National Yang Ming Chiao Tung University Campus Network Use Regulations

Approved at the 5th Administrative Meeting of National Yang Ming Chiao Tung University, held on June 2, 2021.

1. To ensure the campus network can support teaching, research, administrative, and online learning activities, to promote respect for the rule of law, and to provide a basis for Internet users to follow, National Yang Ming Chiao Tung University (hereafter referred to as "the University") has established the Campus Network Use Regulations (hereinafter referred to as "the Regulations") in accordance with the "Campus Network Use Regulations" issued by the Ministry of Education.

2. Internet users must avoid the following behaviors, which may constitute the infringement of intellectual property rights:

   (1) Use of unauthorized computer programs.

   (2) Illegal downloading and copying of works protected under copyright law.

   (3) Uploading of protected works on a public website without the consent of the copyright owner.

   (4) Arbitrary reproduction of articles that have been expressly prohibited from being reproduced by the author on social media, bulletin boards (BBS), or an online discussion forum.

   (5) Establishment of website for the illegal downloading of protected works by the public.

   (6) Performance of other actions that may involve the infringement of intellectual property rights.

3. The abuse of the network is prohibited, and the network users are not allowed to engage in the following behaviors:

   (1) Spreading of computer viruses or other programs that interfere with or disrupt the functionality of the system.

   (2) Unauthorized interception of network transmission messages.

(3) Unauthorized use of network resources through hacking, stealing, or unlawfully accessing other users' accounts and passwords.

(4) Lending of your account to someone else for no reason, or disclosure of someone else's account and password for no reason.

(5) Hiding of accounts or use of fake accounts. This does not apply to anonymous users who have been given express authorization for such actions.

(6) Viewing of others' emails or related computer information.

(7) Misuse of network resources in any way, including the mass transmission of advertisements, chain letters, or useless information through e-mail, the flooding of mailboxes, and the plundering of resources, with the purpose of affecting the normal operation of the system.

(8) Dissemination of fraudulent, defamatory, insulting, obscene, disturbing, or illegal software transaction information or other illegal information through e-mail, online chat, BBS, or similar means.

(9) Engagement in nonteaching and non-research-related or illegal activities using campus network resources.

(10) Disclosure of official, confidential information.

4. To implement procedures described in these regulations, the division of labor and management of network-related matters are as follows:

(1) The University's perimeter network and backbone network connecting each unit are managed by the Information Technology Service Center (hereinafter referred to as "the Information Center").

(2) The internal network of each unit (including teaching, administrative, and non-establishment units) shall be managed by the unit. A management mechanism shall be established for the allocation and use of internal network addresses.

(3) Each unit shall assign network management personnel to provide network management services within the unit. The scope of the power and responsibilities of network management personnel is as follows:

1. The IP address of each unit must be applied for by the unit's network management personnel through completion of the "Information

Service Application Form." Applications for IP addresses must be submitted to the Information Center for review after the applying unit's network administrator has compiled all of the unit's completed application forms.

2. The network management personnel of each unit are responsible for the allocation and management of the issued IP addresses, and accurate user information such as the name, unit, location, contact number, and mailbox of the IP users must be logged. Updates of information must be provided in the case of any change.

3. If the network management personnel of a unit change, the "Network Management Personnel Change Notice" form must be completed to notify the Information Center to update network management personnel information. The form must also be given to the network management work unit to facilitate network maintenance.

4. For IP addresses with special purposes (e.g., for a server, NAT router, or experimental test host), an application must be submitted. The "IP Whitelist Application Form" must be completed, and the information must be logged accurately.

5. The responsibility for managing and promoting Internet use and related regulations must be fulfilled.

6. Personnel must attend the network management staff meeting held by the Information Center.

7. Personnel must participate in information security training and pass network management and information security inspections every academic year.

8. The "Information Security and Intellectual Property Rights Management Inspection Record Form" must be completed regularly.

(4) The Information Center has the right to redistribute the IP addresses of each unit according to the actual usage rate of each unit's IP addresses.

(5) To ensure the proper allocation of network resources, the management unit has the right to appropriately segregate and control network traffic.

(6) For users who consume a large amount of network resources for no reason or who exhibit abnormal network traffic that affects the normal operation of

the network, the management unit may activate traffic control measures or suspend the user's right to Internet use. The network connection shall only be restored after confirmation that the user's Internet usage behavior has normalized.

(7) All types of application servers (including electronic BBS and websites) shall be managed and maintained by dedicated personnel. The personnel in charge may suspend a user's right to use a website if the user violates the rules of website use.

(8) If users identify any defects or loopholes in system security, they should notify the management unit as soon as possible.

(9) To reduce security threats to the University's information system, traffic from the off-campus network (not an internal IP address of the University) shall be blocked, except for those services that are already open to the public. If other open services are required, an application must be submitted.

(10) Restricted internal administrative campus information systems are to be linked and accessed only from internal campus IP addresses or through the University's virtual private network.

(11) The use of P2P software is prohibited in principle on the campus network, but applications may be submitted if such software use is required for academic, teaching, and other special activities. However, if the use of P2P software affects the campus network service, such software shall be blocked.

(12) The Information Center shall provide a security checklist for use by all units on campus and shall conduct information security and intellectual property protection audits each semester with the cooperation of the respective network administrators.

5. Internet users must be aware of any suspected security threats to ensure the safety of Internet use. All information security incidents reported through the Ministry of Education Information and Communication Security Contingency platform and official correspondence shall be handled according to the following principles:

(1) If the IP address reported through the information security notification platform of the educational institution is verified, and if the violation is

minor, the IP address shall be blocked for 2 weeks; if the violation is more serious or a repeated violation, the IP address shall be blocked for 1 month, and a punishment in accordance with the University's reward and punishment regulations shall be administered.

(2) In the case where an official letter is sent by the prosecutor or police, the University does not have the authority to investigate the case. Hence, if the University perceives a need to investigate the case, it shall request the prosecutor or police officer to provide a search warrant to ensure the University's cooperation with the investigation.

6. Users who violate the network usage rules shall be disciplined according to the following conditions:

(1) For a user who presents an immediate threat or disruption to network use, the network connection of the user exhibiting abnormal activity shall be blocked immediately, and the network administrator or the supervisor of the unit to which the user is affiliated shall be notified. The user or the unit's network administrator must report the situation to the Information Center within 1 week of noticing or receiving notification of the problem. After confirming that the problem has been resolved, the Information Center administrator shall lift the network ban.

(2) For a user who does not present an immediate threat or disruption to network use, the user or the network administrator of the unit to which the user is affiliated shall be notified of any abnormal usage behavior. The network management personnel must complete the investigation, counseling, and improvement or the disposal of the notification report within 3 days after receiving the notification and report to the Information Center regarding the handling of the situation. If details of ongoing procures to rectify the situation are not sent to the Information Center within another 3 days, the Information Center may block the network connection of the user exhibiting abnormal activity.

7. Network administrators should respect personal privacy rights and may not arbitrarily view users' personal data or violate their right to privacy, except in one of the following situations in which device administrators or users must cooperate in providing necessary system permissions:

(1) For the maintenance or inspection of system security.

(2) To obtain evidence or investigate misconduct on the basis of reasonable

suspicion of a violation, as detailed in Article 2 and 3 of these Regulations (regarding respect for intellectual property rights and the prohibition of abuse or interference with network systems).

(3) For cooperation with the investigation of the judicial authorities, if an off-campus unit must investigate a crime, the chief secretary of the University should be notified in advance, and the relevant legal letter (credentials) should be presented. After receiving notification from the University Secretariat, each unit shall provide relevant information in accordance with the "Guidelines Governing the Cooperation of Taiwan Academic Network Connection Units to Prevent Cybercrime," "Personal Data Protection Act," and "*Civil* Servant Work Act."

(4) To obtain relevant information to facilitate timely prevention of and rectifying measures in the case of an emergency (e.g., major changes in life or property).

(5) To perform other actions in accordance with the laws of Taiwan.

8. Internet users who violate these regulations shall be subject to the following penalties:

(1) Temporary suspension of network resources (IP blocked for 1 week).

(2) In serious cases, the suspension of Internet resources shall be extended, and the student shall be punished in accordance with the University's regulations and related reward and penalty regulations.

(3) In the event that the user being penalized in accordance with the preceding two articles commits another law violation, the perpetrator shall be held legally responsible in accordance with Taiwan's civil laws, criminal laws, copyright laws, or other relevant laws and regulations.

9. These Regulations shall be implemented after their approval at the University's Administrative Meeting, and the same shall apply for any subsequent amendment.