The University of Electro-Communications
Campus Network Use Policy (for Students)

UEC Network Operation Committee

March 30, 2004

Before using the UEC campus network, sufficient care must be taken in order to comply with two policies, the Acceptable Use Policy (AUP), and the Acceptable Security Policy (ASP).

As stated in the preamble of the Basic Policy for Administration and Use of the UEC campus network, these policies have been established in order to ensure proper administration and use of the network by our users and administrators. This is our responsibility in an information network society, as a university that promotes education and research in advanced communication sciences.

Here is the text from these two policies along with specific examples and notes. If a user violates these policies, or if the UEC Network Operation Committee or the Network Operation Committee of a particular department deems it necessary, that person's use of the internal university network and computers may be terminated without warning, and any information belonging to the user may be altered or erased.

1 UEC Network Operation Standards (P1) Acceptable Use Policy (AUP)

1.1 Protecting basic human rights

The network contents and activities on the UEC campus network must not violate the basic human rights written in The Constitution of Japan. The UEC Campus network cannot be used to carry out actions that infringe on the human rights of others, including violating privacy, making personal attacks, or discriminating based on race, gender, belief, or religion. Specifically the following types of actions are prohibited: violent speech such as discriminatory remarks and slander, promotion of actual violence or crime, promotion of sexual abuse, sex crimes, or child abuse, and intercepting communications or publicizing intercepted communications.

Specific Prohibited Actions:

- Making statements that slander or defame an individual or group in a way that makes the target of the statements identifiable, through the use of a electronic bulletin board, news group, or mailing list.
- Making statements that instigate or promote violent or criminal behavior, through the use of an electronic bulletin board, news group, or mailing list.
- Making statements that instigate or promote sex crimes or criminal behavior, or posting images that contravene the Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children (Child Pornography Prevention Law), through the use of an electronic bulletin board, news group, or mailing list.
- Making statements that slander or defame an individual or group, through the use of email or chat sites.
- Sending images that contravene the Child Pornography Prevention Law, or making comments that contravene the Youth Protection and Upbringing Regulations, towards persons that are subject to protection under the same laws, through the use of email or chat sites.

1.2 No commercial use

The UEC campus network is for scientific research and educational purposes, and SINET's Acceptable Use Policy (AUP) also restricts use to scientific research purposes only. Therefore, any commercial use of the network is prohibited.

Specific Prohibited Actions:

- Participating in a network auction using a university email address.
- Participating in personal buying and selling using a university email address.
- Carrying out commercial activities using a university email address or a server located on the campus.

1.3 Protecting intellectual property rights

Copyrights, design rights, trademarks, and other intellectual property rights must be respected and protected. The copying and distribution of all or part of a copyrighted material without the permission of the author is prohibited. Furthermore, in light of the public nature of the university, the use of software that may infringe upon copyrights is also banned.

Specific Prohibited Actions:

- Using the UEC campus network to send or receive copyrighted material that has been distributed without the permission of the copyright holder (video files, music files, electronic publications, commercial software, or scanned images of printed material).
- Downloading materials from illegal Websites or ftp sites. The possibility of copyright infringement should be carefully examined before downloading files.
- Using software for sharing or exchanging files over the UEC campus network for purposes other than research. Be careful on this point, as some recent file sharing / exchanging software does not always appear to be this kind of software on the surface.

1.4 No infringement of personal information or security

The privacy of all computers at the university, and at organizations outside the university that can be accessed from the university, as well as the privacy of applicable users must be protected. Any infringement of information security such as cyber attacks or communications interceptions are prohibited. For more information refer to the (P2) UEC Acceptable Security Policy (ASP).

Specific Prohibited Actions:

- Launching a cyber attack on a computer or network device connected to the network, whether it is inside or outside the university. A cyber attack includes posting information on an electronic bulletin board that violates the usage policy, or using it in a way that violates the policy.
- Carrying out a cyber attack on an individual computer, file, or folder directory, and looking for personal information. Also disrupting an individual's use of a computer in the same way.
- Using a computer assigned to someone else without the authorized user's permission.
- Publicizing personal information without the individual's permission that is learned during computer or network administration
- Sharing your account and password with others, or temporarily lending them out.
- Selling or disclosing a university email address to someone without the permission of the user.
- Entering a university email address into a questionnaire that may be used for sending out unsolicited spam email.

1.5 Ensuring public benefit

As a public institution, the university is obligated to engage in activities for the public benefit. Excessive personal use of the UEC campus network and computers is not allowed. Unnecessary anonymous sending of information from the UEC campus network must not be carried out. Members of the university are responsible for the content of the information that they send.

Specific Prohibited Actions:

- Playing network games over the UEC campus network. When necessary for research purposes, permission must be obtained.
- Sending information over the UEC campus network that is unsuitable for an education and research institution, such as images and text that are obscene or that make others uncomfortable.
- Using pay-for-content services that are not consistent with educational or research purposes
- Using services that are unsuitable for an educational and research institution such as dating sites.
- Sending or receiving music files, video files, or commercial software (not trial versions but products that have been copied from a CD-ROM, or parts of such products) for personal use. Any personal use that is considered to be excessive.
- Sending information (posting to an electronic bulletin board or mailing list) through a open proxy server outside the university, but making it appear that the information was sent from outside the UEC campus network. Users must take responsibility for the information that they send.

Notes:

The university is a SINET node institution, and is connected to SINET at 1Gbps. This does not mean that we can use the entire bandwidth of 1Gbps, rather we share it with 20 or more other research institutions. We can only use slightly more bandwidth than the others. If the university uses too much of the network bandwidth, the bandwidth available to other research institutions decreases. Therefore, excessive personal use is strictly prohibited.

1.6 Protecting the information network and information security

Information networks provide an indispensable infrastructure for every kind of activity from industry to daily life. Any action that prevents the smooth operation of the information network inside and outside the university is prohibited. Moreover, the information network is not a safe place. Users must be careful to protect the security of their personal information. The security of personal information and information on computers is the responsibility of every user. For more information refer to the (P2) UEC Acceptable Security Policy (ASP).

1.7 Obligation to educate

The people that use or administer the UEC campus network and computers must learn about the technologies, as well as their proper operation. The UEC Network Operation Committee is responsible for devising and implementing an education plan that takes into consideration all relevant laws and the current condition of the network society.

Specific Prohibited Actions:

- Using a university computer or the UEC campus network without first taking a computer literacy seminar
- Using the UEC wireless LAN access point without first taking a wireless LAN seminar
- Using the UEC campus network without first reading the information and guidelines from the Information Network Administration Committee
- Using the UEC campus network without first obtaining guidance from an instructor or a course / research-department faculty member

Notes:

We are planning to carry out regular seminars concerning the UEC campus network and computers. These will cover a wide range of topics from computer use to administrator training and computer security. Be sure to participate in these classes if you are asked to do so.

1.8 Complying with relevant regulations

In addition to the AUP requirements, all information network activities must be in compliance with the relevant laws and regulations.

Specific Prohibited Actions:

- Carrying out activities that contravene any law governing networks and computers

Notes:

The main laws that govern networks and computers include the following

- The criminal and civil codes (actions illegal in the real world are also prohibited online)
- Unauthorized Computer Access Law (regulations to prevent computer and network intrusions)
- Copyright Law (regulations for handling copyrights online)
- Child Pornography Prevention Law (ban on the distribution of child pornography over the Internet)
- Law concerning the Protection of Personal Information (regulations on the handling of personal information)

International treaties are also applicable:

- Berne Convention (international treaty on copyrights)
- WIPO Copyright Treaty (includes the Berne Convention)

Please also note that when using content on networks outside of Japan, the laws of the countries concerned also apply.

2 UEC Network Operation Standards (P2) Acceptable Security Policy (ASP)

2.1 Obligation to protect computers

All the computers connected to the UEC campus network must have measures to prevent various kinds of cyber attacks over the information network such as illegal intrusion, unauthorized access, and denial-of-service attacks. At the same time, it must be recognized that all computers have potential vulnerabilities, and necessary precautions must be taken.

Specific Prohibited Actions:

- Connecting to the university network using a computer with security holes, without first taking the necessary measures. This means for example:
  - Connecting a Windows machine that has not been updated using Microsoft Update or Windows Update.
  - Connecting a Windows machine that does not have anti-virus software installed, or one where the virus definitions have not been updated.
  - Using an OS for which a security warning has been issued, without taking the necessary measures

2.2 Obligation to prevent computer information leaks

Information must not be provided that might expose the vulnerability of the UEC campus network or any computer connected to it. Before providing any information from the UEC campus network or any computer connected to it, careful consideration must be given to its impact.

Specific Prohibited Actions:

- Sending incident or security information reported by the UEC Network Operation Committee to an electronic bulletin board or mailing list outside the university, or to someone not affiliated with the university.
- Distributing security information about university host or network computers learned while using the network. This kind of important information must be notified directly to the Network Operation Committee of the department concerned, and the instructions of the committee must be followed.

2.3 Obligation to manage services provided from computers

Any service run on a computer connected to the UEC campus network must be administered so that no opportunities are provided to expose weaknesses in the UEC campus network and its computers, thereby making them vulnerable to attack. At the same time, administration must be carried out so that a service running on the UEC campus network is not used for information theft or an attack on a network outside the university.

Specific Prohibited Actions:

- Failing to take measures against intrusion or attack from the network, whether inside or outside the university. Recently any Windows machine set to default has become very susceptible to attack.
- Posting information on weaknesses such as security holes in network services at the university or other organizations, including Web content for purposes other than research

2.4 Obligation to protect personal information

Everyone using the UEC campus network must always be aware of the need to protect personal information. Remember that you must properly manage your own personal information when it is transmitted over any information network, whether inside or outside the university. Those administering the university network and the computers connected to it must take measures to protect the personal information of users as much as possible. Furthermore, the administrators may not leak any user's personal information they have learned during the course of their work.

Specific Prohibited Actions:

- Entering personal information (name, address, age, telephone number, email address, etc.) into questionnaires without proper consideration. Remember that it is your own responsibility to protect your own personal information.
- Disclosing or selling the personal information of others found while using or administering the university network or a computer connected to it.

2.5 Obligation to report

In the event that a weakness or personal information leak is discovered in the UEC campus network, or if there appears to be an infringement of the UEC campus network or the information security of a user, the person uncovering the problem must report it immediately to the Information Network Committee in the department or office concerned, or to the UEC Network Operation Committee. The department or office committee receiving such a report must then immediately notify the UEC Network Operation Committee.

Specific Prohibited Actions:

- Not reporting a weakness that is discovered in the UEC campus network or a university computer to the systems administrator or the relevant Information Network Operation Committee.
- Not reporting a virus infection, cyber attack or intrusion, to the systems administrator or the relevant Network Operation Committee.
- Not reporting any behavior that violates this policy to the systems administrator or the relevant Network Operation Committee.

2.6 Obligation to take counter measures

The UEC Network Operation Committee must take immediate measures to counter any infringement of information security including personal information leaks, or security incidents on the UEC campus network, in order to minimize the damage. The UEC Network Operation Committee must analyze the information security infringement, devise a plan for inspection and counter measure implementation, before issuing instructions. Administrators of the university information network and computers connected to the network must carry out the inspection and necessary measures as instructed by the committee.

Specific Prohibited Actions:

- Continuing to use a computer even though it has been infected with a virus or compromised by an intrusion, or is suffering from some other specific damage.
- Continuing to use a vulnerable computer despite an instruction or report from the systems administrator, the relevant Network Operation Committee, or the UEC Network Operation Committee.

2.7 Obligation to educate

The administrators and users of the UEC campus network and its computers need to learn about information security and how to protect personal information. The UEC Network Operation Committee is responsible for devising and implementing an education plan that takes into consideration all relevant laws and the current condition of the network