



الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يُونِيسَيتِي إِسْلَامُ إِنْتَارَا بَغْسَا مَلِيسِيَا

Garden of Knowledge and Virtue

Guidelines on Group Email Account Management

International Islamic University
Malaysia (IIUM)

Document Change Log

Version	Revision	Date	Pages Affected	Remarks/Change Reference
Version 00	00	02/10/26	-	Initial Submission

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Mohd Khairul Sazaney Bin Abu Jaziz	Endorsement from ITD Management	02/10/2026	06/10/2026

1. OBJECTIVE

The objective of this document is to define the official guidelines, ownership responsibilities, and step-by-step procedures for setting up the group Google account management on KCDIOM using the Google Authenticator mobile application.

2. SCOPE

2.1 This guideline applies to all non-personal email accounts managed under the organization's Google Workspace environment (including departmental, office, kulliyah, unit, conference, project and event accounts).

2.2 This guideline applies to all designated Persons In Charge (PIC), administrative personnel, and staff members authorized to operate and access KCDIOM email accounts within IIUM.

3. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as the “University”.
ITD	Information Technology Division
ICT	Information and Communication Technology
KCDIOM	Kulliyahs, Centres, Divisions, Institutes, Offices and Mahallahs
2SV	2-Step Verification (Two-Factor Authentication)
PIC	Person In Charge (The assigned staff member responsible for account management and security compliance)
Google Workspace	Suite of cloud computing, productivity, and collaboration tools including Gmail and Google Drive
Google Authenticator	Mobile security application that generates Time-Based One-Time Password (TOTP)
Non-Personal Account	Kulliyah, Departmental, office, conference, unit or event an email account

4. GUIDELINES AND PROCEDURE

4.1 Account Ownership and PIC Designation

- 4.1.1 Every departmental or office email account (non-personal account) must have an officially assigned one or two Person In Charge (PIC) registered with the KCDIOM.
- 4.1.2 The designated PIC is responsible for managing 2SV settings, maintaining account access, and ensuring compliance with organizational ICT policies.
- 4.1.3 If a department, office, or unit refuses or fails to assign a PIC for an email account, the account will be revoked, suspended, or deactivated by the IT Division.

4.2 Prerequisites for 2SV

Download and install the Google Authenticator app on an appointed PIC mobile device from the official Apple App Store (iOS) or Google Play Store (Android).

4.3 Step-by-Step Setup Procedure

Step 1: Access Security Settings on Computer

- 1. Open a web browser on your computer and sign into your office/department account at myaccount.google.com.
- 2. Click Security on the left-hand menu.
- 3. Under *How you sign in to Google*, select 2-Step Verification > Get Started.
- 4. Scroll to *Authenticator app* and click + Set up authenticator to display the QR code on your screen.

Step 2: Sign In to Google Authenticator App

- 1. Open the Google Authenticator app on your mobile device.
- 2. Tap the profile icon in the top-right corner of the app screen.
- 3. Select Add another account (or tap Sign in if opening the app for the first time).
- 4. Log in using your office/department email address and password. Signing in ensures generated codes are backed up and synchronized to your office cloud account.

Step 3: Scan the QR Code using PIC mobile device

- 1. Confirm that your office/department email profile is selected as the active profile in the top-right corner of the Authenticator app.
- 2. Tap the + (plus) icon in the bottom-right corner.
- 3. Tap Scan a QR code (grant camera permission if prompted).
- 4. Point your mobile device camera at the QR code displayed on your computer screen.

Step 4: Verify Connection and Save Backup Codes

1. Click Next on your computer screen.
2. Type the 6-digit verification code currently generated in your Google Authenticator app into the computer prompt and click Verify.
3. Return to the main 2-Step Verification page, select Backup codes > Get backup codes. Save or print these 10 single-use recovery codes in a secure location for emergency access.

5. IMPLEMENTATION AND NON-COMPLIANCE

5.1 The Director of Information Technology Division holds the responsibility for the implementation of these guidelines and shall take necessary enforcement actions.

5.2 Revocation of Email Account: If an KCDIOM fails to appoint a PIC, or if the assigned PIC does not complete 2SV enablement within the stipulated timeframe, ITD reserves the right to immediately revoke and terminate access to the email account.

5.3 Any unassigned or orphaned accounts will be purged after 30 days of deactivation.

6. ENFORCEMENT

All staff members, KCDIOM and appointed PICs utilizing an official organization or departmental email account are subject to this guideline.

7. MAINTENANCE AND MONITORING OF GUIDELINES

The Information Technology Division is responsible for the formulation, continuous review, and maintenance of this document.

8. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

8.1 This guideline shall be read together with the following documents:

- 8.1.1 ICT Regulations
- 8.1.2 IIUM ICT Policy
- 8.1.3 IIUM ICT Security Policy
- 8.1.4 Policy for Electronic Account
- 8.1.5 Guidelines on Electronic Data Management
- 8.1.6 Guidelines for Responsible Use of ICT Resources
- 8.1.7 Standard for Electronic Accounts

Title of Guideline	:	Guidelines on Group Email Account Management
Number of Guidelines	:	IIUM-ISMS-L3-028
Approving Authority	:	ITD Management
Approval Date	:	06/10/2026
Effective Date	:	06/10/2026
Version No.	:	00
Revision No.	:	00