National Chengchi University Network Usage Regulations

Approved at the 47th meeting of the Computer Promotion Committee on May 7, 2001
Amended and approved at the 51st meeting of the Computer Promotion Committee on May 30, 2002
Amended and approved at the 53rd meeting of the Computer Promotion Committee on February 20, 2003
Amended and approved at the 75th meeting of the Computer Promotion Committee on March 17, 2010

I. The campus network of National Chengchi University (hereinafter referred to as the University) has been established to assist the faculty, staff, and students of the University in teaching, academic research, administrative affairs, and other related activities.

II. All IP addresses of the University and information equipment on campus are considered part of the University's campus network. The information equipment referred to in the previous paragraph includes mainframe computers, personal computers, mobile internet devices, and network equipment.

III. Individuals or organizations using the above equipment are users of the University's campus network.

IV. All activities on the campus network should comply with these Regulations, the *Taiwan Academic Network Management and Norms*, and the *Convention on the Management and Use of Bulletin Board Systems* established by the Ministry of Education.

V. Users of the campus network should be aware at all times not to disrupt the lives of others or violate their rights when using the information equipment.

VI. Users of the campus network are prohibited from the following activities:

1. Transmitting information that infringes intellectual property rights on the Internet or violates relevant laws and regulations.
2. Spying on, stealing, altering, interfering with, or destroying other people's information in any way.
3. Deliberately spreading computer viruses or other unauthorized information.
4. Intruding into computer systems without authorization.
5. Lending personal usernames and passwords to others.
6. Stealing or fraudulently using other people's identity to apply for personal usernames or IP addresses.

7. Deliberately damaging or improperly using information equipment (including computer mainframes, personal computers, or network equipment).
8. Using the campus network to distribute advertising or sell prohibited items or illegal software or data.
9. Engaging in any unauthorized business activities.
10. Spreading false information or defaming others.
11. Endangering or compromising system security or the security of network communication.
12. Violating any other government or University laws and regulations.

VII. Users of the campus network who violate these Regulations or are suspected of infringing upon the rights of others may be restricted or temporarily disconnected from the network. Those whose actions are unlawful will not only be reported to the relevant units of the University for disciplinary action, but shall also be held legally responsible.

VIII. Those who have violated these Regulations and disagree with the University's disciplinary action may file a grievance or seek redress under the University's Student Appeal Handling Guidelines, the Guidelines Governing Organization and Review of Faculty Appeals Committee, or the Regulations on the Establishment of the Staff Appeals Committee.

IX. If a unit or individual determines that misconduct has occurred while using information equipment on campus, they may present evidence to the Computer Center. After the Computer Center has confirmed that misconduct has indeed occurred and has identified its source, it may restrict or temporarily suspend the offender's network connection or notify the information equipment administrator to resolve the situation. In serious cases, offenders may be reported to the relevant units of the University.

X. Should an off-campus unit need to investigate a crime, it should notify the Secretariat in advance. Upon receiving notification from the Secretariat, each unit shall provide relevant information in accordance with the *Guidelines Governing Taiwan Academic Network Units' Assistance in Preventing and Combating Cybercrime*, the *Computer Processed Data Protection Act*, and the *Public Service Act*.

XI. Users of the campus network shall be responsible for keeping their usernames and passwords secure.

XII. Campus network administrators shall respect the right to online privacy and shall not arbitrarily spy on the personal information of other network users or violate their privacy rights, except in the following circumstances:

1. When maintenance or examination of system security is necessary.
2. When there is a reasonable suspicion of a rule violation of the University, to obtain evidence or investigate wrongdoing.
3. When cooperating with the investigations of judicial authorities.
4. When other network management measures are required by law.

XIII. Public computer administrators shall be responsible for the following administrative tasks:

1. Safeguarding and maintaining the usernames and passwords of administrators.
2. Safeguarding and maintaining the usernames and passwords of public computer users.
3. Safeguarding and maintaining of users' personal data.
4. Maintaining public computer services.
5. Maintaining public computer security systems.
6. Maintaining access records of public computer users or system records within the retention period.
7. Maintaining backups of public computer systems and users' important data.
8. Suspending or appropriately punishing those who use system resources inappropriately after being informed of the relevant rules and regulations.
9. Cooperating with the University in dealing with disputes or investigating criminal offenses and providing relevant information.

XIV. Network equipment administrators shall be responsible for the following administrative tasks:

1. Maintaining and managing network and information equipment on campus.
2. Safeguarding and maintaining the usernames and passwords of network equipment administrators.
3. Suspending or appropriately punishing those who use network resources inappropriately after being informed of the relevant rules and regulations.

XV. The information equipment administrators of the University's may announce relevant rules and regulations through official letters, electronic bulletin boards, or by posting them in the links section of the University's official website.

XVI. These Regulations were approved by the Computer Promotion Committee and submitted to the President for approval prior to implementation. The same applies to amendments.