# Asia University Campus Network Usage Regulation

2002.03.14 Established by the 1st Computer Center Temporary Committee Meeting
2002.10.06 Approved to amend by the 2nd Computer Center Committee Meeting
2005.04.28 Approved by the 6th Computer Center Committee Meeting
2005.06.22 Regulation renamed for Asia University by the 5th Administration Meeting of the 2004 Academic Year
2006.04.27 Approved to amend by the 1st OICT Advisory Committee
2009.04.23 Approved to amend by the 4th OICT Advisory Committee
2009.12.28 Approved to amend Articles 4, 6 and 23 by the 5th OICT Advisory Committee
2010.02.09 Issued by Asia Mi Tze No. 0990001086
2014.01.03 Approved to amend by the 1st OICT Advisory Committee of the 2013 Academic Year

Chapter 1 General Rules

1. The purpose of the campus network is to build a good environment for teaching and research. It can provide internal connections of computing devices as well as connecting to external academic networks via the Taiwan Academic Network (TANet) to achieve information exchange and resource sharing.
2. The backbone of the campus network is constructed by the Fast Ethernet and Gigabit Ethernet. Other units, departments and dormitories will be deployed by the local area network and then connected via the backbone to the Office of Information and Communication Technology (OICT).
3. The management of campus network is supervised by the OICT advisory Committee. Common network services for the whole school are maintained by the OICT. The networks inside the sections and departments are managed by the corresponding units themselves.
4. Using campus network has to follow the rules of TANet as follows.
   A. Follow the regulation of TANet:
      i. The regulation asks all the TANet users to follow their rules. Using TANet to transmit threating, sex-related and unfriendly information is prohibited.
      ii. Guiding users to use information, respecting information ethics, understanding internet etiquette and providing advices for all schools to form network management committee and corresponding rules.
   B. Follow the rules of intellectual property protection specified by TANet: Teach users the basics of intellectual property rights and how to use the network resources so that they have enough knowledge to avoid violation of the rules.
   C. Cooperate with the investigation of network crimes for all TANet connecting members: For the collections of evidence verification, all TANet connecting members have to provide related network information for investigation.

D. Follow the Taichung Network Regional Center (TCRC) management regulation: The campus network is connected to the TCRC. We have to follow the rules specified by the TCRC Committee Meeting.

5. The strategy for computer or network crimes:
   A. Declare the concept that violating the law and you have to pay for it. The computer crimes are included.
   B. Revise the school rules to include the punishments of the computer and network crimes.
   C. Deploying the network traffic monitoring system. Following the agreement of the TCRC Management Committee to set the traffic limit for each IP.
   D. The network traffic for each connecting units is shown on the web site.
   E. The network administrator has to investigate on site the IP with the abnormal traffic to avoid inappropriate network usage. For the IP with abnormal network traffic in the dormitory, it will be applied with the corresponding rules.
6. The following network management will be emphasized:
   A. Form a team for the intellectual property protection to take over the following tasks:
      i. Specifying the school rules for the violation of intellectual property rights.
      ii. Planning the explanation the related rules of intellectual property rights
      iii. Inspecting the usage of legal software on campus
      iv. Regulating the usage of campus network and notifying the applicants
   B. Enforce the management of dormitory network:
      i. Dormitory network is included in the management of campus network. The record of the student who lives in the dormitory is paired with the network interface card. Once the network abuse is found, the client will be informed immediately and advised to obey the rules.
      ii. Improving the management devices of dormitory network to become an automatic and real-time management system.
      iii. The abnormal traffic user will be handled by rules of the network management right away.
   C. Enforce public computers and network management:
      i. Public computers will be checked if they are abused or violating the intellectual property rights periodically.
      ii. The network administrators will watch carefully if there is an abnormal traffic on campus to find out deployment of illegal web sites.
   D. When there is a formal notification of violating intellectual property rights, the standard operation procedure OICT takes is as follows:
      i. Whenever a network violation is found or informed, the network of the suspected computer will be suspended.
      ii. The applicant and the corresponding department head of the IP address for the

suspected violating computer will be informed by email and Information Security Event Report. The owner will be notified the consequence of the violation and asked to stop the action.

iii. The accused section has to investigate the case and fill out the Information Security Event Report to OICT in three days. If he miss the deadline, OICT will reply to the prosecutor that the case is true and report to OICT Information Security Committee.

iv. When OICT receives the report, the following actions will be taken:
    1. For first offender: Starting from the date of received Information Security Event Report, the IP will be suspended for two weeks.
    2. For repeat offender: Starting from the date of received Information Security Event Report, the IP will be suspended for two months.

v. OICT collects the materials of the suspected intellectual property rights violation.

vi. Submit to the Intellectual Property Rights Protection and Execution Team for discussion.

vii. Transfer the responder to the corresponding department for punishment:
    1. Students will be forwarded to the Office of Student Affairs.
    2. Faculty and employees will be forwarded to the Personnel Office.

viii. If the suspected violation case is in the judicial procedure, the process can be suspended.

7. If the situation is not included in the guidelines, please consult the regulation of Ministry of Education.

## Chapter 2 IP Distribution and Usage

8. The distribution of physical IP will be adjusted by OICT depending on the available IP numbers and their needs.
9. The usage and distribution of physical IP is managed and monitored by the OICT.
10. Each section should have a person responsible for the IP verification and management. He is also the window to contact with OICT for update in case there is a change.
11. The responsible person in each section should construct an IP assignment table for management. He is responsible for any network abuse and violation.
12. The person who uses an IP not assigned to him intentionally or affects the operation of network in any way will be suspended for the network usage and be punished by the guidelines.
13. A lot of computers in the dormitories, classrooms and laboratories will be assigned for private IPs. Each section should submit its requirements while planning. The OICT will provide physical circuits for the IP planning.
14. The unassigned service ports of an IP will be open for uses. The user is responsible for the network security of his computer.
15. The IP user is responsible for his machine running smoothly. It there is a network issue triggered by

the device, the OICT has the right to stop the network service of that device to keep the campus network running.

16. It is prohibited to install servers or devices and affects the operation of network.
17. The OICT can remove IP usage to avoid the possible information security events if the IP user has the following changes:
    A. The student is at the end of academic year, requests suspension of study or graduation.
    B. During the suspension of network usage because of fatal information security events.
    C. Resignation or position change for faculty.
    D. Equipment deprecation for the administration section.

## Chapter 3 Dormitory Network Usage

18. Dormitory network is part of campus network and the specifications are referred to those of campus network.
19. To use the network in the dormitory, the user has to prepare his own computer, network interface card (RJ-45 interface) and UTP cable. The installation information can consult the Dormitory Network Setup documentation.
20. According to the guidelines of TANet, The dormitory network should be monitored and separated from main traffic. If network abuse is detected, The OICT has to deal with it immediately to keep the operation of network. We may cut off the line if needed.
21. The maintenance of dormitory network is arranged by the order of the Maintenance Reporting System:
    A. The OICT is responsible for the maintenance range starting from the end point of network node to the campus network equipment.
    B. The scheduled maintenance will be posted on the web site three days before the effective date.
    C. It will be posted on the web site in four hours for unexpected situation or emergent maintenance.
    D. The specifications for the management of dormitory network usage will be regulated by the actual network.
22. The OICT is responsible for the management and operation of dormitory network.
23. The OICT should post its management and action plans on the web site according to the real-time network operation following the guidelines.

## Chapter 4 Wireless Networks

24. The wireless network environment is constructed for the faculty, employees, and students to easily access to the network.

25. Wireless network is part of campus network and the specifications are referred to those of campus network.
26. Wireless network is deployed and managed by the OICT. All users can apply the services following the guidelines.
27. Wireless network works in open spaces. For the sake of network security, the OICT can adjust the service range of wireless network. The user is responsible for the risk of the information security while using the service.
28. The user has to prepare his own wireless network card to connect to the wireless network devices.
29. If a section constructs its own wireless network, it is his responsibility for the management and security verification of network usage.

## Chapter 5 Information Security Specifications

30. The person who is involved in the institutional operation should perform information security management operation according to the Asia University Information Security management Regulation for Personnel.
31. The network user has to set up his own password for computer and take good care of all user accounts and passwords. The password should be changed periodically.
32. The selection of password should not be too simple or the same as the account number to ensure the security.
33. The network user is not allowed to illegally obtain other's account or related information by any means.
34. The user has to secure his own information. Update operating system vulnerabilities and virus patterns of antivirus software, backup data periodically.
35. The system administrator cannot release user's information and connection record without authorization.
36. The user who has been registered in the network management system can inquire his own connection record through the system.
37. Personal connection record should keep in the system for at least three months. The record content contains source address, destination address, connecting time and data length. The data content of each connection is not recorded or inquired.
38. For insider to obtain the connection record in the network management system, one has to submit a draft and approved by the president.
39. For outsider to obtain the connection record in the network management system, the prosecutor has to request in formal mail, by the Cyber Crimes Protection Guidelines for TANet Connection Units.
40. The connection record obtained the network management system through legal procedure is only for reference. The OICT does not provide assist of data analysis and explanation.

41. The information security event is handled according to the Information Security Event Notification Guidelines.

## Chapter 6 Network Management Implementing Regulations

42. According to the Chapter 1, the Network Management Implementing Regulations is established and used to manage the network users via related systems and equipment.
43. The network administrator should use systems and equipment to manage the network in real time to ensure the operation. This will provide faculty, employees and students high-quality network environment for administration, teaching and research.
44. There should be a restriction on some specific service ports of network to ensure the network services are not affected, through the traffic of network analysis.
45. All users have to obey the network usage guidelines. The network administrator can suspend the network usage to ensure the whole network working if the following situations occurred:
    A. Over the network traffic limit
    B. It affects the network usage because of the real-time traffic overflow or network resources occupied.

## Chapter 7 Deployment, Change and Temporary Use of Network Physical Circuits

46. For the request of network deployment or physical circuit change, a draft will be submitted, assessed by the OICT and approved by the supervisor. The initiator can start the purchasing and deployment process following the Asia University Procurement Practice.
47. To add or change the network circuits for computer classrooms, laboratories and research rooms, after the assessment of the OICT, the initiator has to find budget to purchase and deploy following the Asia University Procurement Practice.
48. For the request of temporary network, a request form has to be submitted a week before the deployment. The OICT assesses the available items and assist the deployment.

## Chapter 8 Maintenance

49. The OICT is responsible for the maintenance of network to ensure the network operation for administration, teaching and research.
50. The OICT will be informed and sent people to fix the network problems.
51. The scope of network maintenance is limited to adjust network configuration and physical circuits repair, according to the Information Equipment Management Guidelines.
52. The user has to pay for it if the malfunction is due to the misuse of network devices or nodes. If the condition is serious or someone did it intentionally, a report will be filed to ask for the penalty

## Chapter 9 Reward and Penalty

53. According to the TANet Management Guidelines, it will be rewarded if someone help to keep the network in operation, assist to avoid or resolve the danger of network security. This will be issued by the OICT and approved by the president.
54. The network administrator can shut down network node connection or suspend IP for two months and notify his supervisor if the user meets the following situations:
    A. Use an IP that is not applied by him.
    B. The campus network operation is affected because of the improper management of information devices.
    C. Scan other’s computers on the network or fire network attacks.
    D. Use big bandwidth which is not for academic or research purposes and ignore the warning.
    E. Use the network for business without authorization.
    F. Send spam emails using the campus network system.
    G. Violate the Intellectual property rights and related regulations.
    H. Spread information involved personal attacks, abuses or fake message on the network in any ways.
    I. Violate the information security regulations in Chapter 5.
55. If the network usage of user is reported or verified to be crimes, he bears legal liability. The OICT will provide related records for investigation.
56. This regulation is approved by the OICT advisory Committee, issued by the president. For the amendment, the process is same.