الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
Garden of Knowledge and Virtue

Standard for Electronic Accounts - DRAFT

IIUM ICT GUIDELINES

PREPARED FOR:
International Islamic University Malaysia

PREPARED BY:
Information Technology Division

Document Change Log

Release Version	Document No	Date	Pages Affected	Remarks/Change Reference
Version 01	IIUM/ITD/ICTPOL/5.3	13-NOV-2008		
Version 1.1		26/10/2025	4	

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	Add clause 4.1 and 4.2	28/10/2025	

IIUM ICT Guidelines

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 authorized 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

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

4. STANDARD

The standards are as follows:

4.1 This standard 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, recognizing 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.

4.2 This policy shall be implemented in accordance with IIUM's ICT Security Procedure

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/guideline must uphold the principles of confidentiality, availability and integrity as to protect the information data and assets.

4.3 Electronic Accounts:

4.3.1 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 authorized IIUM ICT resources and information.

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

4.3.3 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.

4.3.4 For temporary access to IIUM resources for a specific purpose and period, a guest account may be provided. The parties that authorize 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.

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

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

4.1.8 Expired electronic accounts shall be locked, disabled, removed or otherwise protected from unauthorized access.

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

4.1.10 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.

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

4.4 Electronic Passwords:

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

4.4.2 bAll system-level passwords shall be changed at least every three months.

4.4.3 All stored passwords shall be encrypted.

4.4.4 Passwords shall be transmitted via a secure method (encryption, security certificate) to protect the password and to ensure the correct individual receives the password.

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

4.4.6 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.

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

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

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

4.4.10 Authorized 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.

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 which recently approved:

7.1 IIUM ICT Policy

7.2 ICT Regulations

7.3 Information Management Policy

7.4 IIUM ICT Security Procedure