Regulations for the Management of Campus Computers and Network Resources at Chung Yuan Christian University

Approved in the 854th Administrative Meeting on August 7th, 1997
Revised according to the Letter No. 1050002657 from the Office of the President on August 25th, 2016

Article 1. Chung Yuan Christian University (hereinafter referred to as "the University") establishes the "Regulations for the Management of Campus Computers and Network Resources at Chung Yuan Christian University" (hereinafter referred to as "these Regulations") to effectively manage campus network resources in accordancewith the University's information security management regulations, intellectual property rights, and relevant laws and regulations. These regulations aim to enhance the quality of network services.

Article 2. These regulations apply to all departments and units of the University and cover aspects such as campus server management, network management, and the management of official computer software copyrights.

Article 3. Management of Campus Servers

1. Server Installation Application Guidelines:
   (1) Fill out the "Application Form for Campus Server Installation/Modification" and submit it directly to the Electronic Computer Center (hereinafter referred to as the Computing Center) of our university. Server installation is only allowed after the application has been reviewed and approved.
   (2) Once the server installation has been approved, it should be used to provide services according to the stated purpose of the application and must not be used for other purposes. Each unit is responsible for maintaining the legality of public information on the server and should not post information that is obscene, offensive, or violates intellectual property rights and personal data protection laws.
   (3) Unauthorized server installation is strictly prohibited.
2. The management responsibilities that the applying units should fulfill are as follows:
   (1) Unit Supervisor: Assumes the responsibility of supervising server network services within the unit. Designates one administrator who is responsible for server management and related information security operations within the unit. Assigns a responsible person for each server who is in charge of managing the content of that server.
   (2) Administrator: Serves as the point of contact for all server management and informationsecurity-related operations within the unit. Consolidates the "Campus Server Information Security Checklist of Chung Yuan University" for reporting to the Computing Center.
   (3) Server Responsible Person:
      i. Should conduct server inspections every semester based on the "Campus Server Information Security Checklist of Chung Yuan University". The

administrator compiles the inspection forms of the unit and submits them to the Computing Center for record.

ii. Must implement information security management and should not open unnecessary network services (ports) without authorization.

iii. When there are changes in the server responsible person, the "Application Form for Campus Server Installation/Modification" should be filled out to update the application data.

3. In the event of a server intrusion in the applying unit, the steps for repairing compromised Unix and Windows operating systems, as published by the Technical Service Center of the National Information and Communication Security Taskforce, should be followed.
4. Administrators and server responsible persons are required to attend relevant information security seminars organized by the Computing Center for a minimum of 4 hours each year.
5. Applying units should fulfill their responsibilities in server management. If inadequate management poses a threat to the campus network information security, the Computing Center reserves the right to suspend the network connection of the respective server based on the severity of the situation.

Article 4. Network management shall be carried out in accordance with the "Chung Yuan University Network Usage Regulations."

Article 5. Management of software copyrights for government computers:

1. Government computers should have legally licensed software installed and should not have any illegal software or P2P sharing software installed.
2. Legally licensed software required for official purposes should be procured and installed
   following the application/purchasing procedures of the university.
3. Borrowing of licensed software campus-wide shall be conducted in accordance with the "Related Resource Borrowing Management Procedures" of the Computing Center.
4. Government computers at all levels of the university should undergo an annual software copyright verification. The verification results should be submitted to the Computing Center for record. The Computing Center should conduct periodic software audits and if any unauthorized software is discovered, it should be forcibly removed, and the unit supervisor should be notified for appropriate actions.

Article 6. These regulations shall be approved by the administrative meeting and submitted to the president for officialannouncement. Any amendments shall follow the same process.