Guidelines for Use of Campus Network and Servers

(Corresponding to matters regarding the use of campus networks and servers)

Established: June 30, 2004
Revised: March 25, 2005
Revised: April 1, 2009
Revised: April 1, 2010
Revised: September 21, 2010

1. Purpose

"Guidelines for Use of Campus Network and Servers" describes matters that should be observed at least when using clients or servers connected to the network within the premise of Kobe University (hereafter our university). Specifically, the items described in this document are applied when using personal computers connected to the network on the campus, and when using information services provided by Kobe University. We would like to ask you to observe these guidelines since these are essential matters to implement our university's information security policy.

2. Principles of Use of Networks, Clients, and Servers

Clients and servers should be used in accordance with the acceptable use policy (including requirements, procedures, and arrangements) defined by the system administrator. If not clarified in the policy, these devices should be used in accordance with Appendix A, "Principles of Use of Network, Clients, and Servers," described later. Please note that the most of the matters described in this appendix need to be observed even though when using clients and servers outside the campus.

3. Permission for the Usage of Campus Network and Servers

3.1 Use of clients that are connected to the campus network

- Use of general usage clients

  - ✧ On the campus, clients are installed which can be shared by students and teaching staff members. Permission should be gained from the administrator of the client before use, and those clients should be used in accordance with the acceptable use policy here defined. In many cases, user IDs and passwords are provided for use.
  - ✧ The administrator of each client is different according to the client used. Personal computers available for general students are controlled by the Information Science and Technology Center (hereafter the center); however, there are computers which are controlled by other divisions. Check with the office of each division if the administrator is unknown (depending on each acceptable use policy, permissions for usage are not always issued to all applicants).

- Client use policy
  - ✧ Qualified users for each client and the available use policy are defined by the administrator of each client. Contact the administrator for details.
- Other
  - ✧ Many personal computers, other than client devices for general use, are installed in laboratories and offices. These computers are installed for education, research, or operations. In principle no one other than those permitted can use these clients.

3.2 When the client is connected to the campus network

Each client should be connected to the client in accordance with the procedure defined in “Guidelines for Use of Clients.” Excerpts of the main points are listed below:

- When clients are connected to the campus network, in principle, you should gain permission from the system administrator of the relevant division.
- The person in charge of providing connection permission and assigning IP addresses is different depending on each division. Contact the network administrator of the section you belong to (see Appendix C: the list of network administrators of each division).
- Those connectable clients must be available for installing security measures so as not to cause any damage due to network connection. Technically not all clients that can be connected to the network should be connected. Those clients with an OS for which the technical support provided by the vendor had already expired are unsecured.
- Therefore, those unsecured clients should not be connected to the network.
- Client users are required to take regularly sufficient security measures for clients they use, by following the instructions given by the network administrator. For example, this includes the following things when using a Windows personal computer: applying the latest security patches, keeping virus definition files updated, introducing antivirus software, and not casually opening attachment files of e-mails (see Appendix A,

"Guidelines for installation and use of clients," in order to secure your personal computer).

- Install clients in a room to which only approved users can enter, or configure authentication with user IDs and passwords for clients.

3.3 Use of other servers from clients connected to the campus network

A server is an information device that is accessed by and shared with multiple clients. For example, typical servers include a Web server, mail server, file server, and printer server.

- In principle permission should be gained from the administrator in order to use servers. Where user IDs and passwords are necessary, an application should be submitted to the administrator. However, public Web servers and FTP servers are an exception. The administrator differs according to the server used. Contact the network administrator of the division you belong to for details.
- Use of unqualified servers could be regarded as breach of law (Act Concerning the Prohibition of Unauthorized Computer Access) in some cases. Such acts must be avoided.

Supplementary Provision

These guidelines were put into effect starting June 30, 2004.

Supplementary Provision

These guidelines were put into effect starting March 25, 2005.

Supplementary Provision

These guidelines were put into effect starting April 1, 2009.

Supplementary Provision

These guidelines were put into effect starting April 1, 2010.

Supplementary Provision

These guidelines were put into effect on September 21, 2010, and were applied starting July 1, 2010.

(Appendix)

A: Principles of Use of Network, Clients, and Servers

A1: Prohibition of Use for Other Purposes

- Use of network should be limited to purposes of education, research, academic information services, office work, and other purposes that are necessary in our university.
- Any use for profit without permission is not allowed.
  - Do not use computers and networks installed in our university for profit, even for socially acceptable business transaction.
- Any private use that goes beyond the bounds of social standards is prohibited.
  - Job hunting activities and group activities are accepted as part of extracurricular activities; however, personal and avocational correspondence should be done abstinently

A2: Prohibition of acts of crime or that could lead to crime

It is understood that in general terms no criminal act should be committed. However, criminal acts with regard to use of information networks are not always easily recognized properly. It should be noted that if a user infringes upon the rights of others by committing an illegal act, our university must accept responsibility. However the individual user who committed such an act could also be charged.

- Usage of devices as an act that violates domestic and international laws, or as means of such acts
  - When accessing computers abroad, the related laws of the relevant country should be observed.
- Infringement on copyright and rights neighboring on copyright
  - Infringement on copyright and rights neighboring on copyright
    1. Observe the terms and conditions of use (personal use, license, etc.) that apply to software programs.
    2. The software license should be managed by the user or the responsible system administrator. Reports should be made where disclosure of information regarding the user license is required by the information system management.

3. Prepare necessary budgets for software needed for education and research.

- Publication of parts or all parts of printed materials (literature, pamphlets, or photos etc.), which are scanned by a scanner or photographed using a digital camera, on a website without having expressed permission of the owner of the copyright
- Obtaining of images, which are used on other websites, without having expressed permission of the owner of the copyright in order to publish those images on a website
- Quotation of parts or all parts of written document (not for an appropriate purpose, more than one's purpose, without any attribution, or without citing the name of the writer) without having expressed permission of the owner of the copyright.
- Modification or adaptation of written material without having expressed permission of the owner of the copyright

  Modification without having expressed permission itself could be infringement of the copyright

  Publication of a summary or translation of written material should be done only after gaining expressed permission from the owner of the copyright.
- Infringement on the rights neighboring on copyright of music players, arrangers, adapters, and performers.

  The copyright of sound data, images, and video footage are also protected.
- Infringement on portrait rights

  Publication of a picture of others without having expressed permission of objects or individuals in the picture leads to infringe of portrait rights. In some cases, famous art works or buildings as objects in a picture could also be regarded as infringement of a copyright.

  Although there is no malicious intent on publishing such things, it could be regarded as infringement on a copyright if music or video data, or any other commercial software program is made accessible via a network.
- Publication of obscene text or images
- Fraudulent access to a computer on campus or off campus

  Sending massive amounts of meaningless data to computers on campus or off campus in order to paralyze the network or computers purposely

Use of another person’s account

The use of another individual account should not be done even though the other person gives their permission.

A3: Prohibition of any act that is offensive to public order and morality, and social equality

- Violation of fundamental human rights
  - Slander and libel of others on a website
  - Disclosure of the content of e-mail received (except for when required to do so for office work)
  - Disclosure of another person’s personal information
    - Information can be transmitted to an unspecified number of people on websites or bulletin boards. There could be people who maliciously collect and use such information. Caution should be exercised not to disclose any personal information related to others including residential address, phone numbers, photos, or their date of birth. Caution should be taken and kept to a minimum when disclosing your own personal information.
  - Publication of image data that makes others uncomfortable including pornographic material or pictures on websites
  - Sending direct mails to the unspecified number of people
  - Other acts that cause a breach of the network usage manners (see the book “Information Basics: A Hand Book of Information Literacy of Kobe University”)

B: Measures that should be taken when a violation is found regarding the above-mentioned matters

B1: When fraudulent usage is suspected

If fraudulent usage is suspected, the system administrator could temporarily suspend the user ID or restrict network use.

B2: When fraudulent usage is confirmed

Measures will be taken in accordance with the Incident Procedure Manual.

C: List of administrators of each division

See http://www.istc.kobe-u.ac.jp/conents/service/otherService/wic/.