Guidelines for the Use of Information Systems at the University of Tsukuba

September 26, 2008
Information Infrastructure Committee

1. Purpose of the guidelines

The following guidelines refer to the rules with which users of the information systems need to comply at the University of Tsukuba.

2. Framework of the guidelines

The guidelines consist of the following 5 main areas. Other than these, Guidelines for Releasing Information on the Web have also been established.
The five items are as follows:

- Guidelines for the use of computers
- Guidelines for computer security
- Guidelines for password security
- Guidelines for the use of e-mails
- Guidelines for web browsing software

3. Guidelines for the Use of Computers

3.1 User ID

Users must not use any ID to which they are not assigned.

3.2 Password

The user must set a password that cannot easily be inferred by others, and securely control it.

3.3 Prohibition on unauthorized access

The user must not attempt or engage in unauthorized access to other information systems.

3.4 Clear indication of identity when transmitting information

Users must clearly indicate their name and affiliation when sending personal e-mail or transmitting information on the internet in order to make clear where the responsibility lies. False identity or anonymity is, as a rule, not permitted.
Releasing information on the internet refers to the following operations:

- Sending posts to mailing lists
- Releasing information on web page forms
- Sending posts to newsgroups
- Sending messages on the remote meeting system
- Sending posts on message boards
- Any other similar act pertaining to the above

3.5 Web contents policy

Information released through the internet shall, in principle,

concern research or educational activities. The following activities are not allowed:

(a) Related to criminal and civil laws and regulations
- For the purpose of damaging the reputation of others
- Obscenity
- Infringement of copyright
- Infringement of privacy or image rights
- All other violations of laws and regulations

(b) Related to university regulations
- Commercial activities
- Activities concerning specific political parties or religious groups
- Damaging the reputation of and demeaning the University of Tsukuba
- Campaign activities as described in Public Office Election Law
- All other violations of university regulations

3.6 Use of computer facilities

The user must not take any actions that could possibly damage the facilities such as the computer terminals.

3.7 Net manners

The user must not disturb other users when using the network.

3.8 Network bandwidth

The user must not engage in activities that significantly occupy the bandwidth of the network.

3.9 Off campus access to the university network

The user must comply with the following rules when connecting to the university network from off-campus networks, except for the web services that are open to the public:

(a) The user must pay utmost attention in using authentication information (such as passwords and secret keys) so it will not be leaked. In case authentication information is leaked or there is a possibility of a leak taking place, the user must report to the system administrator of the university network and follow his/her instructions.

(b) The user must not attempt to be connected with the university network from terminals where security is not guaranteed (such as at internet cafes).

3.10 Use of communal terminals

The user, in using the computer terminals in the computer room and shared space, must comply with the following rules:

(a) Lock the computer in the case of temporarily leaving the room while operating a terminal.

(b) Do not leave open the door or windows of the computer room. Do not change the temperature setting on the air conditioner in the room.

(c) Turn off the computer equipment after use. However this does

not apply if the system administrator specifically instructed not to do so.

(d) Avoid wasting paper by not making unnecessary prints.

3.11 Installing application software

The user must comply with the following rules when installing application software:

(a) Do not install nor use P2P file-swapping software.

(b) Do not install nor use software that does not fall in line with the purpose of supporting education or research.

(c) Follow the requirements when installing and running the application.

(d) Before installing new software, always check for malware, such as viruses or spyware, using virus checking software.

(e) Do not install nor use programs of unknown origin.

3.12 Use of external media

The user must comply with the following rules when using external media such as CD-ROMs, floppy disks, and USB flash memory drives:

(a) Do not leave the external media unattended that contains the user’s files.

(b) Do not use unattended external media or media whose origins are unknown on the university computers. Report to the system administrator if you find such media.

(c) In case the used external media are to be handed over or disposed of, completely erase the data using data erasing tools or physically destroy the media so the data cannot be restored.

3.13 Reporting obligation

The user must report promptly to the system administrator when the following are found:

(a) Vulnerabilities or problems in operating systems or applications on the computer terminals, or host computer and network equipment.

(b) Web content that might infringe copyright, classified material, or personal information on the university host computer.

(c) Web content on off-campus host computers that carries without prior consent classified material of the university, personal information of the faculty members, or content to which the university possesses the rights.

4. Guidelines for Computer Security

4.1 Virus protection

The computer terminal administrator shall check to prevent malware such as viruses and worms, and must comply with the following rules:

(a) Be aware of the vulnerabilities of the operating systems and software, and promptly make modifications to fix problems.

(b) Have the computer installed with anti-virus software and always renew the virus information database.

4.2 Installation and use of applications

The computer terminal administrator, when installing and using applications, must comply with the rules in 3.9 as well as the following rules. However, this shall not apply in cases for the purpose of or in support of education and research, for which the system administrator gives permission.

(a) Do not install or use software that could bring pressure on network bandwidth.

(b) Do not install or use applications that intercept information on packets sent out other than one's own terminal (packet sniffing).

(c) Do not install or use any other applications that infringe university regulations of network use.

4.3 Proper management of computer terminals

The computer terminal administrator must comply with the following rules:

(a) Do not alter the computer terminal settings in such a way that other people can use it without authentication. If the computer does not have an authentication function, set it up in a way that only authorized persons can use it.

(b) Set up the terminals to prevent the general public from having access to the university computer via internet.

(c) Do not allow non-account holders to use the university computers, except where it is needed for educational or research-related needs with the administrator's specific permission.

(d) For desktop terminals, lock up the facility so non-account holders cannot physically have access to it, and use wire-locks to prevent theft where they are needed.

(e) For portable terminals, do not leave them unattended even for a short time, and keep them in a lockable place.

(f) Set the BIOS terminal so it cannot be started up by unauthorized persons using CD-ROM or any external media, and also set a password.

(g) When a computer terminal is to be disposed of or handed over, completely erase hard drives and nonvolatile memory using appropriate software or physically destroy them, so the classified information and other vital information will not remain.

4.4 Means to cope with computer viruses

When the terminal is infected with computer viruses or virus-infection is suspected, the computer terminal administrator must remove the affected terminals from the network to prevent the spread of the viruses, contact, report and follow the instruction of the technical personnel of the department. All the network cables, wireless LAN cards, wireless LAN adaptors with USB keys must be removed from the network. If the computer terminals have built-in wireless LAN adaptors, the wireless LAN of the computer must be disabled.

5. Guidelines for password security

5.1 Changing initial password

The users must promptly change the initial password into one of their own once their account has been issued. Do not keep using the initial password in using the university information system.

5.2 Password policy

The user must set a password that meets all the conditions described below:

- Minimum length is 6 characters
- Include one letter from each of the following four categories
  (a) upper-case letters (A-Z)
  (b) lower-case letters (a-z)
  (c) one or more numerical digits (0-9)
  (d) special characters the operating system allows you to use
- Do not set passwords that can easily be inferred as follows:
  - Letters that can be deduced from the user's account information (name, user ID, etc.)
  - Anagram of the above mentioned letters or letters with numbers or special characters
  - Words found in a dictionary
  - Name of prominent figures

5.3 Password security

The user must securely control one's password. Do not write it down nor post a memo onto a computer terminal. The user must not let a third party know one's own password, and must strive to pay utmost attention not to carelessly let others know the password.

5.4 Ban on access to university network from off-campus publicly shared terminals

Because there is a higher risk of the password and account information being stolen, do not try accessing the university network from off campus terminals used by the general public, such as internet cafes.

5.5 Changing password

The users must change their password when the account issuer (the director of the Academic Computing and Communications Center for on-campus accounts, system administrator for each individual system) urges them to. The new password must not appear similar to the original one.

5.6 Obligation of password accident reports

The user must promptly report to the account issuer in case of a third party using one's password or the possible danger of it.

6. Guidelines for the use of e-mail

6.1 E-mail ID and e-mail address

(a) The user must not use an e-mail ID (ID for logging-in to e-mail server hereafter referred to as login ID) and/or an e-mail address that was issued to others.
(b) The user must not share a login ID and/or an e-mail address.
(c) The user must report to the technical personnel of the e-mail system department when one does not need to use e-mail any longer.
(d) The user must consult with the technical personnel of the e-mail system department for special permission or set-up when login IDs and e-mail addresses given for users with specific services, job titles or departments need to be shared by multiple people within the section, or when job responsibility was taken over by a third party.

6.2 Suspicious e-mail policy
(a) The user, unless absolutely necessary, must not open suspicious e-mails that appear to have been sent from unknown or unreliable sources.
(b) The user must not open suspicious e-mail attachments unless absolutely necessary.

6.3 Sending e-mail
(a) Always check to see if the correct e-mail address was entered.
(b) Always check for viruses when attaching files to e-mail.
(c) In the case of sending attachment files that contain confidential information, consider setting passwords on the attached file.

6.4 Contents of the e-mail
The user must not transmit e-mails that fall under the following categories:
- E-mails that infringe on confidentiality
- E-mails that infringe intellectual property rights, copyright, trademark rights, image rights, and licensing rights
- E-mails that are sexually harassing or infringe on human rights
- E-mails that contain rude descriptions and defamation of people
- E-mails that contain pyramid schemes
- E-mails that contain threats, personal money-making schemes and offers

6.5 Configure e-mail software
(a) As a rule, the user must not send e-mails in HTML format. This is to reduce security vulnerabilities for the receiver.
(b) The user must set the e-mail software to use text format (rich text format included). As a rule, the sender should not use the HTML format setting in order to avoid accessing fraudulent homepages and malicious scripts.
(c) The user must not use the preview function on the e-mail software for HTML formatted e-mails.

6.6 SPAM (junk mail)
(a) The user shall not disclose one’s e-mail address unless

absolutely necessary.

(b) The user, when disclosing one's e-mail address through the internet, must strive to exercise one's ingenuity, so the e-mail address cannot be automatically acquired. Some ideas include: paste the e-mail address in the form of image information, use double-byte characters on purpose, and insert unnecessary letters before and after the e-mail address.

(c) The user, when receiving unwanted mails, is encouraged to ignore them. Replying to the sender might result in confirming the e-mail address in use, thus resulting in further junk mail.

6.7 Netiquette

(a) Do not take part in sending or forwarding chain mail (the type of mail that urges the receiver to send multiple copies to other people).

(b) Do not send spam messages (e-mails that are sent at random, such as commercial direct mail) or junk mail (e-mail messages that contain useless pieces of information).

(c) Always put titles on the e-mail messages. The titles should be succinct and relevant in describing the contents of the message.

(d) Avoid using slang and abbreviated expressions that are not known to the public.

(e) Avoid using non-standard characters (Japanese characters that will not be shown correctly depending on the operating system, such as Macintosh).

(f) When writing e-mail, begin a new line after 30 to 35 characters.

(g) Notice the difference between To: and CC: in the address field in sending e-mail. To: should be used when one expects a reply from the receiver of the message.

7. Guidelines for web browsing software

7.1 Purpose of web browser use

The user must understand that the information system of this university is provided for the purpose of promotion of education and research, and performing jobs and its supporting duties, thus access to websites should be within the scope of necessity.

7.2 Web browsing policy

(a) The user must understand that by browsing any given website, the university domain name and IP address will remain as a record on the server of the website.

(b) Do not offend public order and morals by improper messages or use of the internet. Even a simple message on a bulletin board could leave a negative impression regarding the university or people associated with the university.

(c) In web searches, do not browse the results of the search without careful consideration, as it could include links to harmful websites.

(d) Do not carelessly click on links even if it is a well-known site, as there are numerous web links that try to direct the

user to fraudulent sites or make the user download malicious software.

(e) While browsing web pages, do not download software when there is an obscure security warning sign that urges the user to start downloading. There are high possibilities of downloading viruses and malicious software from those sites.

(f) The user must be aware that reloading the same website repeatedly in a short time period could be regarded as a denial-of-service attack (an explicit attempt by attackers to prevent legitimate users of a service from using that service). This could cause blockage of access from the relevant domain or IP address. Other examples such as downloading a large quantity of on-line journals at the same time could result in the same access blockage problem.

(g) Do not carelessly click on the link embedded in HTML formatted mails. Those links could direct the user to fraudulent sites, such as one-click fraud sites or fake websites where they would attempt phishing. Phishing is directing the users to enter a fake website whose appearance is almost identical to the legitimate one, attempting to steal one's authentication information such as ID or passwords. It is typically carried out from links in HTML formatted mails.

7.3 Sending information to the website (entering information on forms, uploading files, etc.)

(a) In sending important information, always use a secure communication protocol such as SSL/TLS. Also check to make sure of the certificate's authenticity.

(b) In browsing websites, enter the URL directly. Using a relay site when entering data could lead to the danger of data rip-off or cross-site scripting. Cross-site scripting is a type of attack targeting the viewers of the website where the authenticity certification is relatively low. After going through a malicious site, when the user enters sensitive data, it would allow code injection called script into the data. The injected script would be sent back to the browser together with the user's input data on the server where the data is not checked. The script will never be shown on the browser screen, but on the browser where script performing is not limited, it will be carried out and important information could be stolen. (Description from the IPA security center: http://www.ipa.go.jp/security/awareness/vendor/programmingv1/a01_02.html)

7.4 Malicious programs

When the computer terminal is infected by a malicious program by downloading and opening a file or an infection is suspected, the computer user must remove the terminal from the network by removing the LAN cables. Afterwards, the user must contact, report and follow the instructions of the technical personnel of the department.