Policy Title	Personal Credentials Creation and Management Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	Information Security Office (ISO)
Pertinent Dates	July 2022

I. SCOPE OF POLICY

The purpose of this policy is to educate Alamein International University students and staff on the characteristics of a Strong Password as well as to provide recommendations on how to securely maintain and manage credentials.

II. DEFINITIONS

Strong Password: is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

III. POLICY STATEMENT

The following are general recommendations for creating a Strong Password:
- A Strong Password should:
  - Be at least 8 characters in length (Letters, Numbers & Symbols)
  - Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
  - Have at least one numerical character (e.g. 0-9)
  - Have at least one special character (e.g. ~`!@#$%^&*()+=_-{}[]\|:;”’?/<>,.)

- Strong Passwords do not:
  - Spell a word or series of words that can be found in a standard dictionary
  - Spell a word with a number added to the beginning and the end
  - Be based on any personal information such as user id, student id, family name, pet, birthday, etc.

IV. RESPONSIBILITIES

This Policy applies to all students and staff that have a username and password to at least one University system or application, independent of whether you are an end user or a system administrator for that system or application.

V. POLICY STANDARDS AND PROCEDURES

The following are several recommendations for maintaining a Strong Password:

- Do not share your password with anyone for any reason
  Passwords should not be shared with anyone, including any students or staff. In situations where someone requires access to another individual's protected resources, delegation of permission options should be explored. For example, Microsoft Exchange calendar will allow a user to delegate control of his or her calendar to another user without sharing any passwords. This type of solution is encouraged. Passwords should not be shared even for the purpose of computer repair. An alternative to doing this is to create a new account with an appropriate level of access for the repair person.

- Change your password upon indication of compromise
  If you suspect someone has compromised your account, change your password immediately. Be sure to change your password from a computer you do not typically use (e.g. university cluster computer). After resetting your password, report the incident to your local departmental administrator and/or the Information Security Office at iso@aiu.edu.eg.

- Consider using a passphrase instead of a password
  A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember. For example, the passphrase "My passw0rd is $uper str0ng!" is 28 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary.

- Do not write your password down or store it in an insecure manner
  As a general rule, you should avoid writing down your password. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed. Using a password manager to store your passwords is not recommended unless the password manager leverages strong encryption and requires authentication prior to use.

- Avoid reusing a password
  When changing an account password, you should avoid reusing a previous password. If a user account was previously compromised, either knowingly or unknowingly, reusing a password could allow that user account to, once again, become compromised. Similarly, if a password was shared for some reason, reusing that password could allow someone unauthorized access to your account.

- Avoid using the same password for multiple accounts
  While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more sensitive accounts such as your Alamein International University account. These passwords should differ from the password you use for instant messaging, webmail and other web-based accounts.

- Do not use automatic logon functionality

Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

The following are Guidelines for individuals responsible for provisioning and support of user accounts:

- Enforce strong passwords

  Many systems and applications include functionality that prevents a user from setting a password that does not meet certain criteria. Functionality such as this should be leveraged to ensure only Strong Passwords are being set.

- Require a change of initial or "first-time" passwords

  Forcing a user to change their initial password helps ensure that only that user knows his or her password. Depending on what process is being used to create and distribute the password to the user, this practice can also help mitigate the risk of the initial password being guessed or intercepted during transmission to the user. This guidance also applies to situations where a password must be manually reset.

- Force expiration of initial or "first-time" passwords

  In certain situations, a user may be issued a new account and not access that account for a period of time. As mentioned previously, initial passwords have a higher risk of being guessed or intercepted depending on what process is being used to create and distribute passwords. Forcing an initial password to expire after a period of time (e.g. 72 hours) helps mitigate this risk.

- Always verify a user's identity before resetting a password

  A user's identity should always be validated prior to resetting a password. If the request is in-person, photo identification is a sufficient means of doing this. If the request is by phone, validating an identity is much more difficult. One method of doing this is to request a video conference with the user (e.g. Skype) to match the individual with their photo id. However, this can be a cumbersome process. Another option is to have the person's manager call and confirm the request. For obvious reasons, this would not work for student requests. If available, a self-service password reset solution that prompts a user with a series of customized questions is an effective approach to addressing password resets.

- Never ask for a user's password

  As stated above, individual user account passwords should not be shared for any reason. A natural correlation to this guidance is to never ask others for their passwords. Once again, delegation of permission is one alternative to asking a user for their password. Some applications include functionality that allows an administrator to impersonate another user, without entering that user's password, while still tying actions back to the administrator's user account. This is also an acceptable alternative. In computer repair situations, requesting that a user create a temporarily account on their system is one alternative.

The following are several additional Guidelines for individuals responsible for the design and implementation of systems and applications

- Change default account passwords

  Default accounts are often the source of unauthorized access by a malicious user. When possible, they should be disabled completely. If the account cannot be disabled, the default passwords should be changed immediately upon installation and configuration of the system or application.

- Implement strict controls for system-level and shared service account passwords

Shared service accounts typically provide an elevated level of access to a system. System-level accounts, such as root and Administrator, provide complete control over a system. This makes these types of accounts highly susceptible to malicious activity. As a result, a lengthier and more complex password should be implemented. System-level and shared service accounts are typically critical to the operation of a system or application. Because of this, these passwords are often known by more than one administrator. Passwords should be changed anytime someone with knowledge of the password changes job responsibilities or terminates employment. Use of accounts such as root and Administrator should also be limited as much as possible. Alternatives should be explored such as creating unique accounts for Windows administration instead of using default accounts.

- Do not use the same password for multiple administrator accounts
  Using the same password for multiple accounts can simplify administration of systems and applications. However, this practice can also have a chain effect allowing an attacker to break into multiple systems as a result of compromising a single account password.

- Do not allow passwords to be transmitted in plain-text
  Passwords transmitted in plain-text can be easily intercepted by someone with malicious intent. Protocols such as FTP, HTTP, SMTP and Telnet all natively transmit data (including your password) in plain-text. Secure alternatives include transmitting passwords via an encrypted tunnel (e.g. IPSec, SSH or SSL), using a one-way hash or implementing a ticket based authentication scheme. Contact the Information Security Office at iso@aiu.edu.eg if you would like an assessment of your application's authentication controls.

- Do not store passwords in easily reversible form
  Passwords should not be stored or transmitted using weak encryption or hashing algorithms. For example, the DES encryption algorithm and the MD-4 hash algorithm both have known security weaknesses that could allow protected data to be deciphered. Encryption algorithms such as 3DES or AES and hashing algorithms such as SHA-1 or SHA-256 are stronger alternatives to the previously mentioned algorithms. Contact the Information Security Office at iso@aiu.edu.eg if you have questions related to the use of a specific encryption and hashing algorithm.

- Implement automated notification of a password change or reset
  When a password is changed or reset, an email should be automatically sent to the owner of that user account. This provides a user with a confirmation that the change or reset was successful and also alerts a user if his or her password to unknowingly changed or reset.

The following are additional Guidelines for system or service accounts - those not designed to be used by humans:
Where possible, service accounts should be randomly generated, long (>= 15 characters), and follow the same complexity requirements for strong passwords above. The longer length mitigates weak encryption ciphers. If software compatibility requires setting a shorter password, please contact the Information Security Office iso@aiu.edu.eg to discuss compensating controls.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

- Acceptable Use of Technology Resources Policy
- Email Communication Policy
- Access Control Policy
- Remote Access Management Policy
- Internet Use Policy
- University Network Use Policy

VIV. CONTACT INFORMATION

- Information Security Office (ISO) iso@aiu.edu.eg

Triggered by:	Name	Date	Sig.
Created by:	Name	Date	Sig.
Revised by:	Name	Date	Sig.
Approved by:	Name	Date	Sig.