Document title: **[Password Policy – August 2018]**

Approval date: **[August 2018]**

Purpose of document:
[The purpose of this policy is to establish a standard for creation of strong passwords, t he protection of those passwords, and the frequency of change.]

Office/department responsible: **Information Security Office, Office of Information Technology**

Approved by: **[** Ms. Nagwa Nicola, Chief Technology Officer**]**

Document classification level: **[PUBLIC]**

Document accessible: **[https://www.aucegypt.edu/about/university-policies]**

Document includes: **[Policy, charts, appendix and approvers]**

Related documents/see also: **[** AUC Data Governance Policy, Information Security Policy, Electronic Mail Email Policy, Acceptable Use Policy, Peer to Peer Sharing Policy**]**

AUC PASSWORD POLICY

Policy Statement

To ensure users are aware of the importance of passwords to prevent unauthorized use, protec tion 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 prot ection of those passwords, and the frequency of change.

Who Approved This Policy

Ms. Nagwa Nicola, Chief Technology Officer

Who Needs to Know This Policy

Entire AUC Community

Web Address for this Policy

https://www.aucegypt.edu/about/university-policies

Contacts

Responsible University Official: Wessam Maher
Responsible University Office: Information Security Office, Office of Information Technology
If you have any questions on the policy, you may send an e-mail to infosec@aucegypt.edu

Definitions

Term (alphabetical order)	**Definition as it relates to this policy**

Policy/Procedures

1. 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.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every four months.
3. Access to University systems will be closed when a password is not changed as scheduled
4. Passwords must not be inserted into email messages or any other forms of unencrypted electronic communication. Exception must be approved explicitly by Information Security.
5. Passwords shouldn't be inserted, transmitted or saved in plain text in any transmission, coding or configuration
6. Multiple step verification mediums "like physical/logical tokens and one time passwords over sms….etc." are considered at the same level of importance and should be preserved and kept safe as well as Passwords.
7. Multiple step verification mediums can be considered a replacement to the password change process. Approval of both Chief Technology Officer and Principal Campus Information Security Officer must be granted for this consideration.
8. Passwords must be changed immediately whenever there is a suspicious activity.
9. AUC Systems administrators & IT Help Desk should keep records for password changes and reset and perform secure procedures for password reset and changes requests.
10. Passwords must not be written on any media "Like sticky notes" and subsequently left in an unsafe location.
11. Default passwords of any electronic system must be changed during the installation of the system.
12. All passwords must conform to the guidelines per the AUC password guideline (please refer to the guidelines section).

13. Systems and application administrators must enforce this policy on their systems.
14. The same password must not be used for multiple accounts.
15. Password change, password reset and identity management processes should be established and managed adequately to ensure optimum security.
16. Public access digital devices/services that doesn't require a password or uses a public shared password should be approved by Principal Campus Information Security Officer to ensure the adequacy of the setup from security perspective.

Enforcement:

Access to University systems will be closed when a user password is not changed as required or if the user doesn't follow the multiple factor steps. 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/Instructions

Refer to the IT Help Desk, support@aucegypt.edu

Related Information

https://www.aucegypt.edu/about/university-policies

Appendices

AUC Password Guidelines

All passwords should meet or exceed the following guidelines. Strong passwords have the following characteristics:

- Contains at least ten characters, for IT systems & administrative accounts at least twelve characters
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain patterns such as aaabbb, qwerty, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123" "AUC123" "auc2020"
- You should never write down a password. Instead, try to create passwords that you can remember easily.

One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. (NOTE: Do not use any of these examples as passwords!)

There are some good password managers/vault solutions that can help you to save all of your passwords and you will need only to remember one key password instead. These solutions has many advantages and disadvantages so you need to be careful while choosing.

History/Revision Dates

Origination Date: September, 2012
Last Amended Date: January, 2017
Next Review Date: December, 2019