September 15, 2009
Executive Vice-President for Information Infrastructure & Security Management

Rules for Kyoto University Information Network Use

You are reminded to pay careful attention to and to abide by the relevant rules and regulations of Kyoto University when making use of the Information Network at our university.

1. Published Regulations concerning information network use

- Basic Policy for Information Security (URL* below)
- Regulations for Information Security Programs (URL* below)
- Information Security Program Standards (URL* below)
  Website URL*: http://www.iimc.kyoto-u.ac.jp/ismo/regulation/
- Rules for Information Asset Use (Approved by the Council of Department Chiefs, September 4, 2007) (see attachment 1)
- Prior notification of the use of P2P file sharing software (NOTE 1) on the Kyoto University Information Network System (KUINS)

2. Compliance Rules

(1) Purpose of Use (Article 3 of th "Rules for Information Asset Use)

Information assets shall not be used for any purpose other than as designated by their administrator.

(2) Prohibition on Transmission of Information (Article 4)

No person shall make via information network such transmission of information that -

i) is deemed to be discriminatory, defamatory, insulting, or harassing,
ii) infringes on the privacy of any individual,
iii) breaches the obligation of confidentiality,
iv) infringes on copyrights or other property rights, or
v) mitght be subject to punishment by law or induce a claim for damages or any other civil liability.

(3) **Prohibition on Use of Information Devices** (Article 5)

No information devices shall be used to conduct or attempt to conduct such acts that -

i) infringe on the confidentiality of communications,
ii) monitor communications on the network or collect information on the use of information devices in breach of relevant provisions in the Information Security Policies,
iii) circumvent access controls or are similarly elusive.
iv) detect security vulnerabilities in the systems without explicit instruction to do so from the administrator.

v) obstruct smooth access to information assets by placing excess loads on the system, or
vi) encourage any of the above-mentioned acts.

(4) Restriction on the use of P2P file sharing software

- In connection with KUINS-3, use of P2P file sharing software (hereinafter P2P) is totally banned.
- In connection with KUINS-2, you must obtain permission from the Departmental Information Security Officer (your dean).

[Reasons]

- P2P is often used to share copyrighted material for non-academic purposes.
- P2P tends to unknowingly distribute files, causing copyright infringements.
- Downloaded files via P2P are often infected with viruses or spywares.
- Computers operating P2P are in danger of leaking data.
- Burdening on the network with excess loads, P2P is a possible cause of the system failure.

(5) **Other Instructions**

Do read through the on-line e-Learning presentation on Information Security.
Always download and install windows security updates.
Safely store your account IDs and passwords.
Use anti-virus software in accordance with their terms of use or similar documentation.

3. About the Copyright Law

Unauthorized distribution of copyrighted materials is against Copyright Laws. Violators may be subject to criminal penalties and/or be sued by the owners of such rights.
As of January 1st 2010, it will also be illegal to knowingly download materials that infringe upon copyright laws.

NOTE 1 - What is P2P file sharing software?

Peer to peer (P2P) file-sharing software is a tool for sharing files with an unspecified number of users via the Internet. P2P is often used in ways that infringe upon copyrights and should be cautioned against.

【Common Titles】

Winny, Share, BitComet, BitTorrent, Lime Wire, Cabos, Win MX

【Who to contact regarding unauthorized access】

1. The Departmental Information Security Officer (Dept. Dean), or the Departmental Information Security Committee.
2. The KU Information Security Management Office

Tel: 075-753-7490

E-mail: i-s-office@media.kyoto-u.ac.jp

Kyoto University Rules For Information Asset Use

(Approved by the Council of Department Chiefs, September 4, 2007)

Chapter 1 General Provisions

Article 1 (Principles)

Faculty members and office personnel, students and other members of Kyoto University are expected to maintain high ethical standards and a strong sense of responsibility, while emphasizing the freedom and independence of education and studies when they use information assets of the University (as defined in Article 2 of the Kyoto University Regulations for Information Security Programs (Notification No. 43, 2003); the same definition applies hereinafter). The purpose of these Rules is to ensure proper and efficient use of information assets, while following the spirit of freedom and harmony advocated in the philosophy of the University. In interpreting and applying these Rules, academic freedom, freedom of expression and other fundamental human rights guaranteed under the Constitution of Japan shall not be violated.

Article 2 (Definition)

In these Rules, the terms "University," "information assets," "Information Security Policies," "department," "faculty members and office personnel," "students," "information security manager of the department," "information system technical staff member of the department," "Information Network Risk Management Committee," "Information Network Ethics Committee," "department committee," "monitoring," and "use records" have meanings as defined in Article 1, and relevant paragraphs in Articles 2, 5, 5-3, 7, 7-2, 8, 11 and 12 of the Kyoto University Regulations for Information Security Programs, respectively.

Chapter 2 Rules

Article 3 (Use for Designated Purposes)

Information assets shall not be used for any purpose other than as designated for such information assets.

Article 4 (Provision of Information Not Allowed)

The following information shall not be provided on any communication network:

(1) Provision of information that is deemed to be discriminatory, defamatory, insulting, or harassing,

(2) Provision of information that infringes on the privacy of any individual,

(3) Provision of information that breaches the obligation of confidentiality,

(4) Provision of information that infringes copyrights or other property rights, or
(5) Provision of information that may be subject to any punishment by law or a claim for damage or any other civil liability.

Article 5 (Use of Information Devices)
No information devices shall be used to conduct, or attempt to conduct, any of the following acts:
(1) Infringement of confidentiality of communication,
(2) Monitoring of communications on the network or collecting information on use of information devices in breach of relevant provisions in the Information Security Policies,
(3) Any act to evade access control (restricting information allowed to be accessed, and access types allowed to be used, by each user who accesses to the information system) or any other similar act,
(4) Unauthorized detection of security vulnerability of systems without request from the administrator,
(5) Any act that obstructs efficient use of information assets, such as placing excess load on the system, and
(6) Any act that encourages any of the above-mentioned acts.

Article 6 (Responsibility for Management)
To prevent acts as referred to in Article 5 above, information managers (faculty members and office personnel who created or collected information; the same definition applies hereinafter) and the information system technical staff members of each department shall perform proper management of information assets for which they are responsible.

Chapter 3 Response to Offences
Article 7 (Establishment of Contact Points)
To receive complaints and other information (hereinafter “complaints”) regarding acts that are suspected to offend any of the rules stipulated in Chapter 2 (hereinafter “suspicious acts”), the Information Security Management Office is established in the IT Services Division, Information Management and Communication Department (hereinafter the "Information Security Management Office"). Each department shall also designate a contact office or person that is responsible for receiving complaints.

Article 8 (Notification of Suspicious Acts)
1. The Information Security Management Office shall notify the Information Network Ethics

Committee (hereinafter the "Ethics Committee") of complaints and information on suspicious acts that the Information Security Management Office has detected.
2. If the Information Network Risk Management Committee finds a suspicious act, it shall notify the Ethics Committee thereof.
3. If the Ethics Committee finds a suspicious act, it shall notify the relevant department committees thereof.

Article 9 (Request to the Ethics Committee)
The department committee shall notify the Ethics Committee of a suspicious act and may request the Ethics Committee to conduct investigation of offenses specified in Article 10 or take the measures specified in Article 11 or both.

Article 10 (Investigation of Offenses)
1. If a suspicious act is found or reported, the relevant department committee shall promptly conduct an investigation to find out relevant facts. In finding out relevant facts, the committee shall follow appropriate procedures, including collecting comments from the party that has conducted the reported suspicious act to the extent practicably possible.
2. Information managers and the information system technical staff members of the relevant departments shall cooperate with such investigation. The department committee may request relevant parties to submit records of monitoring and use such records to the extent necessary for the investigation.
3. The Ethics Committee may conduct an investigation specified in the preceding Paragraphs as it deems necessary. The Ethics Committee shall notify the relevant department committee of commencement of its investigation. The Ethics Committee and the department committee may conduct investigation in collaboration.
4. If the department committee decides on closure of such investigation, the Ethics Committee shall not conduct an investigation of such department.
5. Facts found out in the investigation shall not be disclosed to the public unless otherwise required by law.

Article 11 (Measures Against Offenses)
1. If an act that contravenes any of the rules stipulated in Chapter 2 (hereinafter an "offense") is confirmed, the information security manager of the department may direct the person who has committed such offense (hereinafter an "offender") to stop such offense. However, if urgent countermeasure is deemed necessary, or if the offender cannot be identified, or if the offender does not obey such direction, the information security manager

of the department may take necessary countermeasures to stop such offense, including blocking transmissions related to such offense. The information security manager of the department may ask other departments to cooperate in such blocking or other countermeasures.

2. The Ethics Committee may advise the information security manager of the department to give such direction or take such countermeasures as specified in Paragraph 1 above.

3. The Ethics Committee may give such direction or take such countermeasures as specified in Paragraph 1 above as it deems necessary; provided, however, that the Ethics Committee shall listen to and consider opinions of the information security manager of the department beforehand, unless urgent countermeasure is deemed necessary.

4. If the information security manager of the department decides not to give a direction or take countermeasures, the direction or countermeasures given or taken by the Ethics Committee shall lose effect.

Article 12 (Measures Against Offender)

1. The information security manager of the department may take proper measures against the offender, including provision of security education to such offender.

2. The Ethics Committee may express its opinion regarding proper measures as referred to in Paragraph 1 above.

Supplementary Provisions

These Rules shall take effect on October 1, 2007.

Supplementary Provisions

These Rules shall take effect on April 1, 2009.