

# Taipei Medical University Guidelines for Email Account Management

First drafted and approved at the Information Technology Meeting on December 17th, 2021  
Amendment approved at the Information Technology Meeting on December 15th, 2022  
Amendment approved at the Information Technology Meeting on June 26th, 2024

- Article 1 To effectively manage the email accounts and storage spaces issued by the university, and to safeguard user rights and information security, the *Taipei Medical University Guidelines for Email Account Management* (hereinafter referred to as the "Guidelines") are established.
- Article 2 The managing unit of the email accounts is the Office of Information Technology (hereinafter referred to as the "Office").
- Article 3 The eligible applicants for the email accounts are listed as follows:
1. Tenure-track faculty and staff formally appointed by the university (hereinafter referred to as "Faculty and Staff").
  2. Tenure-track assistants and postdoc researchers qualified by the university.
  3. Students officially enrolled in the university's degree programs.
  4. Graduates of the university's degree programs (hereinafter referred to as "Alumni").
  5. Part-time teachers at the university.
  6. Other personnel approved through special authorization.
- Article 4 The storage capacity for each email account shall adhere to the following categories based on user eligibility:
1. Category A - 100GB storage: Tenure-track faculty.
  2. Category B - 50GB: Tenure-track staff.
  3. Category C - 30GB: Tenure-track assistants and postdoc researchers.
  4. Category D - 20GB: Current students.
  5. Category E - 1GB: Alumni, part-time teachers, retired faculty, and others.
  6. Category F - 0GB: Shared email accounts.
  7. Category G - Cloud shared storage allocated based on the designated tiers of the unit:

Tier	Number of Unit Members	Storage
Tier 1	0-10 people	100GB
Tier 2	11-30 people	300GB
Tier 3	31-50 people	1000GB
Tier 4	More than 50 people	2000GB

Article 5 The application process for email accounts is as follows:

1. Faculty and staff, tenure-track assistants, and postdoctoral researchers:  
After registering with the Office of Human Resources, they should apply through the email account management system.
2. Current students: The Office of Academic Affairs will apply for new student IDs in bulk, and the list will be uploaded to the email account management system.
3. Alumni: The Office of Public Affairs will apply for new student IDs in bulk, and the list will be uploaded to the email account management system.
4. Other personnel shall have their email accounts applied for by the responsible unit, following the procedures outlined in the human resources system and the email account management system.

Article 6 Email Account Usage Duration and Account Deletion Policy:

1. The email accounts of tenure-track personnel will be deactivated the day following the confirmation of their resignation by the Human Resources Department, and the accounts will be deleted three months after their resignation.
2. If the part-time teachers are not reappointed for the following semester, their email accounts will be deleted.
3. In cases of admission revocation, removal of academic standing, transfer, withdrawal, or suspension, the email accounts of students will be deleted based on the notification list provided by the Office of Academic Affairs.
4. Alumni may retain lifetime access to their email accounts; however, the

storage capacity will be adjusted in accordance with Article 4.

5. Retired faculty and staff at the university may retain lifetime access to their email accounts; however, the storage capacity will be adjusted in accordance with Article 4.
6. Each category across the university may be subject to storage limits based on the designated capacity. If the storage exceeds the approved limit, an email reminder will be sent to the user, and the account will be deactivated by the end of the semester. If the user does not request an adjustment within one month after deactivation, the account will be reset. The user or the affiliated unit will be responsible for any lost data.

Article 7 Principle of Email Account Establishment:

1. Faculty and Staff: They may select a unique account name and should avoid using sensitive personal identifiable information for the account.
2. Current Students Alumni: student IDs.
3. Tenure-track Assistant, Part-time Teachers, and Other Personnel: Employee IDs.

Article 8 The email account password must be at least eight (8) characters long and should avoid using passwords that are easy to guess or publicly available information.

Article 9 Units handling official or core business may apply for a "Unit Public Email Account" virtual mailbox. The application and usage guidelines for this account shall be prescribed elsewhere.

Article 10 The rights, responsibilities, and relevant security principles for email account users are as follows:

1. Email sending and receiving must comply with the university's network usage regulations.
2. Emails shall not be used for commercial purposes.
3. Users shall not misuse others' email accounts or interfere with the normal operation of the email system in any way.
4. Users shall not lend their email accounts to others. If a third party inappropriately uses the account and causes damage to the interests of the individual or the institution, the account owner shall bear full responsibility.
5. Users are responsible for backing up the data associated with their email

accounts. The Office will not be liable for safekeeping the data or compensation.

6. When sending sensitive or confidential data via email, the data must be compressed and encrypted. The password for decompressing and the password for the encrypted email should be sent separately.
7. It is recommended that the password for the email account is renewed every six months.

If any inappropriate usage is confirmed, the Office may revoke the user's access rights. Any loss or disputes that occur during the account closure period shall be the sole responsibility of the user.

Article 11 The unresolved matters in these Guidelines will be complied with the government's or the university relevant regulations.

Article 12 The implementation of these Guidelines follows their passage and approval by the Information Technology Meeting. The same shall apply with revisions with these Regulations.