

National Chi Nan University Campus Network Usage Regulations

Passed by the 3rd meeting of the Computer and Network Center Advisory Committee in the 89th academic year on
June 13, 2001

Passed by the 1st meeting of the Computer and Network Center Advisory Committee in the 99th academic year on
January 11, 2011

Promulgated and implemented by National Chi Nan University Letter No. (100) Chi-Xiao-Dian-Zi-1000001513 on
February 11, 2011

Passed by the 1st meeting of the Computer and Network Center Advisory Committee in the 100th academic year on
January 9, 2012

Promulgated and implemented by National Chi Nan University Letter No. (101) Chi-Xiao-Dian-Zi-1010001695 on
February 16, 2012

Articles 10, 19, and 20 amended and passed by the 1st meeting of the Computer and Network Center Advisory
Committee in the 103rd academic year on January 13, 2015

Amended and passed by the 2nd meeting of the Computer and Network Center Advisory Committee in the 111th
academic year on February 23, 2023

General Provisions

1: These regulations are established to support university administration, teaching, research, and development, and to regulate the fair and reasonable allocation and use of network resources, in accordance with the "National Chi Nan University (hereinafter referred to as 'the University') Computer and Network Center (hereinafter referred to as 'the Center') Establishment Regulations".

2: The use of the University network must comply with relevant national laws, Taiwan Academic Network regulations, University rules, Center regulations, and Internet conventions.

Network Line Usage Regulations

3: (Deleted)

4: (Deleted)

5: The total daily upload/download network traffic for each device must not exceed 10,737,418,240 bytes. Exceeding this limit will result in restricted upload/download connection bandwidth. The bandwidth restriction will be automatically lifted at 24:00 daily.

6: In case of network failure, please report it through the electronic service system on the Center's homepage.

7: Users should install anti-virus software on their computers and regularly update virus definitions and system patches. If a computer becomes infected and maliciously attacks other computers, upon report, the network connection will be immediately terminated. After resolving the infection, please apply to the Center through the electronic service system to restore the network connection.

8: According to Taiwan Academic Network management principles, students are not allowed to set up websites in dormitory areas. Therefore, only Private IP addresses are assigned to student dormitory areas and student activity centers.

Taiwan Academic Network Management Principles, Point 5 of Section 1: "To ensure the smooth flow of

academic information on the TANet backbone, please cooperate by segregating and controlling dormitory networks (e.g., using Private IP, NAT, etc.), and manage website setups in dormitory networks to comply with TANet's purpose."

9: All university computers must use the "Obtain IP address automatically" method. All related settings will be automatically configured by the DHCP Server. Users setting private IP addresses will have their network connection terminated for one month upon discovery. For special needs requiring fixed IP addresses, please submit an application form approved by the unit supervisor to the Center's Network Group.

10: To integrate resources, respond to energy conservation, and effectively manage IP addresses and server information security, setting up servers should prioritize applying for the Center's cloud servers. Public Static IP addresses are only issued for server equipment with dedicated management personnel and the Center's cloud servers. Remote access to Public Static IP addresses follows a "principle of prohibition, exception by permission" approach. Those needing exceptions should apply to the Center.

Protection of Network Privacy

11: Based on the Ministry of Education's requirements for the security and effective management of the University's campus network, all network-related services must retain usage records for at least six months. Each service should clearly stipulate the method and scope of collecting, processing, or using users' personal data when utilizing the service, and announce this electronically or in paper form, requiring users' consent before using related campus network services.

12: In accordance with the Personal Data Protection Act, providers of network-related services must properly protect and control users' personal data. Management personnel must not arbitrarily view users' personal data or engage in other privacy-infringing behaviors, except in the following circumstances and with approval from superior management:

- (1) To maintain system security or check system performance.
- (2) When there are reasonable grounds to suspect violations of university rules, to obtain evidence or investigate misconduct.
- (3) To cooperate with judicial authorities' investigations.
- (4) Other network management actions executed in accordance with laws and regulations.

Supplementary Provisions

19: The Center may evaluate and adjust the use and allocation of network resources at any time based on network bandwidth, equipment load, and network security conditions. If users are found violating relevant rules or misusing network resources, their usage rights may be suspended (3-21 days) or referred to relevant units for disciplinary action.

20: It is prohibited to use the University's network resources to interfere with or destroy other nodes' software or hardware systems, such as spreading computer viruses, attempting to access unauthorized computer systems, transmitting threatening, obscene, unfriendly, commercial (advertising) materials, or engaging in other illegal activities (e.g., violating intellectual property rights). Violators will have their usage rights suspended (3-21 days) and be referred to relevant units for disciplinary action.

21: The network resources provided by the University (including various software and hardware equipment, lines, and accounts) are limited to use by University faculty, staff, and students, and may not be lent to others. Violators will have their usage rights suspended or be referred to relevant units for disciplinary action.

22: These regulations shall be implemented after approval by the Center's Advisory Committee meeting.