Rules on the Use of the Network Connection Service with a Campus-wide Account
[Decided by the Director of
Institute for Information Management and Communication
On April 1, 2017]

Article 1 (Purpose)

1. The purpose of these Rules is to set out the matters applicable when a user accesses a terminal for the service provided by the Institute for Information Management and Communication to connect to the KUINS network (hereinafter the "Network Connection Service") with the use of a Campus-wide Account and to thereby contribute to the smooth use of the information network at Kyoto University (hereinafter the "University").

2. These Rules are provided under paragraph 2 of Article 7 of the Rules for Using the Campus-wide Information System (decided by the executive vice-president for information on January 12, 2010).

Article 2 (Definition)

The following terms used herein have the meanings set forth in the respective items:

(1) *Regulations* mean the Kyoto University Regulations for Information Security Programs (Notification No. 43 of 2003) prescribed by the University.

(2) *Information Security Policies* mean the Kyoto University Basic Policy for Information Security (decided by the Board of Executive Directors on March 25, 2015) prescribed by the University and the Regulations set forth in the preceding item.

(3) *Implantation Regulations* mean the Kyoto University Information Security Program Standards (hereinafter the "Program Standards") prescribed by the executive vice-president for information based on the Information Security Policies, as well as other regulations, standards, and plans.

(4) *Institute Use Regulations* mean the Regulations on Use of Computer Systems for Education and Scholarly Information Network Systems of the Institute for Information Management and Communication, Kyoto University (decided by the director of the Institute for Information Management and Communication on April 27, 2012) prescribed by the University.

(5) *Campus-wide Account* means the Campus-wide account specified in item 21 of paragraph 1 of Article 2 of the Rules for Using the Campus-wide Information System.

(6) *Network Connection Service* means the service provided by the Institute for Information Management and Communication to connect to the KUINS network with the use of a Campus-wide Account, which consists of the Wireless LAN Connection Service, the VPN Connection Service, and the Web Information Outlet Service.

(7) *Wireless LAN Connection Service* means the service provided by the Institute for Information

Management and Communication to connect to a wireless LAN in the University with the use of a Campus-wide Account.

(8) *VPN Connection Service* means the service provided by the Institute for Information Management and Communication to connect to KUINS through a VPN with the use of a Campus-wide Account.

(9) *Web Information Outlet Service* means the information outlet service with the Web authentication provided by the Institute for Information Management and Communication.

(10) *User* means a person who acquires a Campus-wide Account through the procedure set forth in Article 4 of the Rules for Using the Campus-wide Information System and uses the Network Connection Service.

(11) *User Terminal* means the user terminal specified in item 7 of paragraph 1 of Article 2 of the Rules for Using the Campus-wide Information System connected to the Network Connection Service upon authentication with a Campus-wide Account.

(12) The definitions of other terms are as set forth in the Regulations and the Program Standards, and the Rules for Using the Campus-wide Information System.

Article 3 (Scope of Application)

1. These Rules apply to all Users.

2. These Rules cover the wireless LAN SSIDs set forth in Schedule 1.

3. These Rules cover the VPN Connection Service set forth in Schedule 2.

4. These Rules cover the information outlet service with Web authentication.

5. Under paragraphs 2 and 3, a service in which a connection is made with a fixed KUINS-III VLAN shall be excluded from the coverage of these Rules and governed by the Rules for Using the Campus-wide Information System.

Article 4 (Regulations Quoted by these Rules that Should be Complied with)

1. In using the Network Connection Service, a User shall comply with laws and regulations and the University's stipulations and procedures for use under the Information Security Policies, Implantation Regulations, Rules for Using the Campus-wide Information System, and these Rules, as well as the Regulations on Protection of Personal Information in Kyoto University (Notification No. 1 of 2005) and the Regulations on Protection of Individual Number and Specific Personal Information in Kyoto University (Notification No. 49 of 2015).

2. In addition to those set forth herein, a User shall, in using the Network Connection Service, comply with regulations, procedures for use, etc., separately prescribed by the relevant department, if any.

3. A User, who uses an information system, whether within or outside university, by connecting a terminal to the Network Connection Service shall comply with laws and regulations, as well as any stipulations concerning the use of that information system prescribed under a contract between that User and the provider or administrator of that information system.

Article 5 (Matters that Should be Complied with in Using the Network Connection Service)

1. A User shall not use the Network Connection Service for any purpose other than as set forth in paragraph 2 of Article 1 of the Rules for Using the Campus-wide Information System.
2. In using the Network Connection Service, a User shall comply with the matters set forth in Sections 4 and 5 of the Kyoto University Rules for Information Asset Use (approved by the deans and directors on September 4, 2007).

Article 6 (Prohibition of Use of P2P Software)

In compliance with item 2 of paragraph 1 of Article 11 of the Rules for Using the Campus-wide Information System, a User shall not use any P2P software with a function to automatically share files with the public.

Article 7 (Matters that Should be Complied with regarding Measures against Malicious Programs)
1. When a User uses the Network Connection Service by using an information system of the University as a User Terminal, the department information system technical staff member with authority over that User Terminal shall implement on that User Terminal such measures as are in conformity with the Malicious Programs Guidelines for Campus-wide Information System of Kyoto University (decided by the director of the Institute for Information Management and Communication on January 22, 2010).
2. The department information security technical manager shall require a User of that department, who uses the Network Connection Service by using any information system not supplied by the University as a User Terminal, to implement on that User Terminal such measures as are in conformity with the Malicious Programs Guidelines for Campus-wide Information System of Kyoto University.
3. A User who uses the Network Connection Service by using any information system not supplied by the University as a User Terminal shall implement on that User Terminal such measures as are in conformity with the Malicious Programs Guidelines for Campus-wide Information System of Kyoto University.

Article 8 (Response to Violation in Use of the Network Connection Service)
1. If the Director of the Institute for Information Management and Communication finds, or receives a report about, any activity suspected to be in violation of the duty for compliance under Article 5, the director shall notify the Information Network Ethics Committee under Article 8 of the Kyoto University Rules for Information Asset Use.
2. If the director of the Institute for Information Management and Communication finds, or receives a report about, any activity suspected to be in violation of Article 4 or 6, the director shall deal with it under Article 17 of the Rules for Using the Campus-wide Information System.

Article 9 (Response to Incidents with User Terminal)
1. If the director of the Institute for Information Management and Communication finds any state suspected to be illegal access to a User Terminal (including cases where it cannot be decided whether it is illegal access or not; the same applies hereinafter) or other security violation, the director shall immediately notify the Information Network Risk Management Committee under paragraph 1 of Article 17 of the Rules for Using the Campus-wide Information System.

2. A department information security manager who has received notice under paragraph 2 of Article 17 of the Rules for Using the Campus-wide Information System shall immediately identify the relevant User and the relevant User Terminal and shall, under paragraph 1 of Article 98 of the Program Standards, investigate the cause of the incident and formulate recurrence prevention measures, as well as submit a written report on the results thereof to the Information Network Risk Management Committee.

3. If the director of the Institute for Information Management and Communication receives from the Information Network Risk Management Committee instructions on the prevention of the spread of damage, the director shall immediately implement measures for the prevention of the spread of damage.

Article 10 (Participation in Education for Information Security Measures)

A User shall participate in lectures under paragraph 1 of Article 20 of the Rules for Using the Campus-wide Information System.

Article 11 (Duties of Department Information Security Technical Manager and Department Information System Technical Staff Member)

The department information security technical manager of a department to which a User belongs and the department information system technical staff member with authority over a User Terminal shall implement, under the instructions of the department information security manager, the following measures on the User Terminal:

(1) Collection of usage records under paragraph 1 of Article 89 of the Program Standards

(2) Steps necessary for preventing a connected User Terminal from causing failure or excessive load on the hardware or software of a campus-wide information system

(3) Cooperation with a Department Information Security Manager to confirm and investigate facts under paragraph 2 of Article 8 and paragraph 3 of Article 9

(4) Cooperation in suspension of a service or other measures against a failure of the Network Connection Service or a security incident

Article 12 (Duties of Users)

1. A User shall cooperate with a department information security manager to confirm and investigate facts under paragraph 2 of Article 8 and paragraph 3 of Article 9.

2. If a User finds any activity suspected to be in violation of the duty for compliance under Articles 4 through 6 or any state suspected to be illegal access to a User Terminal or other security violation, the User shall strive to promptly report such fact to the director of the Institute for Information Management and Communication.

Article 13 (Miscellaneous Provisions)

In addition to the provisions herein, matters necessary for the Network Connection Service shall be determined by the director of the Institute for Information Management and Communication.

Supplementary Provisions

These Rules shall come into force on April 1, 2017.

These Rules shall come into force on June 1, 2017.

Schedule 1: Wireless LAN SSIDs covered by these Rules

SSID
KUINS-Air
eduroam

Schedule 2: VPN Connection Service covered by these Rules

Name of service
IKEv2
PPTP
OpenVPN
SSTP
SSH PortForward
UQ WiMAX