



الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يُونِيسَيتِي إِسْلَامِيْ اِنْتَارَا بَغْسَا مَلِيسِيَا

Garden of Knowledge and Virtue

Policy for Electronic Accounts

International Islamic University
Malaysia (IIUM)

Document Change Log

Version	Revision	Revision Date	Pages Affected	Remarks/Change Reference
Version 01	00	23/07/2012		
Version 02	00	20/03/2014		
Version 02	01	20/11/2025	5,7	Update clause 3.1 & 3.2
Version 02	02	26/02/2026	5,6,7	Update clause 3.5, 3.7 & 3.8
Version 03	00	07/04/2026		Revision of Policy content
Version 03	00	10/04/2026		Fair copy of the Policy

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Adi Azmir Abdul Ghani, ITD	Initial draft	18/09/2008	—
Adi Azmir Abdul Ghani, ITD	Reviewed by ICT Policy Review Committee Meeting No. 2/2008	18/09/2008	—
Adi Azmir Abdul Ghani, ITD	Approved by ICT Council No. 1/2009	—	30/01/2009
Assoc. Prof. Dr Abd Rahman Ahlan, ITD	Approved by ICT Committee No. 2/2012	-	31/07/2012
Prof. Adam Suhamimi	Approved by ICT Committee No. 3/2014		08/12/2014
Abu Hurairah A. Manaf, ITD	Reviewed in ICT Committee Meeting	28/11/2025	
Abu Hurairah A. Manaf, ITD	Submission to ICT Committee No. 01/2026	10/04/2026	
Abu Hurairah A. Manaf, ITD	Submission to ICT Committee No. 02/2026	24/09/2026	24/09/2026

SECTION 1: INTRODUCTION

1.1 Objective

This policy defines the requirements for the creation, management, security, and operation of electronic accounts for International Islamic University Malaysia (IIUM). This policy ensures the security, integrity, and reliability of IIUM's electronic communications, protects sensitive information, and maintains a secure digital environment for all users.

1.2 Scope

This policy shall cover all matters from the creation to closure of the electronic account, password management, account security, and operational control to mitigate unauthorised access and misuse.

1.3 Applicability

This policy applies to all IIUM staff, students, or authorised third parties including but not limited to contractors, consultants, visiting academics, researchers, service providers, and official partners, who use the University's electronic accounts and passwords.

1.4 Terms and Definitions

Term	Definition
Authentication	A process or service to identify and verify an individual.
Authorised Third Party	Any external individual or organisation formally granted permission to access or use the University's electronic accounts, ICT systems, data, or services for a defined purpose, including but not limited to contractors, consultants, visiting academics, researchers, service providers, and official partners, in accordance with applicable policies, agreements, and security requirements.
CDO	Chief Digital Officer
Electronic Account	A mechanism, typically comprising a username and password, and where applicable additional authentication factors such as biometrics, smart cards, or one-time passwords, that enable an individual to identify and authenticate themselves to computer systems, applications, networks, databases, cloud services, or other authorised digital services.
ICT	Information and Communication Technology

ITD	Information Technology Division
University/IIUM	International Islamic University Malaysia
User	Any individual or entity, including staff, students, vendors, and other authorised third parties, who access or use the University's ICT facilities.

SECTION 2: POLICY STATEMENTS

- 2.1 This Policy establishes the requirements for the proper management, protection, and use of electronic accounts, to maintain a secure, reliable, and trustworthy digital environment and to safeguard access to the University's ICT systems, data, and services in accordance with established security and governance requirements.
- 2.2 This policy shall be implemented in compliance with the IIUM's Anti-Bribery Management System (ABMS) in accordance with ISO 37001:2025 requirements, to ensure transparency, integrity, and accountability in all processes. All procurement activities shall reflect a commitment to fostering an anti-bribery culture, recognising and managing conflicts of interest, and applying enhanced due diligence to third parties and sustainability-related aspects. Any actual or suspected bribery, corruption, or conflict of interest shall be reported through secure and protected channels, with whistle-blower protections in place.
- 2.3 This policy shall be implemented in accordance with IIUM's ICT Security Policy in compliance with ISO/IEC 27001:2022 requirements to ensure confidentiality, availability and integrity in all processes. All processes, decisions, and activities under this policy must uphold the principles of confidentiality, availability and integrity to protect information, data and assets.

SECTION 3: IMPLEMENTATION

3.1 Account Creation and Management

- 3.1.1 ITD is responsible for the creation, protection and changes of electronic accounts and passwords.
- 3.1.2 ICT resources that produce, maintain, transmit or permit access to University's data shall be protected by at least an electronic account or other approved authentication mechanisms.

3.2 Password

- 3.2.1 All electronic accounts must be protected by a strong and unique password that meets established security requirements by ITD.

- 3.2.2 Passwords are personal and confidential. Users shall not share their password with any other person, including colleagues, friends, or family members. Passwords shall not be written down or recorded in unsecured or unsafe circumstances.

3.3 Multi-Factor Authentication

- 3.3.1 The University shall implement Multi-Factor Authentication (MFA) for electronic accounts to provide an additional layer of security beyond a password.
- 3.3.2 The MFA must be activated by all users where required.
- 3.3.3 All users shall not bypass, disable or attempt to circumvent MFA control.

3.4 Account Access and Monitoring

- 3.4.1 Access to the University's electronic account is permitted only for authorised IIUM University's staff, students, and approved external third parties, including but not limited to contractors, consultants, visiting academics, researchers, service providers, and official partners, are allowed to have access to the University's electronic accounts.
- 3.4.2 Appropriate access control mechanisms shall be implemented for identification, authentication and authorisation of all users.
- 3.4.3 User activities on the system shall be logged for audit and investigative purposes.
- 3.4.4 Activity logs shall be retained for an appropriate period and reviewed regularly to detect anomalous or unauthorised access.

3.5 Suspicious Activity and Compromise

- 3.5.1 Users who suspect their electronic account has been potentially or compromised must immediately report the incident to the ITD and take steps to secure their account.
- 3.5.2 Procedures shall be in place to investigate and remediate compromised accounts, including temporary suspension of access if necessary.

3.6 Use of Electronic Accounts

- 3.6.1 Use of the University's electronic account is permitted only for authorised users.
- 3.6.2 Users shall not use the University's electronic account for illegal or

fraudulent activities, sending harmful communication, disseminating malicious software or spam, or unauthorised commercial activities.

3.7 Termination

ITD shall terminate the user's access to the electronic account in the following circumstances:

- 3.7.1 Staff - One (1) month upon the termination of employment.
- 3.7.2 Student - Three (3) months after the graduation confirmation by the Senate.
- 3.7.3 Authorised Third Party - automatically terminated upon expiry of the service or contract rendered by or to the University.

3.8 Personal Data Protection and Confidentiality

Users shall adhere with the Personal Data Protection Act 2010 (PDPA) and exercise care when transmitting sensitive information via an electronic account.

3.9 Guidelines or Procedures

The implementation and adherence to this policy shall be carried out in accordance with the guidelines or procedures developed separately from this policy. These guidelines or procedures provide detailed steps, tools and actions required to ensure compliance with the policy's directions and objectives.

3.10 Compliance and Enforcement

- 3.10.1 The Director of the ITD holds the responsibility for the implementation of this policy and shall take necessary actions in the event of violation of this policy.
- 3.10.2 This policy is applicable to the University community and any infringement of the policy may be subject to disciplinary actions and/or any other actions deemed necessary.

SECTION 4: ADMINISTRATION OF THE POLICY

4.1 Ownership of the Policy

The ITD is responsible for the formulation and maintenance of this policy.

4.2 Effective Date

This policy will take effect upon approval by the ICT Committee.

4.3 **Approval and Authority**

The ICT Committee shall be the approving authority for this policy and matters related thereto.

4.4 **Review and Revision Process**

This policy shall be reviewed from time to time to ensure its continued relevance and effectiveness, with reviews conducted at least annually or as circumstances require.

4.5 **References**

- 4.5.1 IIUM ICT Policy
- 4.5.2 IIUM ICT Regulations
- 4.5.3 IIUM ICT Security Policy
- 4.5.4 Personal Data Protection Act 2010 (Act 709)
- 4.5.5 IT Infrastructure Library (ITIL)
- 4.5.6 Control Objectives for Information and Related Technologies (COBIT)
- 4.5.7 IIUM Anti Bribery and Corruption Policy

Title of Policy	:	Policy for Electronic Account
Number of Policy	:	IIUM-ISMS-L1-012
Approving Authority	:	ICT Committee
Approval Date	:	24/09/26
Effective Date	:	24/09/26
Version No.	:	03
Revision No.	:	00