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

Rules for Using the Kyoto University Campus-wide Information System

(Established by the Trustee in Charge of Information Management, January 12, 2010)

Article 1 (Purpose)

1. The purpose of these Rules is to set forth regulations to be followed by users of the Campus-wide Information System of the University as specified in Article 4 of Kyoto University Information Security Program Standards (Approved by Trustee in charge of Information Infrastructure on March 2 , 2009), in accordance with Article 2.5 of the Kyoto University Regulations for Information Security Programs (October 21, 2003 Notification No.43), in order to ensure the information security and efficient use of information systems within Kyoto University (the “University”).
2. The Campus-wide Information System of the University shall be used for the following purposes:
   (1) Educational and research activities of the University and other activities conducted by the University in accordance with the Act of National University Corporations (Law No. 112, 2003); and
   (2) Any other activities specifically approved by the Chief of the Institute for Information Management and Communication

Article 2 (Definition)

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

(1) “Regulations” refers to the Kyoto University Regulations for Information Security Programs (October 21, 2003 Notification No.43).
(2) “Information Security Policies” refers to the Kyoto University Basic Policy for Information Security (Determined by the Board of Executive Directors, on March 25, 2015) and the “Regulations” referred in (1) above.
(3) “Implementation Regulations” refers to the Kyoto University Information Security Program Standards (hereinafter the “Standards”) and other regulations, standards and plans, established by the Trustee in Charge of Information Management in accordance with the Information Security Policies.
(4) “Institute System User Regulations” refers to the “Regulations for Users of the Educational Computer System and the Academic Information Network System of the Kyoto University Institute for Information Management and Communication of the University” (April 27, 2012, Established by the Chief of the

Institute for Information Management and Communication).

(5) “Campus-wide Information System” refers to a group of information systems established and operated as an intelligence infrastructure for the entire organization of the University, comprising of an integrated authentication system (as defined in Item 23 below) and an academic information network system (as defined in Item 15 below), that is designated by the Chief Information Security Officer in accordance with Article 4 of the Standards as the information systems that would be significantly affected by infringement of information security (confirmed by the University Information Security Committee, June 9, 2009).

(6) “Specific Department Information Systems” refers to certain department information systems (as defined in Article 2.8 of the Standards) connected to KUINS in accordance with Article 18.1 or the integrated authentication system in accordance with Article 19.1.

(7) “User terminals” refers to information equipment and devices (excluding equipment and devices comprising part of the Campus-wide Information System or Specific Department Information Systems) used by users and the like in and outside the University for specific use (as defined in Item 40 below) of the Campus-wide Information System and Specific Department Information Systems.

(8) “Operational and Management Organization” refers to the Institute for Information Management and Communication as defined in Article 4.2 of the Standards.

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

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

(11) “Users” refers to faculty members, office personnel and students of the University who are authorized to use the Campus-wide Information System and/or Specific Department Information Systems.

(12) “Temporary users (Campus-wide Information System)" refers to any persons other than faculty members, office personnel and students of the University who are authorized, upon approval of the Chief of the Institute for Information Management and Communication, to use the Campus-wide Information System (including persons who use the System in the course of operation and maintenance of such system, the same applies hereinafter).

(13) “Temporary users (Specific Department Information System)" refers to any persons other than faculty members, office personnel and students of the University who are authorized, upon approval of the information security manager of the department or the information security technical manager of the department, to use the relevant Specific Department Information System.

(14) “Users or the like” refers to users, temporary users (Campus-wide Information System) and temporary users (Specific Department Information System).

(15) “KUINS” refers to the academic information network system as defined in the Institute System User Regulations, comprising KUINS-II having a global IP address and KUINS-III having a private IP address.

(16) “KUINS device manager” refers to a “KUINS connector” as defined in Article 8.2 of the Institute System User Regulations who accesses “KUINS with a global IP address” as defined in Article 10.1 of the same regulations.

(17) “KUINS information wall socket manager” refers to a “KUINS connector” as defined in Article 8.2 of the Institute System User Regulations who accesses KUINS with a private IP address as defined in Article 10.2 of the same regulations.

(18) “Subnet contact person” refers to the Subnet contact person as defined in Article 11.1 of the Institute System User Regulations.

(19) “VLAN manager” refers to the VLAN manager as defined in Article 11.2 of the Institute System User Regulations.

(20) “KUINS payment manager” refers to the KUINS connector as defined in Article 15 of the Institute System User Regulations or any person acting on behalf of the KUINS connector.

(21) “Common code system account” refers to an account assigned to each faculty members or office worker (“SPS-ID”) or an account assigned to a student (“ECS-ID”) (hereinafter, SPS-ID and ECS-ID are collectively referred to as “campus accounts,” used for entity authentication (as defined in Item 35 below) of the user or the like who attempts to access the Campus-wide Information System or a Specific Department Information System.

(22) “Temporary accounts” refers to campus accounts issued to temporary users (Campus-wide Information System).

(23) “Integrated Authentication System” refers to an intelligent infrastructure comprising of an authentication system (as defined in Item 24 below), an integrated LDAP server (as defined in Item 25 below), the Kyoto University Certificate Authority and IC cards (as defined in Item 28).

(24) “Authentication systems” refers to the campus-wide authentication portal system, the authentication system for the faculty member/office personnel groupware, and the educational/research community authentication linkage system.

(25) “Integrated LDAP server” refers to a directory database containing campus accounts, passwords and some attribution data.

(26) “Kyoto University Certificate Authority” refers to the certificate authority as defined in 1.3 of the Kyoto University Electronic Certificate Authority Policy and Operational Rules (established by the Trustee in Charge of Information Management, February 2, 2009).

(27) “Electronic certificate” refers to an electronic certificate issued by the Kyoto University Certificate Authority. It is used to authenticate the identity of a person attempting to log in to an information system and other similar purposes.

(28) “IC card” refers to an IC staff identification card (as defined in Item 29 below), an IC identification card (as defined in Item 30 below), an IC student identification card (as defined in Item 31 below) or a facility

user card.

(29) “IC staff identification card” refers to a staff identification card issued to each full-time faculty member or office worker when he/she joins the University, in accordance with the Kyoto University Rules for Staff Identification Cards (established by the President, February 23, 1985). Data necessary for entity authentication (as defined in Item (37) below) are contained in the IC card.

(30) “IC identification card” refers to an IC identification card issued to a non full-time faculty member or office worker when he/she joins the University, in accordance with the Kyoto University Rules for IC Identification Cards (established by the Chief of the Institute for Information Management and Communication, November 10, 2009). Data necessary for entity authentication are contained in the IC card.

(31) "IC student identification card” refers to a student card issued to each student or undergraduate student by the relevant department. Data necessary for entity authentication are contained in the IC card.

(32) “Facility user card” means a facility user card that may be issued by the Chief of the Institute for Information Management and Communication, in accordance with the Kyoto University Rules for Facility User Cards (established by the Chief of the Institute for Information Management and Communication, November 10, 2009), to any user or the like who does not have an IC staff identification card, IC identification card, or IC student identification card. Data necessary for entity authentication are contained in the IC card.

(33) “Issuing organization” refers to the General Affairs Department with respect to issuance of an IC staff identification card, the department to which the student belong with respect to issuance of an IC student identification card and the Institute for Information Management and Communication with respect to issuance of an IC identification card and a facility user card.

(34) “PIN” (Personal Identification Number) refers to entity identification data used to authenticate entity identification by an IC card containing an electronic certificate.

(35) “Entity authentication” means a process to verify whether an entity presenting an identification code (as defined below) is an authentic entity that has been assigned with that identification code. In most cases, an entity is a natural person, but in some cases where more than one information system and/or devices are involved in the attempt for access, such other information system and devices are also deemed entities. When entity authentication information is presented in a correct manner, together with an identification code, the information system verifies the authenticity of the entity presenting the information.

(36) “Entity identification code” is information presented by an entity to the information system for entity authentication in order for the system to verify that the entity has the proper access authority. A typical identification code is an ID number or code.

(37) “Entity authentication information” is information presented by an entity to the information system for entity authentication in order for the system to verify that the entity has the proper authority to access. Typical entity authentication information is a password or a device containing entity authentication

information.

(38) “Guideline for Communication regarding Unauthorized Access” refers to the Guideline for Communication Regarding Unauthorized Computer Access (established by the University Information Security Committee, February 5, 2013).

(39) "Unauthorized access” means unauthorized invasion of any computer installed on the premises of the University, as defined in Paragraph 1 of the Guideline for Communication regarding Unauthorized Access (including data destruction, unauthorized website alteration, unauthorized mail relaying (spam mail), etc.) and infection with computer virus, which has resulted in any damage.

(40) “Specific use” refers to the use of KUINS by the KUINS connector, a user or the like authorized in accordance with Article 18.7 (including use in the course of operation, maintenance or similar activities; the same definition applies hereinafter), and the use of the Campus-wide Information System or a Specific Department Information System by a user or the like upon entity authentication by a campus account, an IC card or an electronic certificate.

(41) Other terms used in these Rules have the meaning as defined in Regulations and the Standards.

Article 3 (Scope)

1. These Rules apply to faculty members and office personnel and all users and the like.
2. These Rules apply to the following systems:
   (1) Campus-wide Information System
   (2) Specific Department Information System
   (3) User terminals (only if they are used for specific uses)

Article 4 (Request for a campus account and issuance)

Each user or the like who accesses the Campus-wide Information System or a Specific Department Information System upon entity authentication using a campus account must obtain a campus account by submitting a request for a campus account issuance with the Institute for Information Management and Communication in accordance with the procedures separately determined by the Chief of the Institute for Information Management and Communication.

Article 5 (Acquisition of IC card and electronic certificate)

1. Each user or the like who uses the Campus-wide Information System or a Specific Department Information System upon entity authentication using an IC card must obtain an IC card from the relevant issuing organization.
2. A faculty member or office worker who uses the Campus-wide Information System or a Specific Department Information System upon entity authentication using an electronic certificate must obtain an electronic certificate from the Institute for Information Management and Communication.

Article 6 (Authorization to temporary users (Campus-wide Information System) and temporary users (Specific Department Information System))

1. If it is determined that any other person than faculty members, office personnel and students needs to access the Campus Information System under any of the following conditions, the Chief of the Institute for Information Management and Communication shall give such person authorization to access the Campus Information System as a temporary user (Campus-wide Information System):
   (1) The information security manager of a department requests access by such person, clearly indicating the purpose, scope, period and other conditions for such temporary use; or
   (2) Any other situation where the Chief of the Institute for Information Management and Communication determines that access by such person is necessary.
2. If it is determined that any other person than faculty members, office personnel and students needs to access a Specific Department Information System, the information security manager or the information security technical manager of the relevant department shall, in accordance with the procedures determined by the department, give such person authorization to access such Specific Department Information System.
3. If the information security manager of a department has submitted a request to the Chief of the Institute for Information Management and Communication in accordance with 1. (1) above to authorize any person to use the Campus-wide Information System as a temporary user and obtained authorization for such person, the information security manager of the department shall take necessary measures to ensure that such temporary user (Campus-wide Information System) observes these Rules. If it is deemed necessary, the information security manager shall ensure that such authorized temporary user (Campus-wide Information System) attends educational sessions regarding the Information Security Policies and Implementation Regulations of the University and the use of the Campus-wide Information System.
4. If the Chief of the Institute for Information Management and Communication gives authorization for temporary use of the Campus-wide Information System in accordance with 1. (2), the Chief of the Institute for Information Management and Communication shall take necessary actions to ensure that such temporary user (Campus-wide Information System) observes these Rules. If it is deemed necessary, the Chief of the Institute for Information Management and Communication shall ensure that such authorized temporary user (Campus-wide Information System) attends educational sessions regarding the Information Security Policies and Implementation Regulations of the University and the use of the Campus-wide Information System.
5. If the information security manager or the information security technical manager of a department gives authorization for temporary use of a Specific Department Information System in accordance with Paragraph 2 above, the information security manager or the information security technical manager, as the case may be, shall take necessary measures to ensure that such temporary user (Specific Department Information System) observes these Rules. If it is deemed necessary, the information security manager or the information security technical manager shall ensure that such authorized temporary user (Specific

Department Information System) attends educational sessions regarding the Information Security Policies and Implementation Regulations of the University and the use of the Campus-wide Information System.

Article 7 (Observation of related regulations)

1. When using information systems specified in Article 3.2, users and the like shall observe relevant laws, the Information Security Policies and Implementation Regulations of the University, these Rules, procedures regarding the use of information systems, Kyoto University Regulations for Protection of Personal Information (Notification No. 1, 2005), and the Regulations for Protecting Personal Number and Specific Personal Information (Notification No. 49, 2015).
2. When using a Specific Department Information System, users and the like shall observe these Rules and any other regulations and procedures established by the relevant department.
3. When using any information systems in and outside the University by using information systems specified in Article 3.2, users and the like shall observe relevant laws and any contract concluded between such users and the like and the provider or administrator of such information system with respect to the use of such information system.
4. A faculty member or office worker who uses an IC identification card shall, when using an electronic certificate, observe these Rules and the Kyoto University Electronic Certificate Authority Policy and Operational Rules (established by the Trustee in Charge of Information Management, February 2, 2009).
5. A faculty member or office worker who receives an IC staff identification card shall, when using the IC staff identification card, observe these Rules and the Kyoto University Rules for Staff Identification Cards (established by the President, February 23, 1985).
6. A faculty member or office worker who receives an IC identification card shall, when using the IC identification card, observe these Rules and the Kyoto University Rules for IC Identification Cards (established by the Chief of the Institute for Information Management and Communication, November 10, 2009).
7. Students who receive IC student identification cards shall, when using the IC student identification cards, observe these Rules and handling rules established by the issuing organization.
8. Users and the like who receive facility user cards shall, when using the facility user cards, observe these Rules and the Kyoto University Rules for Facility User Cards (established by the Chief of the Institute for Information Management and Communication, November 10, 2009).

Article 8 (Rules for campus account use)

Each user or the like shall observe the following rules when using his/her campus account:

(1) Each user or the like shall not let any other person use his/her own campus account, or shall not use any other person’s campus account;
(2) Each user or the like shall not get or use any other person’s entity authentication information (password);

(3) Each user or the like shall properly control his/her entity authentication information (password) in accordance with the User Password Guidelines established by the Chief of the Institute for Information Management and Communication;

(4) While using a user terminal to access the Campus-wide Information System or a Specific Department Information System upon entity authentication, each user or the like shall exercise proper caution to prevent unauthorized viewing or operation of the screen by other persons;

(5) Each user or the like shall not access the Campus-wide Information System or a Specific Department Information System upon entity authentication of a campus account, by using a terminal that any person outside the University can operate (use).

(6) If the campus account is used by any other person or if there is any threat of such unauthorized use, the user or the like shall immediately report the incident to the Chief of the Institute for Information Management and Communication;

(7) If it becomes necessary to change the campus account data because of name change by marriage or any other reasons, each user or the like shall promptly report regarding such change to the Chief of the Institute for Information Management and Communication; and

(8) When a user or the like has lost a qualification to use the Campus-wide Information System or does not need to use the Campus-wide Information System anymore, he/she shall promptly notify the Chief of the Institute for Information Management and Communication thereof, unless omission of such notification is stipulated in advance by the Institute for Information Management and Communication.

Article 9 (Rules for using IC card and electronic certificate)

1. Users and the like who receive IC cards shall observe the following rules for IC card management:

(1) The IC card shall be safely controlled to prevent unintended use by any other person than the holder of the IC card;

(2) No IC card holder shall give or lend his/her IC card to any other person, or use any other person's IC card;

(3) Each IC card holder shall keep good control of the IC card to prevent its loss. If an IC card is lost, the incident shall be immediately reported to the issuing organization;

(4) If the IC card holder does not need the IC card anymore, or is no longer qualified to use the IC card, he/she shall promptly return the IC card to the issuing organization; unless different procedures are established by the issuing organization for treatment of IC student identification card;

(5) If information indicated on the surface or an electronic certificate contained in the IC card needs to be changed, the IC card holder shall promptly notify the necessary change to the issuing organization;

(6) The electronic certificate stored by the Institute for Information Management and Communication in the IC card shall not be deleted without permission from the Chief of the Institute for Information Management and Communication; and

(7) The PIN used in combination with the IC card shall be properly managed by the IC card holder in

accordance with the User Password Guidelines established by the Chief of the Institute for Information Management and Communication.

2. If an incident in 1. (3) above is reported in connection with an IC staff identification card or IC identification card, the chief of the issuing organization shall promptly report the incident to the Chief of the Institute for Information Management and Communication. If an incident as described in 1. (3) above is reported in connection with an IC student identification card or facility user card, the chief of the issuing organization shall report the incident to the Chief of the Institute for Information Management and Communication by the procedures established by the Chief of the Institute for Information Management and Communication.

Article 10 (Rules for using the Campus-wide Information System)

1. Each user or the like shall not use the information systems stipulated in Article 3.2 for any other purpose than those stipulated in Article 1.2. A Specific Department Information System and a user terminal connected to that System shall be used for the purpose specifically designated for such System, if such designation has been made by the department.
2. When using information systems stipulated in Article 3.2, each user or the like shall observe the rules set forth in Articles 4 and 5 of the Kyoto University Rules for Information Asset Use (approved by the Council of Department Chiefs, September 4, 2007).

Article 11 (Restriction on P2P software use)

1. If a user or the like uses P2P software (hereinafter “P2P software”) having an automatic public file transmission function on the information systems stipulated in Article 3.2, he/she shall observe the following rules:
   (1) P2P software shall not be used for any other purpose than educational/research purposes. When a person needs to use P2P software for educational/research purposes, approval from the information security manager of his/her department (or the Chief of the Institute for Information Management and Communication as for a temporary user (Campus-wide Information System), or the information security manager of the relevant department as for a temporary user (Specific Department Information System)) shall be obtained for the use.
   (2) P2P software shall not be used in KUINS-III.
2. If such P2P software approved to be used in accordance with Paragraph 1.1 above uses KUINS-II, the information security manager of the relevant department shall promptly notify the Chief of the Institute for Information Management and Communication thereof.

Article 12 (Rules for blocking malicious programs)

1. In accordance with the Guidelines for Measures against Invasion by Malicious Programs established by the Chief of the Institute for Information Management and Communication, preventive measures to block malicious programs shall be taken for a Specific Department Information System by the information

system technical staff member of the department that controls such Specific Department Information System.

2. When a user or the like uses an information system within the University as a user terminal to access the Campus-wide Information System or a Specific Department Information System, preventive measures to block malicious programs shall be taken for such user terminal by the information system technical staff member of the department that controls such user terminal, in accordance with the Guidelines for Measures against Invasion by Malicious Programs established by the Chief of the Institute for Information Management and Communication.

Article 13 (Suspension of a campus account and reinstatement)

1. If the Chief of the Institute for Information Management and Communication finds any use of campus account that violates Article 7 or Paragraph 1, 2 or 3 of Article 8, or receives a report that entity authentication information of an entity was, or may be, used by an unauthorized person, he/she shall block access by such campus account to all or part of the Campus-wide Information System that uses campus accounts for entity authentication and to all or part of the Department Information System connected to the integrated authentication system in accordance with Article 19.1, and report the incident to the information security manager of the department to which the user or the like possessing such campus account belongs.
2. Upon receipt of a report in accordance with Paragraph 1 above, the information security manager of the department shall promptly deliver a notice of such incident to the relevant user or the like, unless such person cannot be contacted by telephone, postal mail or any other reasonable means.
3. If the user or the like whose campus account was suspended or restricted from access wishes reinstatement of his/her campus account, he/she shall request the Chief of the Institute for Information Management and Communication of such reinstatement.
4. Upon receipt of such request as referred to in Paragraph 3 above, the Chief of the Institute for Information Management and Communication shall promptly reinstate such campus account after checking its safety.

Article 14 (Nullification of IC card/electronic certificate and reissuance)

1. If the Chief of the Institute for Information Management and Communication finds any use of IC card/electronic certificate that violates Article 7 or Paragraph 2 or 7 of Article 9, or receives a report that entity authentication information of an entity was, or may be, used by an unauthorized person, he/she shall notify the IC card issuing organization of such incident, nullify the relevant electronic certificate and report the incident and measures taken therefor to the information security manager of the department to which the user or the like using such IC card/electronic certificate belongs.
2. Upon receipt of a report in accordance with Paragraph 1 above, the information security manager of the department shall promptly deliver a notice of such incident to the relevant user or the like, unless such person cannot be contacted by telephone, postal mail or any other reasonable means.

3. If the user or the like whose IC card was nullified wishes reissuance of a new IC card/electronic certificate, he/she shall request the issuing organization thereof.
4. If the user or the like whose electronic certificate was nullified wishes reissuance of a new IC card/electronic certificate, he/she shall request the Institute for Information Management and Communication.
5. Upon receipt of such request as referred to in Paragraph 4 above, the issuing organization or the Institute for Information Management and Communication shall promptly reissue a new IC card/electronic certificate after checking the safety of using such IC card/electronic certificate.

Article 15 (Actions against offences of the Campus-wide Information System)

If the Chief of the Institute for Information Management and Communication finds or receives a report of any act suspected to violate the rules defined in Article 10, he/she shall report such act to the Information Network Ethics Committee in accordance with Article 8 of the Kyoto University Rules For Information Asset Use (approved by the Council of Department Chiefs, September 4, 2007).

Article 16 (Emergency measures against incidents)

1. If the Chief of the Institute for Information Management and Communication finds any incident suspected to be unauthorized access to the Campus-wide Information System (including any situation where it is uncertain whether an access is authorized or unauthorized; the same shall apply hereinafter) or material infringement of security of the Campus-wide Information System, he/she shall immediately report such incident to the Chief Information Security Officer.
2. Upon receipt of such report, the Chief Information Security Officer shall immediately notify the Information Network Risk Management Committee of the incident. The Chief Information Security Officer may also give instructions to the Chief of the Institute for Information Management and Communication, depending on the situation resulting from such incident, to temporarily block the network connection between the Campus-wide Information System and a Specific Department Information System or a user terminal and take any other proper measures to prevent expansion of the damage.
3. The Chief of the Institute for Information Management and Communication shall investigate the cause of the incident and develop preventive measures, in accordance with Article 98.1 of the Standards, and shall report in writing the result of the investigation to the Information Network Risk Management Committee.
4. If involvement of a department in an incident referred in Paragraph 1 above is confirmed or suspected, the information security manager of such department (or the department of the user who used a user terminal that is not the information systems of the University) shall cooperate in the investigation conducted by the Chief of the Institute for Information Management and Communication under the direction of the Chief Information Security Officer, to find the cause of the incident.
5. The Information Network Risk Management Committee shall examine such report of an incident received from the Chief of the Institute for Information Management and Communication, and take necessary

measures to prevent reoccurrence of the same and similar incidents, in accordance with Article 98.2 of the Standards.

Article 16-2 (Responses to incidents involving user terminals)

1. If the Chief of the Institute for Information Management and Communication finds any incident suspected to be unauthorized access to a user terminal (including any situation where it is uncertain whether an access is authorized or unauthorized; the same shall apply hereinafter) or infringement of a user terminal, he/she shall immediately report such incident to the Information Network Risk Management Committee.
2. Upon receiving a report from the Chief of the Institute for Information Management and Communication pursuant to Paragraph 1 above, the Information Network Risk Management Committee shall report to the information security manager of the department to which the terminal's user belongs. The Committee may also in light of the circumstances direct the Chief of the Institute for Information Management and Communication to prevent expansion of the damage.
3. Upon receiving a report pursuant to Paragraph 2 above, the information security manager of the department shall immediately identify the applicable user and user terminal, investigate the cause of the incident and develop preventive measures in accordance with Article 98.1 of the Standards, and report in writing the result of the investigation to the Information Network Risk Management Committee.
4. The Information Network Risk Management Committee shall examine a report received under Paragraph 3 above and take necessary measures to prevent reoccurrence of the same and similar incidents, in accordance with Article 98.2 of the Standards.

Article 17 (Actions against Offences)

1. If any act suspected to violate any rule defined in Article 7 or Article 11 is found or reported, the Chief of the Institute for Information Management and Communication shall promptly conduct an investigation to find out relevant facts. To find out the facts, opinions of the person who has committed such offense shall be heard if practically possible.
2. If involvement of a department in an incident referred in Paragraph 1 above is confirmed or suspected, the information security manager of such department (or the department of the user who used a user terminal that is not the information systems of the University) shall cooperate in the fact-finding and investigation conducted by the Chief of the Institute for Information Management and Communication regarding such incident or the relevant Specific Department Information System and the user terminal.
3. Upon taking measures in Paragraph 1 above, the Chief of the Institute for Information Management and Communication shall promptly report such measures taken to the Chief Information Security Officer.
4. If it is found, as a result of the investigation, that an offense was committed, the Chief Information Security Officer may take any of the following measures, via the Information Security General Manager:
   (1) Issue a warning to discontinue such act to the information security manager of the department of such offending person;

(2) Issue a warning to the information security manager of the department to block the information transmission involved in such offending act;
(3) Issue to the information security manager of the department a notice of suspension or deletion of the campus account of the offending person;
(4) Report the incident to the department to which the offender belongs and the President of the University; and/or
(5) Take any other measures in accordance with relevant laws and regulations.

Article 18 (Device connection to KUINS and permission and suspension of use)

1. Any faculty member or office worker who plans to submit a request to obtain approval for connecting any device to KUINS in accordance with Article 8.1 of the Institute System User Regulations shall obtain prior consent from a person who will be designated as a KUINS payment manager, and then notify the information security technical manager of his/her department of such plan.
2. Any person who plans to connect any device to KUINS-II in accordance with Article 8.1 of the Institute System User Regulations shall obtain prior consent from the subnet contact person of the relevant subnet with which the connection will be made. When a request for use approval is submitted, information on the device to be connected and its configuration shall also be provided. When such equipment connected or its configuration is changed, the KUINS device manager shall promptly submit a report of such change.
3. If the information security technical manager wishes to install KUINS-III information wall sockets in his/her department, he/she shall designate a staff member in the department as a KUINS information wall socket manager for such information wall sockets before submitting a request to the Chief of the Institute for Information Management and Communication.
4. Any person who plans to connect any device to KUINS-III in accordance with Article 8 of the Institute System User Regulations shall obtain prior consent from the VLAN manager of the relevant VLAN to which such information wall sockets will belong to.
5. If the person who has connected a device to KUINS does not need the connection anymore, or is no longer qualified to use KUINS, he/she shall promptly notify the Chief of the Institute for Information Management and Communication and the information security technical manager of his/her department thereof.
6. The KUINS device manager, the KUINS information wall socket manager, the subnet contact person and the VLAN manager shall cooperate in the fact-finding and the investigation conducted by the Chief of the Institute for Information Management and Communication in accordance with Article 13. 1 or 13.2.
7. If any user or the like uses KUINS upon approval by the information security technical manager of the department (i.e. any user or the like is allowed to use a Specific Department Information System, or the user terminal of any user or the like is connected to a Specific Department Information System, and the transmission pass through KUINS), the KUINS device manager or the KUINS information wall socket manager shall monitor that rules defined in these Rules are observed by such user or the like.

Article 19 (Connection of Specific Department Information System to the integrated authentication system and permission and suspension of use)

1. When the Specific Department Information System of a department is connected to the integrated authentication system (including use of an IC card for the purpose of entity authentication; the same shall apply hereinafter), the information security technical manager of the department shall submit a request for approval of such connection to the Chief of the Institute for Information Management and Communication, clearly indicating the purpose and scope of use of information provided by such connection, unless such scope is designated in advance by the Chief of the Institute for Information Management and Communication.
2. The information security technical manager shall report to the information security manager of the department regarding such connection made in accordance with Paragraph 1 above.
3. When personal information (as defined in Article 2.7 of the Regulations) is provided by the connection requested and permitted in accordance with Paragraph 2 above or connection within the extent designated in advance, the Chief of the Institute for Information Management and Communication shall notify or publicly announce to relevant users and the like about the purpose of use of such Specific Department Information System and personal information.
4. If the connection to the integrated authentication system is not needed any more, the information security technical manager of the relevant department shall promptly notify the Chief of the Institute for Information Management and Communication thereof.
5. The information security technical manager of the department shall take necessary measures to ensure that information provided to the Specific Department Information System by the connection to the integrated authentication system is not used beyond the purpose and scope of use indicated in the request for connection.

Article 20 (Attendance at information security education programs)

1. Users shall attend educational programs regarding the Information Security Policies, the Implementation Regulations and use of the Campus-wide Information System, following the annual education plan established by the Chief Information Security Officer in accordance with Article 104.3 of the Standards.
2. Each faculty member or office worker, when he/she first joins Kyoto University, shall confirm with the information security manager of the department he/she is assigned to regarding the method to attend the educational programs referred to in Paragraph 1 above.
3. If a faculty member or office worker is not able to attend any educational program referred to in Paragraph 1 above due to a reason not attributable to the fault of such person, he/she shall promptly report his/her inability to attend the program and the reason therefor to the Information Security General Manager via the information security manager of his/her department.
4. Temporary users (Campus-wide Information System) or temporary user (Specific Department Information

System) shall, if deemed necessary by the Chief of the Institute for Information Management and Communication or the information security manager of the department who has given permission to use the system to such persons, shall attend educational programs regarding the Information Security Policies, the Implementation Regulations and use of the Campus-wide Information System.

5. The Chief Information Security Officer shall report the status of attendance at educational programs referred to in Paragraphs 1 and 4 above to the information security manager of the department to which the relevant user or the like belongs in accordance with Article 104.6 of the Standards.
6. The information security manager of a department shall confirm the status of attendance at educational programs by users and the like designated by the University Information Security Committee and shall direct, as needed, such users and the like to attend educational programs.

Article 21 (Duties of the information security technical manager and the information security technical staff member of the department)

The information security technical manager of the department that uses the Campus-wide Information System and the information security technical staff member of the department that controls a Specific Department Information System shall, under the direction of the information security manager of the department, shall conduct the following duties:

(1) Monitoring of transmissions in accordance with Article 88.1 of the Standards;
(2) Collection of use records in accordance with Article 89.1 of the Standards
(3) Taking necessary measures to prevent the connected Specific Department Information System from causing troubles, excessive loads and other problems to hardware, software and other components of the Campus-wide Information System;
(4) Cooperation in fact-finding and investigations conducted by the Chief of the Institute for Information Management and Communication in accordance with Article 16.3 and Article 17.1; and
(5) Cooperation in suspension of services and other actions to address a problem or security incident related to the Campus-wide Information System.

Article 22 (Duties of users and the like)

1. When a user or the like uses, as his/her user terminal, an information system that is not provided by the University to access the Campus-wide Information System or a Specific Department Information System, preventive measures to block malicious programs shall be taken for such user terminal, in accordance with the Guidelines for Measures against Invasion by Malicious Programs established by the Chief of the Institute for Information Management and Communication.
2. Users and the like shall make reasonable efforts to cooperate in fact-finding and investigations conducted by the Chief of the Institute for Information Management and Communication in accordance with Article 16.3 and Article 17.1.
3. If a user or the like finds any incident suspected to violate the rules defined in Articles 7 to 11, any incident

suspected to be unauthorized access to the Campus-wide Information System or a Specific Department Information System or material infringement of security of the Campus-wide Information System, he/she shall make reasonable effort to immediately report such incident to the Chief of the Institute for Information Management and Communication.

Article 23 (Miscellaneous)

Any matter that is not provided for in these Rules and is necessary for the use of the Campus-wide Information System shall be determined by the Chief of the Institute for Information Management and Communication.

Supplementary Provisions

These Rules shall take effect on January 12, 2010.

Supplementary Provisions

These Rules shall take effect on February 5, 2013.

Supplementary Provisions

These Rules shall take effect on April 1, 2015.

Supplementary Provisions

These Rules shall take effect on April 1, 2016.

Supplementary Provisions

These Rules shall take effect on April 1, 2017.