National Taiwan Normal University Guidelines for the Management of Campus Servers

Passed in the 35th Administrative Meeting on May 14, 2008
Amendment approved by the Information Security and Personal Data Protection Committee in the 1st meeting of the 2022 academic year on June 28, 2023
Amendment approved by the Information Security and Personal Data Protection Committee in the 1st meeting of the 2024 academic year on Dec 30, 2024

A. General Provisions

I. These Guidelines were established in accordance with the Cyber Security Management Act to improve the information security management of the University's servers.

II. The servers referred to in these Guidelines are servers that provide external services, such as websites, e-mail and webmail, FTP, and NAS.

III. The management of servers of the University's units must comply with the "Cyber Security Management Act," "Ministry of Education School Network Usage Regulations," "Taiwan Academic Network Management and Norms," and "National Taiwan Normal University Guideline for Use and Management of University Network," and reference the University's Information Security Management System (ISMS) and information security-related regulations.

B. Personnel

IV. Dedicated personnel must be appointed to be responsible for server maintenance and management, and cooperate with the University's guidance for related information security operations. Server administrators must attend information security workshops every year.

C. Placement

V. The servers of each unit must be located on campus, and should prioritize cloud virtual hosts. The application method is detailed in the "National Taiwan Normal University Information Technology Center Regulations for the Management and Fee Collection of Virtual Hosting Service. "If units need to purchase their own hardware equipment due to special circumstances, the principle is to apply for centralized server management services. The application method is detailed in the "National Taiwan Normal University Information Technology Center Service Guidelines for the Management of Servers."

D. Server management

VI. The servers of each unit should be under centralized management. Those requiring external access have to submit an application to the Information Technology Center. Servers without approval will be restricted from external connections. Additionally, remote maintenance from off-campus must be conducted via VPN.

VII. If the server of a unit is suspected of being hacked, has abnormal network traffic, sends spam emails, or has significant security vulnerabilities, the server's network access rights may be suspended if the situation is verified to be true.

E. Audit

VIII. Specifications of the "Server Information Security Control Measures Checklist" must be implemented in the management of servers in each unit. The Information Security and Personal Data Protection Group conducts an information security audit of the unit's servers every year. Each unit must complete improvements within the deadline for deficiencies found in audits, and submit them to the Information Security and Personal Data Protection Group for reference.

F. Establishment and amendment

IX. These guidelines shall be implemented after being approved by the Information Security and Personal Data Protection Committee. The same applies to all subsequent amendments.