Access Control Policy
Arab Open University – Kingdom of Saudi Arabia

Article (1): Title

This policy shall be referred to as the "Access Control Policy at the Arab Open University."

Article (2): Definitions

- University: Arab Open University in the Kingdom of Saudi Arabia.
- President: The President of the Arab Open University in the Kingdom of Saudi Arabia.
- Asset Owner: An individual or group assigned by the University administration to maintain the confidentiality, security, and availability of information, including reviewing access rights and classifying assets.
- Assets: Information with value to the University, such as networks, devices, information, software, media, and information systems.

The terms and expressions used in this policy shall have the meanings assigned to them unless the context indicates otherwise.

Article (3): Introduction

The Arab Open University aims to ensure cybersecurity requirements related to the use of its systems and to document official procedures governing user access to the University's information and technical assets. The policy also seeks to prevent unauthorized individuals from accessing University systems to safeguard information.

This policy aligns with the cybersecurity requirements and controls issued by the National Cybersecurity Authority, in accordance with Control No. 2-2 of the Essential Cybersecurity Controls (ECC-1:2018).

The policy applies to all user identities and accounts from initial registration through to the revocation of access rights, as needed. It covers all users of the University's information assets and systems, including permanent and temporary administrative and academic staff.

Any violation of this policy shall subject the violator to disciplinary action in accordance with the established procedures of the Arab Open University.

Article (4): Policy Objectives

4-1 Regulate and manage account access based on business and security requirements.

4-2 Document official procedures for managing user access.

4-3 Protect the confidentiality, integrity, and availability of information stored on the University's network and systems.

Article (5): Access Control Policy Provisions

5-1 Creation, Modification, and Suspension of User Accounts

5-1-1 Each system user shall be assigned a unique username and specific access rights by the Asset Owner. Sharing usernames is strictly prohibited.

5-1-2 Each user shall be provided with login credentials, requiring at least one authentication factor (e.g., password, verification code).

5-1-3 Delegation, modification, or revocation of user access rights shall not occur without authorization from the competent authority.

5-1-4 The principle of separation of duties shall be applied when creating accounts and defining access rights.

5-1-5 User access rights shall adhere to the following principles:

- Need-to-know and need-to-use.
- Separation of duties.
- Principle of least privilege.

5-1-6 User access rights shall be revoked upon termination of their contract with the University (retirement, resignation, dismissal), effective on the last working day.

5-1-7 In cases where an employee is suspected of actions harmful to the University before or during termination, access rights shall be revoked prior to issuing the termination notice.

5-1-8 Access rights shall be updated if the user's assigned tasks change, ensuring alignment with their new duties.

5-2 User Password Management

5-2-1 Authentication via passwords shall be enabled for all University systems prior to granting access.

5-2-2 User accounts shall be disabled after three failed login attempts.

5-2-3 Passwords shall be changed if suspected of compromise,

5-2-4 Passwords shall be mandatorily changed at least every 180 days and must not repeat previous passwords.

5-2-5 Password resets must be processed by the IT Department after official verification of the user's identity if automatic recovery fails.

5-2-6 Passwords must comply with length and complexity requirements.

5-2-7 Passwords must remain confidential and never be disclosed (e.g., via phone, email, or written notes).

5-3 Privilege Management

5-3-1 Access to privileged accounts (e.g., system/network administrators) must be strictly controlled and authorized.

5-3-2 Privileged accounts shall only be used when necessary and not for routine tasks.

5-3-3 Users of privileged accounts must be trained before use.

5-3-4 Privileged account users must also have separate accounts for routine tasks.

5-3-5 Privileged account passwords must be protected and changed regularly.

5-4 Review of User Access Rights

5-4-1 The IT Department and Asset Owners must review user access rights annually.

5-4-2 Any misuse of access rights must result in restrictions on those rights.

Article (6): Exceptions

All University staff must adhere to this policy. Any exceptions require approval from the IT Department.

Article (7): Sanctions

Any violation of this policy shall subject the violator to disciplinary action in accordance with the established procedures of the Arab Open University.

Article (8): General Provisions

Cases not covered by this policy shall be referred by the IT Department to the University Council for resolution.