Policy for Electronic Accounts - DRAFT

IIUM ICT POLICY DOCUMENT

PREPARED FOR:
International Islamic University Malaysia

PREPARED BY:
Information Technology Division

IIUM ICT Policy

Document Change Log

Release Version	Date	Pages Affected	Remarks/Change Reference
Version 1.0	23-JUL-2012		
Version 2.0	20-MAC-2014		

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. Dr. Mohammad Adam Suhaimi, ITD			

IIUM ICT Policy

1. OBJECTIVE

1.1 The objective of this document is to define the policy to authorize and direct the establishment of standards, guidelines and procedures in the creation of IIUM electronic accounts and their passwords, protecting them and any operational matters on the electronic account and its password.

1.2. This policy shall covers any staff and students, or any other entity that has IIUM account name, user identification or password that allows access to IIUM networks, electronic infrastructure, devices, data, hardware and software of IIUM.

2. TERMS AND DEFINITIONS

Term	Definition
ITD	Information Technology Division
Standards	Mandatory activities, actions, rules or regulations designed to provide policies with the support structure, and specific direction they require to be meaningful and effective. They are often expensive to administer and therefore shall be used judiciously.
Guidelines	General statements designed to achieve the policy objectives by providing a framework within which to implement procedures, whereby standards are mandatory, guidelines are recommendations.

Procedures	Explains specifically on how the policy and the supporting standards and guidelines will actually be implemented in an operating environment.
Authentication	A process or service to identify and verify an individual.
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.
CIO	Chief Information Officer
HOD	Head of Department

3. POLICY STATEMENTS

3.1 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, 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.

3.2 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.

3.3 ITD shall create standards, guidelines and procedures on creation, protection and changes of electronic accounts and passwords.

3.4 The distribution of the established standards, guidelines and procedures, or part of them, should be distributed only to IIUM staff and students in need to adhering to this policy.

3.5 ICT resources that produce, maintain, transmit or permit access to IIUM data shall be protected by at least an electronic account or other approved authentication mechanisms.

3.6 Different levels of password security are to be created for users and accounts with differing levels of access and authorization.

3.7 Only authorized IIUM staff, students and other related entities are allowed to have access to IIUM electronic accounts.

3.8 Contractor/Vendor's access is to be automatically terminated once their contract expires.

3.9 Users should be held responsible for every transaction being carried out using their login account.

4. IMPLEMENTATION AND NON-COMPLIANCE

4.1 The Director of Information Technology Division holds the responsibility for the implementation of this policy and shall take necessary actions in the event of violation of this policy.

4.2 Anyone found to have violated this policy may be subject to loss of certain privileges or services. Possible disciplinary actions may be proposed to the relevant higher authority.

4.3 Vendor, consultant or contractors that abuse the privileges shall provide compensation for any loss suffered due to abuse or unauthorized usage.

5. ENTITIES AFFECTED BY THIS POLICY

5.1 IIUM staff, students, consultants, vendors or others who use IIUM owned electronic accounts and passwords.

6. MAINTENANCE OF POLICY

6.1 The Information Technology Division is responsible for the formulation and maintenance of this policy.

7. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

7.1 ICT Regulations

7.2 ICT Security Procedure

7.3 Standards for Electronic Accounts