INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA (IIUM)

Document No : IIUM/ITD/ICTPOL/5.3

Effective Date : 13/11/2008

Standard for Electronic Accounts

Chapter : Security

Status : APPROVED

Version No : 01
Revision No : 01

1.0 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.

2.0 GOVERNING POLICY

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

3.0 STANDARD

The standards are as follows:

3.1 Electronic Accounts:

3.1.1 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 authorized IIUM ICT resources and information.

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

3.1.3 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.

3.1.4 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.

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

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

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

3.1.8 An account lockout mechanism with the maximum failure limit set to five (05) 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.

3.1.9 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.

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

3.2 Electronic Passwords:

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

3.2.2 All system-level passwords shall be changed at least every three (3) months.

3.2.3 All stored passwords shall be encrypted.

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

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

3.2.6 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.

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

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

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

3.2.10 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.

4.0 RESPONSIBLITY 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.

5.0 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.

6.0 DEFINITION

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.

7.0 REVISION HISTORY

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