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

Guidelines for Establishment of Access Points of Wireless LAN Connected to KUINS

(Approved by the Chief of the Institute for Information Management and Communication on February 8, 2012)

1 Purpose

The following guidelines provide for considerations at the Information Security Committee of each department in Kyoto University (hereinafter, "University") according to Article 31, paragraph 2 of the Kyoto University Information Security Program Standards (hereinafter, "the Program Standards") and Article 23 of the Rules for Using the Kyoto University Campus-Wide Information System (hereinafter, "the Rules of Usage") when each department establishes an access point of the wireless LAN that conforms to IEEE 802.11 standard (hereinafter, "AP") connected to the Kyoto University Integrated information Network System (hereinafter, "KUINS"), in order to help improve information security of the University.

2 Considerations on the use of APs

1 An information system technical staff member who is responsible for management of an AP (hereinafter, "AP staff") shall take measures to limit the access to the relevant AP. (Article 2, item (14) of the Rules of Usage)

2 An AP staff shall take appropriate measures to ensure that only the Users defined in the Rules of Usage have access to the relevant AP, in principle. (Article 2, item (10) of the Program Standards)

3 A department information security technical manager (hereinafter, “Department Manager”) shall prepare the authorization procedure for the temporary use of relevant APs by the Temporary Users of any specific department information systems defined in the Rules of Usage. (Article 2, item (13) of the Rules of Usage and Article 2, item (11) of the Program Standards)

4 In the procedure prescribed in paragraph 3, the Department Manager shall take necessary measures to ensure that such Temporary Users observe the Rules of Usage. (Article 6, paragraphs 2, 4 and 5 of the Rules of Usage)

3 Specific department information systems and user terminals that can be connected to APs

1 An AP staff shall take necessary measures to limit specific department information systems and user terminals that can be connected to APs. (Article 2, items (6), (7), and (14) of the Rules of Usage and Article 31, paragraph 2, item (8) of the Program Standards)

4 Procedures for Establishing APs

1 An AP staff shall obtain approval for establishing an AP from the Manager of the department where the AP is to be established. (Article 18 of the Rules of Usage)

2 A Department Manager shall prepare the application procedure to start and end the establishment of APs. (Article 31, paragraph 2, item (1) of the Program Standards)

3 An AP staff shall obtain prior consent for connecting an AP to KUINS-II from the relevant subnet contact person. (Article 18, paragraph 2 of the Rules of Usage)

4 An AP staff shall obtain prior consent for connecting an AP to KUINS-III from the relevant VLAN manager. (Article 18, paragraph 4 of the Rules of Usage)

5 Technical Requirements for APs

1 An AP staff shall protect the communications through the relevant AP with encryption. (Article 31, paragraph 2, item (7) of the Program Standards)

2 An AP staff shall ensure that, in principle, the relevant AP encrypts its communication by virtue of either WPA or WPA2 with AES, of which protection satisfies paragraph 1 of this article. WEP must not be used as an encryption method for the purpose.

3 For the encryption with WPA-PSK or WPA2-PSK, an AP staff shall decide a text consisting of 10 characters or longer that is sufficiently hard to guess as a passphrase. The passphrase must be changed at least once a year, and conform to the Password Guideline for Users of Kyoto University Campus-Wide Information System.

4 An AP staff shall take necessary measures for the firmware or the like that runs at the relevant AP in conformity with the Kyoto University Guideline for Measures against Invasion by Malicious Programs to Campus-Wide Information System. (Article 12 of the Rules of Usage)

5 A Department Manager shall defining naming rules regarding the SSID of the AP in the department if necessary.

6 Exceptional measures

1 An AP Staff, who cannot comply with the guidelines above due to unavoidable circumstances, shall make an application to obtain approval from the relevant Department Manager.

2 The Department Manager shall provide for the procedure to review the exceptional

measures stated in this article.

3 An Department Manager, who gives approval for the exceptional measures stated in this article, shall record the reviews regarding the exceptional measures, and report to the Information Security General Manager. (Article 96, paragraph 2 of the Program Standards)

Supplementary Provisions

1 Department Managers must take necessary measures to ensure that all existing APs connected to KUINS conform to these guidelines by March 31, 2013.

Supplementary Provisions

This guideline becomes effective from April 1, 2015.