Information Classification Level: PUBLIC

October 2022

PASSWORD POLICY

Policy Statement

Ensure users know the importance of passwords to prevent unauthorized use, protect user accounts, and eliminate compromise of the entire AUC network.

Reason for Policy/Purpose

This policy aims to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Who Approved This Policy

Associate Vice President for Digital Innovation

Chief Information Security and Risk Officer

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.
If you have any questions on the policy, you may send an e-mail to infosec@aucegypt.edu

Policy/Procedures

1. All passwords of administrative, highly privileged accounts (e.g., root, enable, administrator, application administrative accounts, etc.) must be changed annually.
2. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed annually.
3. Accounts' multiple login failure locks should be enforced for protection.
4. Access to University systems will be closed when a password is not changed as scheduled
5. Passwords must not be inserted into email messages or any other forms of unencrypted electronic communication.
6. Passwords shouldn’t be inserted, transmitted, or saved in plain text in any transmission, coding, or configuration

7. 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.
8. Multiple-step verification mediums can be considered a replacement for the password change process. Approval of both Chief Technology Officer and Chief Information Security and Risk Officer must be granted for this consideration.
9. Passwords must be changed immediately whenever there is a suspicious activity.
10. AUC Systems administrators & IT Help Desk should keep records for password changes and reset and perform secure procedures for password reset and changes requests.
11. Passwords must not be written on any media “Like sticky notes” and subsequently left in an unsafe location.
12. Default passwords of any electronic system must be changed during the installation of the system.
13. All passwords must conform to the guidelines per the AUC password guideline (please refer to the guidelines section).
14. Systems and application administrators must enforce this policy on their systems.
15. The same password must not be used for multiple accounts.
16. Password change, password reset, and identity management processes should be established and managed adequately to ensure optimum security.
17. Public access digital devices/services that don’t require a password or use a public shared password should be approved by Chief Information Security and Risk Officer to ensure the adequacy of the setup from a 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.

Appendices

AUC Password Guidelines

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

- Contain at least ten 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,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
- Account Lockout duration is ten minutes; lockout in Banner and SAP is permanent and is manually unlocked.
- Account Lockout threshold is five attempts, three in SAP and Banner systems.
- The maximum password age for SAP is 90 days.
- The minimum password length for SAP is eight characters.
- Password history is 7
- The minimum password age is one day.

Poor, or weak, passwords have the following characteristics:

- It can be found in a dictionary, including a foreign language, or exists 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, preceded, or followed by a number (for example, secret1 or 1secret).
- Are some versions 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 to create a password based on a song title, affirmation, or other phrases. 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 save all of your passwords, and you will need only to remember one key password instead. These solutions have many advantages and disadvantages, so you need to be careful while choosing.

History/Revision Dates

Origination Date: September 2012
Last Amended Date: October 2022
Next Review Date: October 2025