National Taiwan Normal University Guidelines for the Use and Management of the University Network

Passed during the 35th Administrative Meeting on May 14, 2008

Amended and passed during the 11th Administrative Meeting in the 2020 academic year on April 28, 2021

I. National Taiwan Normal University has formulated these guidelines in accordance with the "Ministry of Education School Network Usage Regulations" and "Taiwan Academic Network Management and Norms" to provide network users with a standard they can follow for the promotion of compliance with the law and for the effective management of the university's networks (including dormitory networks, hereinafter collectively referred to as the network) to support teaching, academic researches, and administrative application services.

II. Network users shall respect intellectual property rights and avoid the following conduct that might infringe upon intellectual property rights:

(I) Using unauthorized computer programs or software.
(II) Illegally downloading or copying works under the protection of copyright laws.
(III) Posting protected works on public websites without authorial permission.
(IV) Reproducing articles from online forums against stated prohibitions by the authors.
(V) Setting up websites that provide illegal downloads of protected works.
(VI) Using peer-to-peer (P2P) software to download or share unauthorized files.
(VII) Conducting other activities that might infringe upon intellectual property rights.

III. Network users may not:

(I) Spread computer viruses or other programs that may disrupt or corrupt systems.
(II) Intercept network packets, snoop on messages, or engage in other illegal activities.
(III) Use unauthorized network resources or leak the user names and passwords of others by means of cracking, stealing, or using others' user names and passwords without authorization.
(IV) Share accounts with others.
(V) Hide accounts or use fake accounts.
(VI) Snoop on others' emails or files.

(VII) Abuse network resources in any way, including sending large amounts of ads, chain letters, or spam via emails, or affect the normal operation of systems by sending large amounts of packets to occupy resources.

(VIII) Disseminate fraud, slander, insults, obscene or harassing messages, illegal software transactions, sale of drugs and alcoholic products or other illegal messages via email, online chatting, social networks, or other methods with similar functions.

(IX) Engage in other conduct that are inconsistent with the purpose of the university network, or engage in illegal conduct.

IV. Units that provide network services to the public such as electronic bulletin boards (BBS), websites, e-mail, FTP, and network drives shall comply with the following rules:

(I) Install anti-virus software, scan for viruses regularly, and keep virus definitions up to date.

(II) Periodically patch the vulnerabilities of operating systems and application programs.

(III) Set up firewalls and close communication ports that are not in use to avoid viruses and hackers.

(IV) Set up computer audit records, and check and back up the records regularly.

(V) The settings of user names and passwords must meet the requirements of security principles and must be updated regularly.

(VI) Mechanisms such as verification codes must be built for forums and message boards to prevent large amounts of illegal comments, and the contents of the comments should be moderated regularly.

V. The management responsibilities of units that provide Internet services are as follows:

(I) Appoint experts to manage and maintain the information and communication equipment under control.

(II) Build self-regulation mechanisms on computer and network usage for computer users.

(III) Appoint information security personnel to control information security and training in relevant educational training courses.

(IV) In the event of abnormal network activities, appropriate segregation and control on network traffic must be performed.

(V) Comply with the management mechanisms, handling procedures, and enforcement rules in these guidelines.

VI. The Internet services should respect and protect online privacy and must not view users' personal data or conduct any activity associated with the infringement of privacy. However, the following situations are not subject to the limits set in the preceding sentence:

(I) When maintenance or examination of system security is necessary.
(II) When seeking evidence or investigating misconduct related to putative violations of the University code of conduct, and there are reasonable grounds for such suspicions.
(III) When cooperating with the investigations of judicial departments.
(IV) Other conduct in compliance with the law.

VII. Network connections will be limited or temporarily disconnected if any conduct is proven to be in violation of these guidelines. In the event of serious offenses, the case may be sent to relevant departments of NTNU for punishment. The violator will be held legally responsible if the conduct involves illegal matters.

VIII. These Guidelines have been implemented after approval by an Administrative Meeting. The same shall apply to all subsequent amendments.