STANDARD OPERATING PROCEDURE : AIT OFFICIAL EMAIL ID

INTRODUCTION

1.   The Institute assigned email account shall be an official means of communication with all students, faculty, and staff. Email accounts are available for Faculty, staff, students, and alumni.

2.   Users are solely responsible for all information sent to them via their Institute assigned Official email account. Users who choose to forward mail from their Institute email accounts are responsible for ensuring that all information, including attachments, is transmitted in its entirety to the preferred account.

3.   The account and the contents of the account are governed by AIT copyright and intellectual property policy.

4.   All account holders must adhere to the AIT policy for the email account use. The use of the AIT email account will indicate acceptance of this procedure.

AIM

5.   Staff and Students are expected to check their AIT Official e-mail account on a frequent and consistent basis.

PROCEDURE

Expectations about Staff/ Student Use of AIT Official Email

6.   AIT recommends checking e-mail thrice a week at a minimum; in recognition that certain communications may be time-critical.

Username and Password

7.   Your initial/default User ID and Password are provided to you upon admission/employment to AIT. It is the user's responsibility to set the password to as per Microsoft password policy for office 365 mail id.

Characters allowed	A – Z, a - z, 0 – 9, @ # $ % ^ & * - _ ! + = [ ] { }	\ : ' , . ? / ` ~ " ( ) ;
Characters not allowed	Unicode characters, Spaces, Strong passwords only: Cannot contain a dot character '.' immediately preceding the '@' symbol
Password restrictions	8 characters minimum and 16 characters' maximum Strong passwords only: Requires 3 out of 4 of the following: • Lowercase characters • Uppercase characters • Numbers (0-9) • Symbols (see password restrictions above)

8.   Email passwords and other credentials may not be shared. Email systems that rely exclusively on a User ID/ password combination for security shall require periodic password changes to ensure that the account maintains its integrity. Multi Factor Authentication will be enabled on email id to improve security.

9.   Admin will create a group email address, &, if necessary, a shared email account, for any academic or administrative department. Users will be able to create groups but if found misuse of group creation, AIT admin have rights to stop group creation & delete such groups from mail System.

Creation and Deletion Email Accounts

10.   Following procedure will be adapted for creation/ deletion Email IDs :-

11.   **Faculty/ Staff**.

(a)   **General Account Creation for Staff**. The Registrar Office is responsible to inform the Email admin to create new accounts for newly recruited staff.

(b)   **Account Deletion**. When a Staff member leaves AIT by retirement, resignation or termination, the email account will revert to the Institute. The Registrar is responsible for informing the Email admin about deactivation of the email account after service termination. Personal Email id of staff gets deleted after resignation and termination.

(i)   The retired faculty or staff member account will be deactivated after completion of his/ her administrative and financial dues. The registrar will inform the email admin after this to deactivate the account.

(ii)   Designation/ Post email id will get transferred to newly appointed staff on the same post.

(ii)   After completion of the contractual period of an employee, the registrar should inform email admin to deactivate the email account.

12.   **Students**.

(a)   **Creation and Deletion of Accounts**. When an individual student secures admission in AIT, his/her email account will be created. Student should use this AIT email account only for internal communication with all stakeholders of AIT and academic related communication with other outside stakeholder like employers, University, AICTE, and other Institutes. Students should not use this AIT email account for any private and illegal activities. If any student found involved in any illegal activities through email, then his/her AIT email account will be immediately frozen, and matter will be handed over to the investigating committee. Further decisions will be based on the investigating committee's report.

(b)   If a student cancels his/her admission, then the mail account will be deleted within a period of 7 days of cancellation of admission.

13.   **Alumni Accounts**. Graduating students will retain their email account as Alumni till the next three year after passing out as per following :-

(a)   Only Exchange license (mailing facility) up to 3 years.

(b)   Other Apps License should be removed, 1 year after passing out.

Privacy Provisions

14.   AIT will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that the systems should not be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, AIT can assure neither the privacy of an individual user's use of the Institute's electronic mail resources nor the confidentiality of messages that may be created, transmitted, received, or stored thereby.

15.   To create new email id of students, respective department HOD will share the Student Information.

Abuse of Accounts

16.   The Acceptable Use Procedure, Institute policies and the current legal standards apply to all accounts. Under authorization from the appropriate Institute authority, Admin can block an abusive account in order to investigate complaints.

17.   The owner of an email account is responsible for its use and is presumed to send all email actually sent from that account. Users may not alter an email address to disguise or block the identity of the sender.

Violation of Policy/ Potential Compromised Activities

18.   Users will restrict from sending messages outside the organization (AIT) due to potential compromised activity if found on mail box :-

(a)   AIT Official mail id accounts being blocked due to reasons such as,

   (i) Sending suspicious messages outside the organization.

   (ii) Sending bulk mail inside an organization with attachment.

   (iii) Forwarding mail multiple times to other users.

(b)   To avoid such an incident please follow instructions strictly.

   (i)   Keep a strong password.

   (ii)   Change password frequently.

   (iii)   Check regular mail and avoid an unattended mailbox.

   (iv)   Regularly check the sent mail tab.

   (v)   If any suspicious activities are found in your mailbox, write to email administrator, or contact your respective department staff.

Protection of Accounts from External Abuse Such as Spam or Viruses

19. Admin/System uses several levels of email scanning for SPAM and viruses before delivery. System cannot guarantee that all viruses will be caught by these measures. Therefore, all computers on campus and personal computers/ Mobile are required to use current anti-virus, anti-spam and anti-spyware tools. Students and Staff should update the antivirus regularly on the system and scan the system with a full scan option.

20. Don't open Spam mail. If required, check "From" email id instead of display name. Never respond to spam Mail and do not forward to others:-

(a) User will report to the email admin regarding SPAM Message. If bulk spam messages are received on the AIT domain by external senders, then the admin will restrict that sender to send the mail on AIT domain account. If an individual user receives messages from an unknown sender, the user can block the sender from his/her account and will report to admin to further security things.

(b) If a user opens spam mail and replies to the unknown sender, immediately after knowing that it was a phishing/ spam mail user should report to the email admin. The user will also immediately change password using a different device and after that scan the affected device- PC/ Mobile immediately with full scan option.

Renaming of Accounts for Personal Name Changes

21. Employee account holders who have legal name changes can request that through Registrar AIT. Students may contact the office of the Registrar.

Group Creation/ Deletion Policy

22. Students club in charge or any coordinators, faculty members, higher authority are allowed to create a group for one year, but they should take the permission from email admin for the same.

23. Groups created without permission will be deleted by the Email admin.

24. Groups: All Groups created by Students should be deleted with the change in Academic Year.

25. Students and staff have the facility of creating Groups on Teams and Mail id for Academic Purpose.

26. All staff and students should follow rules while creating a Group on Teams and Mail id.

27. Give proper name which will be fulfilled Academic purpose as per standard naming convention for Groups and Teams Meeting.

28. While creating, write the purpose of group creation in the Description Field.

29. While creating a group on Office 365 Official email id please don't enable the following option.

Let People Outside the Organization Send Email to the Group.

30.   Email Group Facility should be used only for AIT inside communication; Outsiders should not be able to send mail to AIT office365 group.

31.   All students/ staff should delete groups which are created for previous Academic Year. Before deletion, Students/ Staff can download data.

CONCLUSION

32.   The above procedure will be strictly adhered for proper utilisation of email IDs and stop their misuse completely.

File No : AIT/0001/Gen Ruling/Adm
Army Institute of Technology
Alandi Road, Dighi Hills, Pune - 15

Date: 6 | Aug 2023

(Abhay A Bhat)
Brig (Retd)
Director

Distribution

1.   Principal.
2.   HOD E&TC.
3.   HOD Mech.
4.   HOD Comp.
5.   HOD IT.
6.   HOD ASGE.
7.   TPO
8.   Registrar

9.   All Wardens.
10.   Exchange.
11.   MI Room.
12.   Central Store.
13.   Office Copy