THE AMERICAN UNIVERSITY IN CAIRO
الجامعة الأمريكية بالقاهرة

December 12, 2013

PASSWORD POLICY

Policy Statement

To ensure users are aware of the importance of passwords to prevent unauthorized use, protection of user accounts and to eliminate compromise of the entire AUC network.

Reason for Policy/Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Who Approved This Policy

Executive Vice President for Administration & Finance	Mr. Brian MacDougall
Date:	
Chief Technology Officer	Ms. Nagwa Nicola
Date:	December 12, 2013

Who Needs to Know This Policy

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any AUC facility, or has access to the AUC network (including contractors and vendors with access to AUC systems).

Web Address for this Policy

http://www.aucegypt.edu/about/policies/Pages/default.aspx

Contacts

Responsible University Official: Mr. Wessam Maher, Senior IT Security Officer
Responsible University Office: University Technology Infrastructure (UTI) – IT Security office
If you have any questions on the policy or procedure for this policy, you may:

1. Call 2615.3543, or
2. Send an e-mail to wessam.maher@aucegypt.edu

Definitions:

Term (alphabetical order)	Definition as it relates to this policy
AUC	The American University in Cairo
AUC Community	This term refers to the AUC faculty, staff ,alumni and students
UTI	University Technology Infrastructure

Policy/Procedure:

General :

- All passwords of administrative, highly privileged accounts (e.g., root, enable, administrator, application administrative accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every four months. Access to University systems will be closed when a user password is not changed every four months as required.
- Passwords must not be inserted into email messages or any other forms of unencrypted electronic communication.
- Passwords must not be written on any media and subsequently left in an unsafe location.
- Default passwords of any electronic system must be changed during the installation of the system.
- All passwords must conform to the guidelines per the AUC password guideline *(please refer to the guidelines section)*.
- Systems and application administrators must enforce this policy on their systems.
- The same password must not be used for multiple accounts

Enforcement :

Access to University systems will be closed when a user password is not changed every four months as required. Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or dismissal from the University.

Forms:

NA

Related Information:

NA

Appendices (Optional):

NA

History/Revision Dates:

Origination Date:	September 13, 2012
Last Amended Date:	December 12, 2013
Next Review Date:	December 12, 2014