to log-in passwords and authentication methods for social media accounts:

(1) Passwords shall be managed appropriately. Specifically, log-in passwords shall be of sufficient length and complexity, knowledge of the password restricted, and the same password not shared among multiple users.

(2) Account authentication enhancement measures, such as two-step authentication and one-time passwords, shall be used wherever available.

(3) Terminals used for logging in to social media shall be managed rigorously, in light of the possibility that, if lost or stolen, such terminals could be fraudulently used for account hijacking.

(4) If unauthorized access is gained to a terminal used for logging in to social media, there is a possibility of unauthorized remote operation of the terminal or theft of passwords stored on the terminal. Appropriate security measures shall be implemented in order to prevent such occurrences. At a minimum, these measures shall include application of the latest security patches and introduction of anti-malware software on such terminals.

4. In the event that account hijacking is detected, in order to minimize damage, responsible persons under Paragraph 1 shall promptly alter log-in passwords, suspend accounts, and post announcements on self-managed websites, etc., as well as carrying out appropriate responses in accordance with procedures established pursuant to the provisions of Paragraph 3 of Article 97.

5. In the event that a user impersonation is detected, the information security manager of the department shall use the University website to announce the impersonating account and that the social media service in question is not being used, and use reliable outlets and media to raise awareness of the problem.

6. When using a social media service to provide information requiring stability, faculty members and office personnel shall also provide the same information on a website managed by the University.

Article 60-2 (Measures in the Use of Cloud Services)

The department information security technical manager shall implement the following measures in the use of cloud services.

(1) Determine whether or not to entrust the handling of information in light of its classification and handling restrictions.

(2) Select contractors after evaluating the risks of application of laws and regulations other than those of Japan in relation to the information to be handled by the cloud service, and as necessary specify the locations at which the outsourced work is to be conducted and the applicable laws and courts of jurisdiction stipulated contractually.

(3) Consider measures for smooth transfer of work upon the cessation or termination of the cloud service, and require these measures when selecting contractors.

(4) Taking into account the characteristics of the cloud service, design security measures with an overview of information distribution channels as a whole, and stipulate requirements to ensure that security is properly maintained throughout all information distribution channels including the cloud service components thereof.

(5) Evaluate and determine in a comprehensive and objective manner that the cloud service and the provider of that service are sufficiently reliable, by reference to the content of information

security audit reports relating to the cloud service and the application of various approval and accreditation systems.

Chapter 4 Classification and Handling of Information

Article 61 (Creation or Acquisition of Information)

Faculty members and office personnel shall pay keen attention to the purpose of execution of the education, research, and other activities of the University when creating or acquiring information related to the information system.

Article 62 (Determination of Classification and Handling Restrictions on Information Created or Acquired)

1. When creating information, faculty members and office personnel shall assign a classification to the information and decide whether handling restrictions should be placed on such information, in accordance with the Kyoto University Information Classification Standards (hereinafter the “Classification Standards”), based on the confidentiality, integrity, and availability of the information.
2. When managing information acquired from parties outside the University, faculty members and office personnel shall assign classifications to such information and decide if handling restrictions should be placed on such information, in accordance with the Classification Standards, based on the confidentiality, integrity, and availability of the information.

Article 63 (Indication of Classification and Handling Restrictions)

Faculty members and office personnel shall indicate the classification and handling restrictions assigned to each piece of information in a manner that specifies the persons authorized to access the information, and indicate the handling restrictions placed on such information, as necessary.

Article 64 (Succession of Classification and Handling Restrictions)

If information that has been assigned with a classification is quoted or used in newly created information, faculty members and office personnel shall succeed such classification and handling restrictions to the newly created information.

Article 65 (Changes in Classification and Handling Restrictions)

1. If faculty members and office personnel consider that the classification assigned to certain information should be changed, they shall consult with the originator or acquirer of such information. If such originator or acquirer determines that the classification should be changed, he/she shall reassign a proper classification to the information.
2. If faculty members and office personnel consider that the handling restrictions placed on certain information should be changed, they shall consult with the originator or acquirer of such information. If such originator or acquirer determines that the handling restrictions should be changed, he/she shall place proper handling restrictions on the information.

Article 66 (Use of Information in Accordance with Classification)

1. Faculty members and office personnel shall handle information appropriately in accordance with the classification and handling restrictions indicated in the information.
2. When handling information using external electromagnetic recording media, faculty members and office personnel shall manage the information appropriately in accordance with the provisions of Article 53.

Article 67 (Safekeeping of Information According to Classification)

1. The information security technical manager of each department shall implement proper access control to information that needs to be protected.
2. The information security technical manager of each department shall consider whether measures against disaster should be taken for safekeeping of backups of electromagnetic and

optical records or copies of important design specifications, which are data that require integrity or stability, and shall take necessary measures to prevent the loss of both originals and backups/copies at the same time as a result of disaster, as necessary.

3. The information security technical manager of each department shall establish servers in secure areas for information systems handling information that needs to be protected.

Article 68 (Transportation and Sending of Information)

1. When removing information that needs to be protected from a secure area and transporting it to another location, or when sending such information using off-campus communication lines, faculty members and office personnel shall determine transport or sending methods with a view to ensuring security, and shall institute measures appropriate for ensuring security in accordance with the classification and handling restrictions for such information.
2. When removing from a secure area a recording medium on which information that needs to be protected is recorded or printed, faculty members and office personnel shall determine transport methods with a view to ensuring security, and shall institute measures appropriate for ensuring security in accordance with the classification and handling restrictions for such information.
3. When sending an electromagnetic record containing information that needs to be protected by e-mail, etc., faculty members and office personnel shall determine sending methods with a view to ensuring security, and shall institute measures appropriate for ensuring security in accordance with the classification and handling restrictions for such information.

Article 69 (Deletion of Information)

1. Faculty members and office personnel shall promptly delete information stored on electromagnetic recording media when it is no longer required for work purposes.
2. When destroying electromagnetic recording media, faculty members and office personnel shall ensure that no information remains within the media, by erasing all information so it cannot be restored.
3. When disposing of confidential information that is in written form, faculty members and office personnel shall convert such material to a non-restorable condition.

Article 70 (Information Backup)

1. Faculty members and office personnel shall implement information backups using appropriate methods in accordance with the classification of the information.
2. Faculty members and office personnel shall appropriately manage backups of information that they obtain, determining storage locations, methods and periods in accordance with the classification and handling restrictions for such information.
3. Faculty members and office personnel shall delete, erase, or dispose of information backups using appropriate methods after expiration of the storage period.

Chapter 5 Entity Authentication

Article 71 (Implementation of Entity Authentication Function)

1. The information security technical manager of each department shall determine whether entity authentication is necessary for each information system. For information systems that handle information that needs to be protected, entity authentication shall be conducted.
2. The information security technical manager of each department shall provide identification and entity authentication functions for all information systems that are determined requiring entity authentication.
3. The information system technical staff members of each department shall control such entity authentication information used in such information systems requiring entity authentication so that the information is not known to any unauthorized person. Such control includes:
   (1) Encryption of entity authentication information when it is stored;
   (2) Encryption of entity authentication information when it is transmitted; and
4. If it is necessary in such information system requiring entity authentication to ask users and the like to periodically change their entity authentication information, the information security

technical manager of each department shall provide in the system a function to periodically prompt users and the like to make such change. In addition, any of the following functions shall also be provided:

(1) A function to check that users and the like have changed their entity authentication information periodically; or
(2) A function to suspend the use of the information system if a user or the like has not changed his/her entity authentication information periodically.

5. In information systems that are determined to require entity authentication, the information security technical manager of each department shall provide a function that if a user or the like becomes aware that his/her entity authentication information or IC card or any other similar item on which his/her entity authentication information is stored was, or may be, used by any other person, the system suspends entity authentication by using such entity authentication information or such IC card on which his/her entity authentication information is stored or suspends access to the information system by using the identification codes stored on such IC card.
6. In information systems that are determined to require entity authentication, if entity authentication by knowledge of personal information is used, the information security technical manager of each department shall provide the following functions:
   (1) A function enabling a user or the like to set up his/her entity authentication information; and
   (2) A function to make sure that entity authentication information set by the user or the like is not easily known by other persons.
   (3) A function to require a specified minimum level of security strength when setting entity authentication information.
7. In information systems requiring entity authentication, if any entity authentication method other than authentication by knowledge, possession of an identification item, or biometric information is used, the information security technical manager of each department shall verify that the method satisfies all the following requirements in addition to other requirements applicable to such authentication method. Requirements for such authentication method shall be established, including but not limited to the following requirements:

   Such entity authentication method shall be designed so that
   (1) No entity other than the authentic entity shall be authenticated by mistake (Prevention of authentication by mistake);
   (2) Entity authentication by an authentic entity shall not be refused for any reason not attributable to such authentic entity (Prevention of refusal by mistake);
   (3) The authentic entity shall not easily be able to assign or lend his/her entity authentication information to other persons (Prevention of agency);
   (4) Entity authentication information shall not easily be reproduced (Prevention of reproduction);
   (5) Any information system technical staff member may disable the log-in capabilities of any person based on such staff member’s judgment (Disabling function);
   (6) The entity authentication method has sufficient availability for use in the operation (Availability for service);
   (7) If provision of information or equipment from external sources is necessary to add new entities, such provision shall be fully continued during the service life of the information system (Continuity); and
   (8) If entity authentication information assigned to an entity cannot be used for any reason, new entity authentication information shall be able to be reissued safely to such authentic entity (Reissuance ability).
8. To issue an entity authentication storage device for carrying out entity authentication by possession of an identification item on an information system that has been determined to require entity authentication, the information security manager of the department shall establish a procedure for issuing and returning such devices.
9. If biometric information is used for entity authentication, the information security technical manager of each department shall not use such biometric information for any other purpose than

as agreed by the relevant entity in advance. Use of such biometric information shall not infringe the privacy of the relevant entity.

10. If the information security manager of the department becomes aware of a case of security invasion or possibility of security invasion, he/she may ask the relevant authentic entity to change his/her entity authentication information, or void the account of such entity.

Chapter 6 Access Control

Article 72 (Implementation of Access Control Function)

1. The information security technical manager of each department shall determine whether access control is necessary for each information system. For information systems that handle information that needs to be protected, access control shall be conducted.
2. The information security technical manager of each department shall provide access control functions in all information systems that are determined requiring access control.

Article 73 (Proper Access Control)

1. The information security technical manager of each department shall instruct users and the like to take access control measures appropriate for the information system they use.
2. Faculty members and office personnel shall use the function provided by the information system to set up necessary access control, based on the classification and handling restrictions assigned to and placed on information stored on such information system.

Article 74 (Security Measures Against Unauthorized Access)

1. If the information security technical manager or an information system technical staff member of the department becomes aware of any unauthorized access, he/she shall promptly report to the information security manager of the department and the Information Network Risk Management Committee. Upon receipt of such report, the information security manager of the department shall promptly report to the Chief Information Security Officer of such incident.
2. Upon receipt of the report in accordance with Paragraph 1 above, the Chief Information Security Officer and the information security manager of the department shall implement additional measures necessary to block such or similar unauthorized access.

Chapter 7 Account Management

Article 75 (Implementation of Account Management Function)

1. The information security technical manager of each department shall determine whether account management is necessary for each information system. For information systems that handle information that needs to be protected, account management shall be conducted.
2. The information security technical manager of each department shall provide account management functions in all information systems that are determined requiring account management.

Article 76 (Establishment of Account Management Procedures)

1. The information security technical manager of each department shall establish detailed account management procedures for all information systems that are determined requiring account management, including:
   (1) If account management is conducted based on applications submitted by entities, procedures to verify that an applicant is the authentic entity;
   (2) The method of delivering the newly issued entity authentication information to the authentic entity, and procedures for managing changes in such information; and
   (3) The method of setting up access control information and procedures for managing changes in such information.
2. The information security technical manager of each department shall appoint a person

responsible for account management for each information system that is determined requiring account management.

Article 77 (Shared Accounts)

1. The information security technical manager of each department shall determine whether use of a shared account is necessary for each information system that is determined requiring account management.
2. When issuing an account for each information system that is determined requiring account management, the person responsible for account management shall indicate to the user or the like receiving such account whether it is a shared account or an account unique to such entity. When a shared account is issued, such shared account may be used only on the information system(s) allowed by the information security technical manager of the department to use the shared account.

Article 78 (Issuance of Accounts)

1. Upon receipt of an application for account issuance from a user or the like, the person responsible for account management shall promptly issue an account to such applicant unless the application is submitted during a period in which a direction for account suspension or deletion, as stipulated in Article 95.3.(3), is imposed on such applicant.
2. The person responsible for account management shall issue an account only to an entity authorized to use such information system that is determined requiring account management.
3. When issuing an account, it is desirable for the person responsible for account management to issue a tentative password with a time limit or take another similar measure.
4. In an information system that is determined requiring account management, the person responsible for account management may issue an account assigned with administrator authority only to the extent necessary for the operation or duties related to the operation.
5. In an information system that is determined requiring account management, the person responsible for account management shall set up the access control configuration to the minimum extent necessary, considering operational duties and necessity.

Article 79 (Report of Issuance of Accounts)

1. When an account is issued, the person responsible for account management shall promptly report to the information security technical manager of the department.
2. The information security manager of each department may request the department information security technical manager to submit a report of account issuances, as necessary.

Article 80 (Verification of Account Validity)

1. The person responsible for account management shall periodically check for issued accounts falling under any of the following conditions:
   (1) Accounts whose use authority has expired or been revoked;
   (2) Accounts whose deletion and retention periods specified by the information security manager of the department have expired;
   (3) Accounts assigned with passwords not conforming to password rules; or
   (4) Accounts that have not been used for a specified period.
2. When an account is added or deleted due to personnel transfer or any other reason, the person responsible for account management shall check that no improper access control is set up for such account.

Article 81 (Deletion of Accounts)

1. If the person responsible for account management finds any account that falls under Article 80.1.(1) or (2), or receives directions to delete an account in accordance with Article 95.3.(3), he/she shall delete such account promptly and report thereof to the information security manager of the department.
2. In an information system that is determined requiring account management, if a user or the like no longer needs to use the information system, the person responsible for account management

shall delete the account of such user or the like, and report thereof to the information security manager of the department.
3. Upon receipt of the report in accordance with Paragraph 2 above, the information security technical manager of the department shall promptly deliver notice of account deletion to the user or the like whose account has been deleted concerning the report, unless such person cannot be contacted by e-mail, telephone, postal mail, or any other reasonable means.
4. The information security manager of each department may request the department information security technical manager to submit a report of account deletions, as necessary.

Article 82 (Suspension of Accounts)
1. If the person responsible for account management finds any account that falls under Article 80.1.(3) or (4), or receives directions to suspend an account in accordance with Article 95.3.(3), or receives a report that entity authentication information of an entity was, or may be, used by an unauthorized person, he/she shall suspend such account promptly and report thereof to the information security manager of the department.
2. Upon receipt of the report in accordance with Paragraph 1 above, the information security manager of the department shall promptly deliver notice of such suspension to such user or the like, unless such person cannot be contacted by e-mail, telephone, postal mail, or any other reasonable means.
3. The information security manager of each department may request the department information security technical manager to submit a report of account suspensions, as necessary.

Article 83 (Reinstatement of Accounts)
1. If the user or the like who received suspension of his/her account wishes reinstatement of his/her account, he/she shall request the information security manager of the department for such reinstatement.
2. Upon receipt of the request referred to in Paragraph 1 above, the information security manager of the department shall instruct the person responsible for account management to check such account's safety and investigate the possibility of reinstating it.
3. The person responsible for account management shall check such account's safety and investigate the possibility of reinstating it in accordance with the instructions given in the preceding paragraph, and promptly reinstate it if it is to be reinstated.

Article 84 (Use of an Account Assigned with Administrator Authority)
Any person who is assigned with an account attached with administrator authority shall use such account only to the extent necessary for performing his/her duties as administrator.

Chapter 8 Management of Trace Logs

Article 85 (Implementation of Trace Log Management Function)
1. The information security technical manager of each department shall determine whether management of logs of event traces is necessary for each information system.
2. In information systems that are determined to requiring trace logs, the information security technical manager of each department shall provide a function to collect traces of events to conduct trace log management.
3. In information systems that are determined to require the collection of trace logs, the information security technical manager of each department shall set up the information system so that necessary information items are recorded for each event when such event is logged as a trace.
4. In information systems that are determined to require trace logs, the information security technical manager of each department shall establish an action policy to be followed when the department's system cannot, or may become unable to collect trace logs, and shall provide a function in the information system for coping with such situation, as necessary.
5. In information systems that are determined to requiring trace logs, the information security technical manager of each department shall place access control on collected trace logs so that

no unauthorized deletion, alteration or access is made to collected trace logs, and shall properly manage trace logs recorded on an electromagnetic recording medium or other device or medium.

Article 86 (Collection and Retention of Trace Logs by Department Information System Technical Staff Members)

1. In information systems that are determined to require trace logs, the information system technical staff members of each department shall log traces of an event, by using a function provided by the information security technical manager of the department in the information system.
2. In information systems that are determined to require trace logs, the information system technical staff members of each department shall set a retention period for collected trace logs, and retain such trace logs until the end of such retention period. Logs shall be promptly deleted upon expiration of such retention period unless extension of the period is necessary.
3. In information systems that are determined to require trace logs, if the system cannot, or may become unable to, collect trace logs, the information system technical staff members of each department shall take the actions prescribed in Paragraph 4 of the preceding article.

Article 87 (Advance Notification of Trace Log Management to Users and the Like)

In information systems that are determined to require trace logs, the information security manager or the information security technical manager of each department shall notify to information system technical staff members of the department and users and the like in advance that trace logs may be collected by the system and retained, checked, and analyzed.

Article 88 (Monitoring of Communications)

1. The scope of monitoring as stipulated in Article 13.1 of the Regulations shall be limited to the extent necessary for ensuring security of the information system and shall not include unnecessary monitoring of contents of communications, and such scope of monitoring shall be specifically designated by the Chief Information Security Officer or the information security manager of the department who instructs such monitoring. Provided, however, that if monitoring of contents of specific information is deemed necessary to cope with a specific incident, the Chief Information Security Officer or the information security manager of the department may give directions to monitor the contents of such information, considering the urgency, nature and extent of security invasion by such incident.
2. For monitoring within the scope specified in the first sentence of Paragraph 1 above, as the procedures stated in Article 13.1 of the Regulations, the matter shall go through deliberation by the University Information Security Committee in advance if the Chief Information Security Officer instructs that such monitoring be carried out, or deliberation by the department's information security committee in advance if the information security manager of the department gives orders for such monitoring. For monitoring conducted in accordance with the proviso of Paragraph 1 above, the person who gives directions for such monitoring shall listen to the opinions of persons designated in accordance with Article 13.1 of the Regulations before giving directions for monitoring or investigation, and shall receive a report of the results of such monitoring or investigation.
3. Information stipulated in Article 13.2. of the Regulations shall be limited to information that leads to identification of a person involved in the security invasion and is deemed necessary to cope with such security invasion considering its urgency, nature and extent. Such information stipulated in Article 13.2. of the Regulations shall be disclosed to relevant parties in accordance with the procedures and criteria for material security invasion designated by the person who has given directions of monitoring.
4. “Persons” stipulated in Article 13.2 of the Regulations shall be the Information Network Risk Management Committee and the Information Network Ethics Committee.
5. Records of information collected through monitoring (hereinafter "monitoring records") shall be designated as information that needs to be protected, and the person who has directed such monitoring shall be named as the creator of such information.

6. The person who gives directions of such monitoring shall designate and notify in advance to the persons who perform such monitoring the period during which monitoring records shall be retained. The persons who perform monitoring shall destroy monitoring records immediately upon expiration of their designated retention period. However, such monitoring records may be retained after the designated period as reference materials for future network operation and management, by deleting the portions relating to personal information. It is desirable that these materials are kept in an organized manner so that they can be made available whenever needed.
7. The persons who perform such monitoring and persons who receive monitoring records may inspect and save such monitoring records only to the extent necessary for network operation and management. Unnecessary inspection of monitoring records shall not be made. Monitoring records that are no longer necessary shall be immediately destroyed. The contents of monitoring records shall not be disclosed to any other person unless otherwise required by law or statutory regulations or other similar situation.

Article 89 (Use Records)

1. An information system technical staff member of the department who manages information devices used by more than one person (hereinafter the "information device manager") may collect use records (hereinafter "use records") relating to such information devices to the extent necessary for purposes designated in advance. No unnecessary collection of use records that are not relevant to such designated purposes shall be permitted.
2. Such purposes as referred to in Paragraph 1 above shall be limited to purposes necessary for the use of such information devices, including compliance with laws and regulations, information security, and charging of use fees to users. Use records shall not be collected for the purpose of collecting personal information, unless the information security manager of the department that manages such information devices deems that collection of personal information from use records is necessary for educational purposes.
3. Use records shall be designated as confidential information requiring integrity, and the information device manager shall be named as the creator of such information, except for use records otherwise designated by the information security manager of the department.
4. The information device manager may inspect user records only to the extent necessary for fulfilling the purposes specified in Paragraph 1 above. However, unnecessary inspection of other persons' personal information and contents of communication shall not be made.
5. Such information device manager may disclose use records to other persons to the extent necessary to fulfill the purposes specified in Paragraph 1 above.
6. The person who collects use records of information devices in accordance with Paragraph 1 above shall notify the information security manager of the department and the user of the device in advance, of the purpose of the use record, which shall be any of the purposes as specified in Paragraph 1; the scope of information collected by the use record; and persons to which such use record may be disclosed in accordance with Paragraph 5 above. If the information security manager of the department determines that any portion of such use record is inappropriate, such inappropriate portion shall be corrected.
7. The information device manager and the person who has received disclosure of such use records may keep those records to the extent necessary for fulfilling the purposes as specified in Paragraph 1 above. Use records that are no longer necessary shall be immediately destroyed. However, such use records may be retained by the information device manager as reference materials for future network operation and management, by deleting the portions relating to personal information. It is desirable that these materials are kept in an organized manner so that they can be made available whenever needed.

Article 90 (Collection and Management of Personal Information)

1. When a person is asked to provide his/her personal information by any electronic means, the scope of information requested, the purpose of use of such information, and the scope of persons to whom such information may be disclosed shall be notified to such person in advance.
2. Upon request from the person who has provided his/her own personal information, the personal

information collected in accordance with Paragraph 1 above shall be disclosed to such requesting person, modified or deleted, and procedures therefor shall also be indicated.
3. The information security technical manager of each department shall institute necessary measures to enable detection of improper removal of personal information handled by the information system according to the contents of such information.
4. The information security technical manager of each department shall institute necessary measures to limit the number of terminals used to process personal information handled by the information system according to the contents of such information.

Article 91 (Protection of Information Possessed by Users and the Like)
Information possessed by users and the like may be inspected, reproduced or provided only to the extent necessary for the operation of the information system or for coping with an incident.

Chapter 9 Encryption and Electronic Signatures

Article 92 (Adoption of Encryption Function and Function to Assign Electronic Signature)
1. For information systems that handle confidential information (excluding written documents), the information security technical manager of each department shall consider whether an encryption function should be provided in the system.
2. The information security technical manager of each department shall provide an encryption function in all information systems that are determined requiring encryption.
3. For information systems that handle information requiring integrity, the information security technical manager of each department shall consider whether a function to assign an electronic signature should be provided in the system.
4. The information security technical manager of each department shall provide an electronic signature assignment function in all information systems that are determined requiring electronic signatures.
5. In choosing an algorithm for the information system determined to require encryption or assignment of electronic signatures, the information security technical manager of each department shall examine the safety and reliability levels necessary for the system, and shall choose an algorithm included in the list of electronic government-recommended ciphers, if possible. However, if an algorithm for encryption or electronic signature is newly adopted (including renewal), an algorithm shall be chosen from the list of electronic government-recommended ciphers or the list of the University's proven ciphers (if such list has been created). If such encryption or electronic signature function is designed to be able to choose more than one algorithm, at least one algorithm shall be chosen from those lists.

Article 93 (Management of Encryption and Assignment of Electronic Signatures)
1. In an information system determined to require encryption or assignment of electronic signatures, the information security technical manager of each department shall establish procedures for creating a key used for decryption of encrypted information or a key for assignment of electronic signatures, the valid period of the key, procedures for abandonment or renewal of the key, procedures that should be followed if the key is revealed, and any other relevant matters.
2. In an information system determined to require encryption or assignment of electronic signatures, the information security technical manager of each department shall designate a storage medium or storage location for the key used for decryption of encrypted information or they key for assignment of electronic signatures.
3. In an information system determined to require assignment of electronic signatures, the information security technical manager of each department shall provide to the signature verifier, by a secure method, information or the means of verifying the validity of electronic signatures.
4. In an information system using encryption or an information system using assignment or verification of electronic signatures, the information security technical manager of each department shall periodically obtain information on any compromising of the algorithms chosen

for encryption or electronic signature and share that information with users and the like as necessary.

Article 94 (Measures for Faculty Members and Office Personnel when Using Encryption and Electronic Signatures)

1. When encrypting information or assigning electronic signatures to information, faculty members and office personnel shall follow the predetermined algorithms and methods.
2. Faculty members and office personnel shall manage keys used for decryption of encrypted information or assignment of electronic signatures appropriately in accordance with predetermined key management procedures.
3. Faculty members and office personnel shall conduct backups of keys used for decryption of encrypted information in accordance with key backup procedures.

Chapter 10 Infringements and Exceptions

Article 95 (Actions Against Infringements)

1. If users and the like become aware of cases of material infringement of any information security-related regulation, they shall report it to the information security manager of the department concerned.
2. If the information security manager of the department receives a report, or becomes aware, of a case of material infringement of any information security-related regulation, he/she shall promptly investigate the case to determine the facts relevant to such case. To determine the facts, the opinions of the person who has committed such infringement shall be heard as far as practically possible.
3. If it is found as a result of the investigation that an infringement was committed, the information security manager of the department may take any of the following measures:
   (1) Issue directions to the infringer to stop such infringing act;
   (2) Issue directions to the information security technical manager of the department to block the information transmission involved in such infringing act;
   (3) Issue directions to the information security technical manager of the department to suspend or delete the account of such infringer;
   (4) Take any other measures in accordance with relevant laws and regulations.
4. For measures stipulated in Items (2) and (3) in Paragraph 3 above, the information security manager of the department may request such measures via the information security manager of another department.
5. If the information security manager of the department receives a report, or becomes aware, of a case of material infringement of any information security-related regulation, or has taken any measures specified in Paragraph 3 above, he/she shall promptly report it to the department to which the infringer belongs and to the Chief Information Security Officer.

Article 96 (Exceptions)

1. The University Information Security Committee shall designate a person who will examine requests for exceptions (hereinafter "authorizer") and establish procedures for such examinations.
2. The authorizer shall examine a request for exception from a user or the like, according to established examination procedures, and determine whether to approve or refuse the request. In determining approval or refusal of an exception request, the authorizer shall create a record of the examination of the request, which shall include the following information, among others, and shall submit the record to the Information Security General Manager.
   (1) Information on the decision-maker who has examined the request (name, job title, department, and contact number);
   (2) Details of the request:
   – Information on the requesting person (name, department, and contact number);

– Applicable provisions in the information security-related regulations for which exception was requested (names of the regulations and provision numbers, etc.);
– Duration of the exception requested;
– Details of the exception requested (alternative security measures, etc.);
– Method of creating a report to notify that the duration of exception has expired; and
– Reason(s) for the exception request;

(3) Details of the examination results:
– Approval or refusal of the request;
– Reason(s) for approval or refusal;
– Applicable provisions in the information security-related regulations for which exception is approved (names of the regulations and provision numbers, etc.);
– Duration of the exception approved;
– Details of the exception approved (alternative security measures, etc.); and
– Method of creating a report to notify that the exemption has been terminated.

3. On the last day of the duration of the approved exception, the authorizer shall check if he/she has received a report from the person to which the exception approval was given. If a report has not been received on that day, he/she shall contact the person to whom the exception approval was given and a report is expected and take necessary measures, unless the authorizer has notified that no report is necessary.

Chapter 11 Measures Against Incidents

Article 97 (Preparation for Possible Incidents)

1. The Chief Information Security Officer shall establish a system to prevent expansion of, and to restore from, damage that may be caused if an information security-related incident occurs.
2. The Information Security General Manager shall establish procedures for reporting an incident from users and the like to the information security manager of each department, and shall communicate such reporting procedures to all users and the like.
3. The Information Security General Manager shall establish procedures to be followed when an incident occurs.
4. To prepare for an accident that may occur to an information system that is determined to be especially important for fulfillment of the education, research, and other activities of the University, the Information Security General Manager shall create an emergency contact network that contains emergency contact numbers and contact methods of the information security technical manager and information system technical staff members of the department, and the information that should be reported to these persons.
5. The Information Security General Manager shall investigate the need for incident response training, and shall establish the content and structures for such training in regard to information systems that are determined to be especially important for fulfilment of the education, research, and other activities of the university.
6. The Information Security General Manager shall appoint a contact person or section to receive reports of incidents from persons outside the University, and shall externally publish the method for contacting such contact person or section.
7. The information security manager of each department shall establish an organization to ensure that incidents are quickly responded to with measures that include: reporting and providing information about the incident, investigating the causes of the incident, and establishing preventive measures.

Article 98 (Investigation of Causes of Incidents, Preventive Measures, and Reporting)

1. If an incident occurs, the information security manager of the department shall investigate the cause(s) of the incident, establish preventive measures, and report the findings of the investigation in writing to the CSIRT Manager.
2. When the CSIRT Manager is made aware of an incident, they shall immediately implement

necessary measures in accordance with the procedures established by the Information Security General Manager pursuant to Paragraph 3 of Article 97.

3. The Information Network Risk Management Committee and the Information Network Ethics Committee shall examine the report of such incidents, and take the necessary measures, including implementing preventive measures.
4. If it is discovered that there has been an incident concerning the University's information system, the Chief Information Security Officer shall provide information about the incident to the Ministry of Education, Culture, Sports, Science and Technology as soon as possible. If it is discovered that there has been an incident concerning any of the information assets as stipulated in Article 3.1 of the Regulations other than the University's information system, the Chief Information Security Officer shall provide information about the incident to the Ministry of Education, Culture, Sports, Science and Technology as soon as possible, as necessary.
5. The information security communications manager in each department shall supervise communications between the department and the CSIRT, and communications among the departmental information security manager, the information security technical manager, the information system technical staff members, and the information security committee.

Chapter 12 Information Systems Other Than Those Provided by the University

Article 99 (Security Management Relating to Information Systems Other Than Those Provided by the University)

The Information Security General Manager shall establish rules for security management measures that should be taken when other information systems than those provided by the University are used for processing information that needs to be protected.

Article 100 (Collection and Management of Permission and Notice of Use of Terminals Other Than Those Provided by the University)

1. When it is necessary to process information that needs to be protected (excluding Confidentiality Class 2 information) using terminals other than those provided by the University, faculty members and office personnel shall obtain the permission of the information security technical managers of their respective departments.
2. When it is necessary to process Confidentiality Class 2 information using terminals other than those provided by the University, faculty members and office personnel shall notify the information security technical manager of their respective departments, unless the information security technical manager has advised that no notification is necessary.
3. The information security technical manager of each department shall collect records related to the use of terminals other than those provided by the University for processing information that needs to be protected.
4. When the period during which use of any terminals other than those provided by the University is permitted for processing information that needs to be protected (excluding Confidentiality Class 2 information) has expired, if no report has been received from the person to whom such permission is given, the information security technical manager of each department shall contact that person to check the use status and take necessary measures, unless the information security technical manager has advised that no report is necessary.
5. When the period during which use of any terminals other than those provided by the University for processing Confidentiality Class 2 information was notified has expired, the information security technical manager of each department shall check the use status and take proper measures, as necessary.

Chapter 13 Prohibition of Acts that Degrade Off-Campus Information Security Level

Article 101 (Prohibition of Acts that Degrade the Off-Campus Information Security Level)

1. Persons who are responsible for operating and managing the University Information System

shall take the following measures to prevent acts that degrade the level of off-campus information security, as necessary.

(1) Measures against malware shall be taken for provided applications and content.

(2) Measures against vulnerabilities shall be taken for provided applications.

(3) Content should not be provided in execution program format unless there is no other means of providing the content..

(4) If there is a means of verifying that provided applications and content are genuine with no unauthorized alterations, etc., such as the use of electronic certificates, such means shall be furnished to the recipients of such applications and content.

(5) Methods for the provision of applications and content shall be determined and developed so that, when using provided applications and content, users are not required to alter settings in a manner that lowers information security standards, such as forcing them to use versions of operating systems, software, etc. that contain vulnerabilities.

(6) Services shall be developed so that applications and content do not include functions such as could provide third parties with information on service users or other persons, against their will, where such functions are not essential to the use of such services.

2. Faculty members and office personnel shall include the matters in each item of the preceding paragraph in procurement specifications when outsourcing development and/or production of applications and content.

Article 102 (Use of University Domains)

1. The information security technical manager of each department shall include in his/her specifications on information systems the use of domain names with the suffix ".kyoto-u.ac.jp" (hereinafter "University domain name"), in order to enable users of websites, etc. for external access to ascertain that such websites, etc. are actually provided by the University. However, cases as set forth in Articles 59 and 60 are excluded.
2. When outsourcing production of websites, etc. for external access, faculty members and office personnel shall include the use of the University domain name in procurement specifications in the same manner as is stipulated in the preceding paragraph.

Article 103 (Preventing Solicitation to Malicious Websites)

The information security technical manager of each department shall institute measures to ensure that users are not solicited via search engines, etc. to access malicious websites impersonating the University's website.

Chapter 14 Education and Training

Article 104 (Education on Information Security Measures)

1. The Chief Information Security Officer shall ensure that education on the Information Security Policy and the Regulations is provided to the information security manager, information security technical manager, and information system technical staff members of each department and users and the like (hereinafter "persons subject to education").
2. The Chief Information Security Officer shall consider the contents of educational programs on the Information Security Policy and the Regulations that should be provided to persons subject to education and develop materials used in such educational programs.
3. The Chief Information Security Officer shall plan and develop a schedule for educational programs on information security measures and establish a system to provide such programs so that each person subject to education can attend the programs at least once a year.
4. The Chief Information Security Officer shall plan and develop a schedule for educational programs on information security measures and establish a system to provide such programs so that each person subject to education may attend the program within three (3) months from enrollment, or arrival at or transfer to his/her post, at the University.
5. The Chief Information Security Officer shall establish a system to manage the attendance status of persons subject to education in the educational program on information security measures.
6. The Chief Information Security Officer shall notify the attendance status of each person subject

to education in the educational program on information security measures to the information security manager of the department to which each person belongs.

7. If any person subject to education has not completed the educational program on information security measures, the information security manager of the department shall advise such person to promptly attend the program. If the person subject to education does not follow such advice, the information security manager of the department shall report to the Chief Information Security Officer thereof.
8. The Chief Information Security Officer shall report each year to the University Information Security Committee the attendance status of persons subject to education in the educational program on information security measures
9. The Chief Information Security Officer shall include education on the Information Security Policy and the Regulations of the University in the contents of training programs on information security measures for persons subject to education and establish a system to provide such training programs.

Article 105 (Provider and Attendees of Educational Programs)

1. The Information Security General Manager shall plan educational programs on the operation and use of the information system and the security of the information system, which shall be provided to persons engaged in operation of the University Information System and users and the like, and provide education to ensure compliance with the Information Security Policy, the Regulations, procedures and other relevant rules.
2. The information security technical manager and information system technical staff members of each department shall provide educational programs to users and the like in accordance with the education plan.

Chapter 15 Assessments

Article 106 (Development of Annual Self-Assessment Schedule)

The Chief Information Security Officer shall establish an annual information security self-assessment schedule.

Article 107 (Preparation for Self-Assessment)

The information security manager of each department shall create a self-assessment form and establish information security self-assessment procedures for each role assigned to faculty members and office personnel.

Article 108 (Implementation of Self-Assessment)

1. In accordance with the annual information security self-assessment schedule developed by the Chief Information Security Officer, the information security manager of the department shall direct faculty members and office personnel to conduct self-assessment.
2. Faculty members and office personnel shall conduct self-assessment by using the information security self-assessment form and self-assessment procedures designated by the information security manager of the department.

Article 109 (Evaluation of Self-Assessment Results)

1. The information security manager of the department shall check that information security self-assessment has been completed by all faculty members and office personnel and evaluate the results of such self-assessments.
2. The Chief Information Security Officer shall check that information security self-assessment has been completed by the information security manager of each department and evaluate the results of such self-assessments.

Article 110 (Improvement Based on Self Assessments)

1. Based on the results of the information security self-assessments, faculty members and office personnel shall take actions to improve matters that can be improved within the scope of their authority, and report to the information security manager of the department such actions taken or to be taken.
2. The Chief Information Security Officer shall evaluate the overall results of the self-assessments, and give directions to the information security manager of the department to take actions for improvement as he/she deems necessary.

Article 111 (Audits)
The information security manager of each department and other persons concerned shall cooperate in an audit performed by the Chief Information Security Officer, in order to ensure proper and efficient performance of the audit.

Article 112 (Implementation of Risk Assessment)
1. To assess the value of, threats to, and vulnerability of, information assets, the Chief Information Security Officer shall establish procedures to assess the risks involved in operating the information system.
2. The Chief Information Security Officer shall direct the Information Security General Manager and other persons who are responsible for managing information assets to conduct risk assessment at least once a year in accordance with the following procedures and to report the results of the assessment:
   (1) The persons responsible for managing information assets shall conduct risk assessment for information assets they handle, in accordance with procedures for information system operation risk assessment;
   (2) Based on the results of such risk assessment, the persons responsible for managing information assets shall decide specific preventive measures to be implemented for identified risks, or specific procedures of incident countermeasures to be taken for information assets if a problem occurs. Risks identified for which it is decided that no measures will be taken shall also be reported.
3. Based on a report by the person responsible for managing information assets, pursuant to the preceding paragraph, the Chief Information Security Officer shall revise the Information Security Policy, the Regulations, and other relevant procedures.

Article 113 (Revisions)
1. Persons who have established the Information Security Policy, the Regulations, and other procedures established based on such Policy or Regulations shall review those rules from time to time to consider whether any revision is necessary, and shall make revisions as they deem necessary.
2. If the persons responsible for operating and managing the University Information System find any shortcoming or problem in a matter relevant to information security measures implemented by them, they shall make proper revisions to such matter to solve such shortcoming or problem.

Supplementary Provisions
These Standards shall take effect on April 1, 2009.

Supplementary Provisions
These Standards shall take effect on April 1, 2015. However, the provisions of Paragraph 1, Article 52 shall take effect on April 1, 2016.

Supplementary Provisions
These Standards shall take effect on April 1, 2017.

Supplementary Provisions
These Standards shall take effect on April 1, 2019.

Supplementary Provisions
These Standards shall take effect on MONTH DAY, YEAR.

(Exhibit)

Terminology

Access control: A security technique that entails limiting the persons permitted to access information.

Algorithm: an arithmetical process designed to achieve a specific purpose.

Application: *software that runs on an operating system for a specific purpose such as the provision of a service, creation of documents, or transmission of e-mail.***Assignment** (regarding information related to entity authentication, permission information in access control, etc.): issuance of, renewal of and making changes to information.

Authority management: the management of information related to entity authentication and permission information (including identification codes and entity authentication information) in access control.

Availability: ensuring the condition where information and relevant information assets can be accessed by persons authorized to access such information whenever they are needed, without interruption.

Availability Class 1 information: information other than Availability Class 2 information (excluding written information).

Availability Class 2 information: information handled in the course of any operation (excluding written information) that may cause difficulty (excluding minor difficulties) in the conduct of education, research, and other activities of the University, or in stable performance of such operations if such information is damaged, lost or unavailable for use.

Cloud service: a service provided through a model involving the use of an interface defined by a provider to gain network access to shareable physical or virtual resources that are expandable and flexible, which allows users to freely establish and manage resources and which offers sufficient scope for setting conditions relating to information security.

Cloud service provider: a business that provides cloud services or develops and operates information systems using cloud services.

Communication line: a system to which more than one server or terminal is connected and that transmits information in a designated communication format. A communication line comprising a line and communication line devices is called a physical communication line. A communication line that is configured on such physical communication line and that can transmit information in accordance with a designated communication format between servers and terminals is called a logical communication line.

Communication line device: Device that is installed to connect multiple communication lines or a communication line and an information system and that controls information transmitted on such line(s). Includes hubs, switches, routers, etc., as well as firewall software and the like.

Confidential information: Confidentiality Class 2 and Class 3 information.

Confidentiality: ensuring the condition that information is provided only to persons who are

authorized to access such information.

Confidentiality Class 1 information: information other than Confidentiality Class 2 and Class 3.

Confidentiality Class 2 information: information handled in the course of any operation that does not need to be classified as “secret,” but is not to be immediately disclosed publicly.

Confidentiality Class 3 information: information handled in the course of any operation that needs to be classified as “secret.”

Contractor: a person who, pursuant to outsourcing, implements all or part of the activities relating to data processing, including the planning, development, and operation of University information systems.

Data center: a general term for any dedicated building for the establishment and operation of internet servers, data transmission devices and the like.

Data processing by information systems other than those provided by the University: data processing performed in connection with the operation of the University by using any information system other than those provided by the University. Refers not only to data processing performed directly by devices but also to the use of services provided by such devices. In the definition of this term, “service” refers to e-mail service, etc. used by individual users. For example, a user may forward data via the e-mail service that he/she uses to have that data processed, or may send business mails from his/her personal mail account provided by such e-mail service.

Denial-of-Service Attack: an attack made by a malicious third party or the like that takes advantage of a software vulnerability to render server or communication line device software inoperable or obstructs regular use of services by accessing a server, communication line device or communication line to a level in excess of its capacity.

Devices and the like: general term for the components of information systems (servers, terminals, communication line devices, hybrid devices, special purpose devices, software, etc.), external electromagnetic recording media and the like.

Domain name: a name that is assigned on a network, divisible into units indicating country, organization, and service, and that is expressed using alphabetic characters and some symbols. In the case of the web address www.kyoto-u.ac.jp, for example, the kyoto-u.ac.jp portion is the domain name.

Encryption: applying a predetermined arithmetic operation to alter data so that it cannot easily be deciphered by a third party.

Entity authentication storage device: a device on which entity authentication information is stored and provided to the authentic entity for ownership or possession. Entity authentication by possession is a method in which the information system identifies an entity possessing such device as an authentic entity. A magnetic tape card and IC card are typical entity authentication storage devices.

Exception: an action taken by a faculty member or office person that does not conform to relevant rules or measures stipulated in information security-related regulations for which implementation he/she is responsible, but is allowed upon approval. An exception may be approved if (1) it is difficult for such faculty member or office person to observe the relevant rules or measures, and an alternative method is adopted to ensure proper and continued performance of his/her duties, or (2) if he/she presents justifiable reasons for not conforming to such rules or measures.

External service subject to terms and conditions: a data processing service provided online subject to terms and conditions determined by a private business operator or other external organization, whereby a user who agrees to the terms and conditions and completes a simple account registration may produce, store, and send information on the server that provides the service, regardless of whether the service is charged for or provided at no cost. Typical examples include e-mail, file storage, and groupware services. However, this excludes services that provide sufficient scope for a user to set conditions regarding the information security they require.

Fix file: a patch file or version upgrade software used to fix a security hole.

Goods deliverer: a person engaged in delivery service and who delivers goods to a faculty member or office person conducting activities within the secure area and who does not need to enter the secure area. Delivery services include collection and delivery of goods by courier service, delivery of office supplies, and other similar services.

Handling restrictions: restrictions placed on the handling of information, such as prohibiting reproduction, prohibiting operation, prohibiting redistribution, implementing mandatory encryption, destroying after reading, etc.

Indication: a method to ensure that all persons handling any information have the same understanding regarding the classification assigned to such information. In principle, each piece of information should be assigned a classification indication. However, if the regulations or rules established for a specific information system set forth the classification of information recorded in such system and if such regulations or rules are known and fully understood by all persons who use such information system, then such method is also deemed an “indication.”

Information device manager: an information system technical staff member in each department designated in accordance with Article 5.3 of the Kyoto University Regulations for Information Security Programs.

Information manager: a faculty member or office person who creates or collects information (Article 61) and who is responsible for deciding classification and handling restrictions (Article 62), the indication of such classification and handling restrictions (Article 63), and any changes in such classification and handling restrictions (Article 65).

Information requiring integrity: See “Integrity Class 2 information.”

Information requiring stability: See “Availability Class 2 information.”

Information security-related regulations: operational procedures that describe how rules and measures set forth in these Standards should be practiced in real information systems and operations.

Information system other than those provided by the University: any information system other than the information systems provided by the University. Computers and mobile terminals possessed by users for private use and information systems provided to loaned employees of the University by organizations from which such loaned employees are provided are also deemed “information system other than those provided by the University.”

Information that needs to be protected: confidential information, information requiring integrity, and information requiring stability.

Integrity: ensuring conditions so that information is not destroyed, or falsified or deleted.

Integrity Class 1 information: information other than Integrity Class 2 information (excluding

written information).

Integrity Class 2 information: information handled in the course of any operation (excluding written information) that may cause difficulty (excluding minor difficulties) in the administration of the University or in proper performance of such operation if such information were incorrect, falsified, or damaged.

Log-in: an action made by an entity to request entity authentication. Entity authentication is performed after the entity has logged in. Accordingly, a successful log-in does not necessarily mean that the entity is an authentic entity.

Logged on: the status in which an entity has been verified by the information system as an authentic entity as a result of logging in.

Malware: a general term for computer viruses, worms (programs that self-propagate rather than relying parasitically on other programs), spyware (programs that gather various types of information contrary to the intentions of the users of such programs) and other programs that cause consequences in an information system not intended by the user of that system.

Malware definition file: data used by antivirus software to detect malware.

Mobile terminal: any laptop PC, smartphone, tablet, or other terminal that is portable to another location depending on the purpose of the operation, regardless of the form of such terminal. Laptop PCs used only in one designated location are not deemed mobile terminals.

Multiple factors authentication/composite authentication: a method of authenticating an entity by using a combination of two or more entity authentication factors. A typical example of this method is entity authentication made by requiring both IC card presentation and password input.

Off campus: any location outside the organizations or facilities controlled by the University.

Off-campus communication line: any logical communication line to which servers and terminals not managed by the University are connected and used for communication between such servers and terminals, regardless of the type or nature of the physical lines comprising such communication lines (wired or wireless, actual or virtual, or controlled by the University or other organizations), and regardless of the type of communication devices installed on such line.

Off-campus data processing: data processing related to operations of the University performed outside the University. Off-campus data processing includes not only online data processing performed by connecting from outside the University to the information system of the University, but also includes offline data processing performed outside the University facilities.

On-campus: any location within the organizations or facilities controlled by the University.

On-campus communication line: any logical communication line to which servers and terminals managed by the University are connected and used for communication between such servers and terminals, regardless of the type or nature of the physical lines comprising such communication lines (wired or wireless, actual or virtual, or controlled by the University or other organizations), and regardless of the type of communication devices installed on such line.

Outsourcing: engagement of a party outside the University to undertake all or part of the University's data processing activities under contract. Includes all types of outsourcing regardless of contractual form, including "commissioning," "quasi-commissioning," and "contracting."

Publicly announced security hole: a security hole that is in a condition where it may be known by

anyone, including a security hole publicly announced by the manufacturer or provider of software or hardware, or publicly announced by security-related organizations.

Recording medium: a tangible object on which information is recorded or printed. Recording media include paper and other tangible objects containing printed text, graphics, and other content perceptible to humans (“written information”), and recording media related to records created using electronic, magnetic, and other methods not perceptible to humans that are designed for use in data processing by information systems (“electromagnetic records” and “electromagnetic recording media”). Electromagnetic recording media include built-in electromagnetic recording media installed in servers, terminals, communication line devices and the like, and external electromagnetic recording media such as USB flash drives, external hard disk drives, and DVD-R discs.

Service: a function or group of functions provided by applications running on the server to servers and terminals that connect to the system.

Shared identification code: an identification code assigned for the purpose of shared use by more than one entity. As a general rule, an entity should be assigned an identification code unique to such entity. However, in certain situations, one identification code may be shared by more than one entity, in accordance with the restrictions or use status of the information system and any other factors. Such identification code used by more than one entity is also then called a “shared identification code.”

Social media service: a type of online service that enables users thereof to communicate with one another.

Software: a description of processes and commands used to operate a server or terminal in a form that can be understood by the server or terminal. In these Standards, software includes both the operating system and the applications that run on the operating system.

Special purpose device: a teleconferencing system, IP telephone system, network camera system, or other distinct component of an information system that is used for a specific purpose and is connected to a communication line or has built-in electromagnetic recording media.

Transfer of information: transmitting information recorded by electromagnetic, optical or other means to another information system or organization over which the person responsible for that information has no control, as well as transporting electromagnetic recording media, PCs, or written documents on which the information is recorded.

Unauthorized access: the use or operation of a server or terminal by a person authorized to use such server or terminal but using an unauthorized process, or use or operation of a server or terminal by a person not authorized to use such computer.