Standard for Electronic Accounts

International Islamic University Malaysia (IIUM)

Document Change Log

Version	Revision	Date	Pages Affected	Remarks/ Change Reference
Version 01	00	13/11/2008	All pages	Initial draft
Version 01	01	26/10/2025	4	Add clause 4.3 and update Section 7
Version 01	02	12/02/2026	6	Add clause 4.2.2
Version 01	03	11/03/2026	6	Update clause 4.2.5

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Adi Azmir Abdul Ghani, ITD	Initial draft	18/09/2008	-
Adi Azmir Abd Ghani, ITD	Reviewed by ICT Policy Review Committee Meeting No. 3/2008	13/11/2008	-
Adi Azmir Abd Ghani, ITD	Approved by ICT Policy Review Committee Meeting No. 3/2008	_	13/11/2008
Abu Hurairah Abd. Manaf	Endorsement by ITD Management	20/11/2025	20/11/2025
Abu Hurairah Abd. Manaf	Endorsement by ITD Management	12/02/2026	12/02/2026
Abu Hurairah Abd. Manaf	Endorsement by ITD Management	13/03/2026	13/03/2026

1. OBJECTIVE

The objective of this document is to provide a standard for electronic accounts used to identify and authenticate individuals and their access to IIUM ICT resources and infrastructure

2. TERMS AND DEFINITIONS

Term	Definition
Departmental Accounts	Accounts shared by multiple but individually authorised individuals for a specific purpose. For example, an account to manage a departmental electronic email account.
Electronic Account	A mechanism, which usually consist of a username and password, or other additional information such as biometric, a card or second password that allows individuals to identify themselves to a computer system or other entities.
User-level Password	Password for email, web services, desktop computer, etc.
System-level Password	Password for root, admin, administrator, application administration accounts, etc.

3. GOVERNING POLICY

3.1 (IIUM/ITD/ICTPOL/5.1) Policy for IIUM Electronic Accounts

4. STANDARD

The standards are as follows:

4.1 Electronic Accounts:

4.1.1 Individual who is granted access to IIUM ICT resources and information shall be assigned his or her own unique electronic account(s) or authentication mechanisms to enable him or her to access and use authorised IIUM ICT resources and information.

4.1.2 Sharing of accounts is prohibited, except for departmental or system accounts.

4.1.3 An account manager shall be identified for each departmental or

system account. The account manager shall establish a formal method to grant, track and terminate individual access and activity.

4.1.4 For temporary access to IIUM resources for a specific purpose and period, a guest account may be provided. The parties that authorise and issue guest accounts shall establish a formal method for authentication, accountability and tracking procedures. All guest accounts shall be created with an expiration date and time, and shall be disabled immediately upon the expiration date and time.

4.1.5 Initial delivery of electronic account password shall be established using a unique and randomly generated password.

4.1.6 Resetting of electronic account password shall be re-established using a unique and randomly generated password.

4.1.7 Expired electronic accounts shall be locked, disabled, removed or otherwise protected from unauthorised access.

4.1.8 An account lockout mechanism with the maximum failure limit set to five attempts shall be established in order to minimise the risk that an unauthorised party will gain access to restricted or confidential IIUM resources and information.

4.1.9 Accounts suspected for misuse or for having compromised shall be suspended or locked. Immediate report shall be forwarded to the Director of ITD. Prior to reactivation, accounts of this kind shall require password resets, with the assignment of a new and unique password.

4.1.10 A periodic account management will be conducted by the system administrator to ensure updated privileges are assigned and to ensure unauthorised access.

4.2 Electronic Passwords:

4.2.1 Resetting of electronic account password shall be re-established using a unique and randomly generated password.

4.2.2 Passwords shall have a minimum length of eight (8) characters and must include at least one uppercase letter, one lowercase letter, one numeric character, and one special character to enhance password strength.

4.2.3 All system-level passwords shall be changed at least every three months.

4.2.4 All stored passwords shall be encrypted.

4.2.5 Passwords shall be transmitted using secure and controlled mechanisms to maintain confidentiality and integrity, and to ensure that the credentials are received only by the intended recipient. Where transmission via email is necessary, the password shall be protected using appropriate security controls (e.g., encryption, password-protected attachments, or secure one-time access links). The recipient's identity shall also be verified through an independent communication channel prior to activation or use of the password.

4.2.6 A password shall be different from the username. Blank passwords shall not be allowed.

4.2.7 IIUM staff number, IIUM student matriculation number, Malaysian Identification Number, Passport Number and birth date shall not be used in their entirety or part, for the password.

4.2.8 IIUM passwords shall not be shared with anyone for any reason at any time.

4.2.9 IT technical staff shall not ask for the password of IIUM staff, student, or others possessing an IIUM electronic account password.

4.2.10 Password shall not be written down or stored permanently in any manual or electronic files.

4.2.11 Authorised IT personnel shall perform periodic or random password cracking and guessing activities. The account which password was cracked or guessed shall be disabled until the password has been reset.

4.3 This standard 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 standard must uphold the principles of confidentiality, availability and integrity as to protect the information data and assets.

5.0 RESPONSIBILITY FOR IMPLEMENTATION

The responsibility for the implementation of this standard lies with the Heads of Departments of ITD and other relevant IT personnel at Kulliyyah/Division/Centre/ Institute that oversee the overall operations of the departments/offices, which relate to provisioning, maintaining, and securing electronic accounts and related ICT resources.

6.0 ENTITIES AFFECTED BY THIS STANDARD

IIUM staff members, students, consultants, vendors and others that use, create, administer and maintain IIUM owned electronic accounts and passwords and related ICT resources.

7.0 RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

This policy shall be read together with the following or any documents below:

7.1 IIUM ICT Policy

7.2 ICT Regulations

7.3 IIUM Information Management Policy

7.4 IIUM ICT Security Policy

7.5 IT Infrastructure Library (ITIL)

7.6 Control of Business IT (COBIT)

Title of Standard	:	Standard for Electronic Account
Number of Standard	:	IIUM-ISMS-L3-016
Approving Authority	:	ITD Management
Approval Date	:	13/03/2026
Effective Date	:	13/03/2026
Version No.	:	01
Revision No.	:	03