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

# Kyoto University Guideline for Measures against Invasion by Malicious Programs to Campus-wide Information System

(Established by the Chief of the Institute for Information Management and Communication, January 12, 2010)

1. This Guideline is established to stipulate matters to be observed by the information system technical staff member of a department and users and the like in order to prevent invasion by malicious programs to Specific Department Information Systems or user terminals connected to the Campus-wide Information System in accordance with Article 12 of Rules for Using the Kyoto University Campus-wide Information System.

2. The information system technical staff member of the department controlling user terminals (excluding information systems not provided by the University) shall take the following anti-malicious program measures for user terminals (excluding information systems not provided by the University):

(1) If anti-malicious program software (software to protect information systems from virus, spy ware, Trojan horse, worm, bot, route kit and other malicious programs) is available, such software shall be installed and run on the information system in accordance with the agreement with the provider of the software;

(2) The anti-malicious program software and the malicious program definition file used by such software shall continually be updated;

(3) When new software is installed, the scan function of the anti-malicious program software shall be run to confirm that new software does not contain malicious programs. The scan function shall also be run periodically to check for invasion by any malicious program;

(4) The information system technical staff member of the department shall pay close attention to release of information on security vulnerability of the computer system and security update programs. When a security update program is released, it shall always be installed on the computer system;

(5) Upon receipt of instruction from the Chief of the Institute for Information Management and Communication, the information system technical staff member shall implement anti-malicious program measures for the relevant information system in accordance with such instruction;

(6) No software inappropriate for educational/research activities and any other activities of the University shall be installed;

(7) Software of unknown origin shall not be installed; and

(8) The information system technical staff member of the department shall monitor and control software installed on a user terminal used by more than one person who belongs to the department.

3. The information system technical staff member of the department controlling a Specific Department Information System shall take the following anti-malicious program measures:

(1) Implement the anti-malicious program measures specified in Paragraph 2 (excluding Item (8)) of this Guideline for such Specific Department Information System; and

(2) Monitor and control software installed on such Specific Department Information System.

4. Each user or the like shall take the following anti-malicious program measures:

(1) If the user or the like uses any information system not provided by the University as a user terminal to connect to the Campus-wide Information System or a Specific Department Information System, he/she shall check to ensure that anti-malicious program measures equivalent to those listed in Paragraph 2 are implemented for such user terminal.

(2) If the user or the like finds any problem in using the Campus-wide Information System or a Specific Department Information System, he/she shall immediately report the incident to the information security manager of the department that controls such information system.