NATIONAL TAIWAN UNIVERSITY
Computer and Information Networking Center
Network Service Account Management Regulations

December 11, 2003	Passed by the Administrative Meeting of the Computer and Information Networking Center
June 19, 2008	Passed by the Administrative Meeting of the Computer and Information Networking Center
August 19, 2009	Passed by the Administrative Meeting of the Computer and Information Networking Center
December 09, 2009	Passed by the Administrative Meeting of the Computer and Information Networking Center
October 19, 2011	Passed by the Administrative Meeting of the Computer and Information Networking Center
April 13, 2016	Passed by the Administrative Meeting of the Computer and Information Networking Center
November 19, 2020	Passed by the Administrative Meeting of the Computer and Information Networking Center

Article 1 The National Taiwan University (NTU or "the University") Computer and Information Networking Center ("the Center") formulates the *Network Service Accounts Management Regulations* ("the Regulations") to provide a central authentication and single sign-on system for the various network services on campus.

Article 2 Account services shall be made available to NTU faculty, staff, students, and alumni, as well as personnel related to the University's operations.

Article 3 All account usage shall comply with the University's *Campus Network Usage Regulations*, the Ministry of Education's *Taiwan Academic Network Management and Norms*, and other laws and regulations of Taiwan.

Article 4 A list of detailed network services and privileges that can be accessed from each account is available on the Center's website.

Article 5 Applying for and modifying accounts

1. Student accounts shall be created automatically upon admission. Usernames shall be the same as student ID numbers.
2. Applications for faculty and NTU Hospital staff accounts shall be submitted online.
3. Except for a name change reflected on the national ID card, no new applications may be submitted within one year of account creation or a previous name change.
4. The following documents must be submitted to apply:
   1) University service documents
   2) An application form signed personally by the applicant
   3) Personnel who are not controlled by the Personnel Office or Office of Research and Development shall additionally submit a certificate (with clear indication of the date of expiry) issued by the inviting or hiring unit.

The above documents shall be submitted to the Center for review and passage before an application may be processed.

Article 6 Validity period

1. If a student takes a leave of absence, their account shall be retained. If a student is dismissed/expelled from the University, their account shall be deactivated. When a student graduates, their account shall be automatically converted to an alumni account. The determination of student status shall be based on the records maintained by the Office of Academic Affairs.
2. A faculty and staff account shall be deactivated upon termination of the user's employment at the University, except in the case of retirement, where their accounts may be retained for life. The determination of employment status shall be based on the records maintained by either the Personnel Office or the Office of Research and Development.
3. The validity period of accounts of personnel who are not controlled by the Personnel Office or Office of Research and Development shall be based on the validity period approved by the Center.

Article 7 Based on the principle of fairness, each person/ID or unit may only apply for one account.

Article 8 The following documents must be submitted in order to request services involving personal data such as account inquiries, password resets, and account modifications and deletions:

1. Personal identification documents
2. University service documents

The above documents must be submitted to the Center for review and passage before an application may be processed.

Article 9 Account usage

1. Users are prohibited from lending their accounts to others, borrowing accounts, or hacking into others' accounts.
2. For-profit commercial activities are prohibited.
3. The transmission, storage, or dissemination of viruses, illegal software, spam emails, or fraudulent, pornographic, defamatory, obscene, harassing, or threatening contents is prohibited.
4. Sending anonymous or forged letters in the name of others is prohibited.
5. To respect the intellectual property rights of others, the use, storage, or transmission of pirated software is prohibited.
6. Moving, modifying, or viewing files or directories belonging to others is prohibited without permission.
7. Any attempt to damage the system, interfere with system operation, intercept network transmission packets, or act in a manner that impacts system security or interferes with the system is prohibited.

Article 10 Information security control

1. Passwords shall be updated regularly in accordance with the Center's policy. The password length, strength, and update frequency shall be set by the Center separately.
2. To strengthen identity authentication, users shall provide additional information such as a mobile phone number or backup email address as auxiliary authentication mechanisms.
3. The Center may require users to regularly update personal information and sign a usage consent form, and the Center may deactivate an account if the user fails to complete the process by the specified deadline.
4. The Center may delete deactivated accounts that are not restored within a certain time frame.

Article 11 Destruction of hard copies of personal data

1. In order to protect personal data and comply with audit requirements, hard copies of the application forms will be retained by the Center in accordance with relevant regulations following account creation.
2. The retention period shall be subject to the applicable Center regulations, such as ISO standard operating procedures. The Center shall regularly destroy expired hard copies of personal data.

Article 12 The Center may immediately deactivate an account if the user violates any applicable regulations, and, depending on the seriousness of the violation, the Center may refer the user to the University for handling.

Article 13 The Regulations shall be passed by the Center's Administrative Meeting and then implemented.