


King AbdulAziz University
Cyber-Security Center

Identity and Access Management Policy

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022 CE	

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	15/11/2021 CE	Shuruq bint Khalid Banafi	ISO27001
2.0	14/11/2022 CE	Daniyal ibn Muhammad al-Ghazzawi	In accordance with the requirements of the Authority

Table of Contents

<i>Objectives</i>	<i>4</i>
<i>Scope and Applicability of the Work.....</i>	<i>4</i>
<i>Policy Clauses</i>	<i>4</i>
<i>Roles and Responsibilities</i>	<i>8</i>
<i>Compliance with the Policy</i>	<i>9</i>

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, for identity and access management of informational and technical assets pertaining to King AbdulAziz University, so as to reduce cyber-risks and to protect the University from internal and external threats, through focus on the essential elements of protection, which are: Confidentiality, integrity, and availability of information.

This policy aims to comply with cyber-security requirements and the relevant legislative and regulatory requirements, which is itself a legislative requirement expressed in Control 2-2-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

This policy covers all King AbdulAziz University informational and technical assets, and applies to all King AbdulAziz University employees.

Policy Clauses

1– Identity and Access Management

1-1 Access Management

1-1-1 Access management procedures that clarify the mechanism for granting and revoking access and modification privileges to King AbdulAziz University informational and technical assets must be documented and approved. This mechanism must be monitored and its implementation ensured.

1-1-2 User identities must be established in accordance with the legislative and regulatory requirements pertinent to King AbdulAziz University.

1-1-3 Identity authentication and verification is required prior to granting users access privileges to informational and technical assets.

1-1-4 Documentation and approval of a matrix for managing user permissions and privileges on the basis of the following principles for controlling login and access is required:

1-1-4-1 The need-to-know and need-to-use principles.

1-1-4-2 The segregation of duties principle.

1-1-4-3 The least privilege principle.

1-1-5 Authentication and privileges controls must be applied to all King AbdulAziz University technical and informational assets through a central automated access control system, such as the Lightweight Directory Access Protocol (LDAP).

1-1-6 The use of generic user accounts to access King AbdulAziz University informational and technical assets is forbidden.

1-1-7 System settings must be configured to automatically close after a specified period of time (session timeout). (It is advised that the period not exceed 15 minutes).

1-1-8 Unused user accounts must be disabled after a specified period of time. (It is advised that the period not exceed 90 days).

1-1-9 The settings of all identity and access management systems must be configured to relay logs to a central logs and monitoring system, in accordance with the Cyber-Security Events Logs and Monitoring Policy.

1-1-10 Users must not be granted privileges to access or directly interact with databases pertaining to critical systems, which may only be done through applications, with the exception of database administrators. (CSCC-2-2-1-7)

1-1-11 Clear procedures for interacting with service accounts must be documented and approved, their secure management must be ensured between applications and systems, and interactive login through them must be disabled. (CSCC-2-2-1-7)

1-2 Granting Access Rights

1-2-1 Access Rights Requirements for User Accounts

1-2-1-1 Access privileges are granted at user request via a form, or via the system approved by the user's direct manager and the system owner, in which are specified the name of the system, the type of request, the privileges to be granted, and the period of their validity (in the event that the access privileges are time-bound).

1-2-1-2 Users are to be granted access privileges to King AbdulAziz University informational and technical assets in accordance with their roles and responsibilities.

1-2-1-3 A unified mechanism for establishing user identities must be employed, in such a way as to allow the tracking of activities performed using the user ID and the linking of those activities with the user, such as the formula <the initial letter of user's first name>.<user's last name>, or the employee number previously assigned by the General Office for Human Resources.

1-2-1-4 The ability of users to access multiple devices simultaneously (concurrent logins) must be disabled.

1-2-2 Access Rights Requirements for Important and Critical Accounts

In addition to the requirements mentioned in the Access Rights Requirements for User Accounts section, the controls explained below must be implemented for accounts that possess important and critical privileges:

1-2-2-1 The access rights possessed by the individual user must be specified for users requesting important and critical privileges (administrator privilege), and these rights must be granted based on their job tasks, taking into account the principle of segregation of duties.

1-2-2-2 Password history must be activated to track the number of passwords that have been changed.

1-2-2-3 The names of default accounts must be changed, especially for accounts possessing important and critical privileges, such as the "root", "admin", and "sys id" accounts.

1-2-2-4 The use of accounts possessing important and critical privileges for daily work activities is prohibited.

1-2-2-5 Verification of user accounts possessing important and critical privileges pertaining to technical and informational assets must be done via multi-factor authentication (MFA), using at least two of the following methods:

- Knowledge (something the user knows, such as a password).
- Possession (something only the user possesses, such as a temporary login program or device that generates a random number or short message, known as a “one-time password”).
- Inherent quality (A biological characteristic or quality pertaining only to the user, such as a fingerprint).

1-2-2-6 Access to critical systems and systems used to manage and monitor critical systems must require the use of multi-factor authentication (MFA) for all users.

1-2-3 Remote Access to King AbdulAziz University Networks

1-2-3-1 Remote access privileges to informational and technical assets are to be granted once prior permission has been obtained from the Cyber-Security Center, and such access must be restricted via multi-factor authentication (MFA).

1-2-3-2 Events logs pertaining to all private remote access sessions must be maintained and monitored according to the sensitivity of the informational and technical assets involved.

1-3 Revoking and Changing Access Rights

1-3-1 The Office for Human Resources must notify the Deanship of Information Technology to take the necessary actions in the event of user transfer or change of duties or the end/termination of the employment relationship between a user and King AbdulAziz University. The Deanship of Information Technology must terminate or modify users’ access privileges based on their new job tasks.

1-3-2 In the event that a user’s access privileges are terminated, it is forbidden to delete the events logs pertaining to the user, which must be maintained in accordance with the Cyber-Security Events Logs and Management Policy.

2– Identity and Access Review

2-1 User IDs must be reviewed, and access privileges to informational and technical assets must be verified, according to user job tasks, based on the principle of controlling access and privileges, on a periodic basis. User access IDs for system systems must be reviewed at least once every three months.

2-2 User profiles pertaining to informational and technical assets must be reviewed, based on the principle of controlling access and privileges, on a periodic basis. User profiles pertaining to critical systems must be reviewed at least once a year.

2-3 All login attempts, whether failed or successful, must be logged, documented, and reviewed periodically.

3– Password Management

3-1 A secure password policy with high standards must be implemented for all King AbdulAziz University accounts. The table below includes examples of the password controls for each type of user:

Password Controls	All Users	Privileged Users	Service Accounts
Minimum number of password characters	Eight numbers, letters, or special characters	12 numbers, letters, or special characters	Eight numbers, letters, or special characters
Password log	Recalls five passwords	Recalls five passwords	Recalls five passwords
Maximum password life	120 days	120 days	120 days
Password complexity	Enabled	Enabled	Enabled
Example of password complexity	D_dyW5\$_	R@rS%7qY#blu	r?M4d5V=
Duration of account closure	30 minutes or until the system unlocks	30 minutes or until the system unlocks	30 minutes or until the system unlocks
Account closure limit	Five unsuccessful login attempts	Five unsuccessful login attempts	No attempts exist/not applicable
Account closure timer reset period	30 minutes (administrator may lift account closure manually)	30 minutes (administrator may lift account closure manually)	Not applicable
Use of multi-factor authentication	Enabled for remote access only	Enabled	Not enabled

3-2 Password Standards

3-2-1 Passwords must include at least eight (8) characters.

3-2-2 Passwords must be complex, containing at least three of the following characters:

3-2-2-1 Upper case letters.

3-2-2-2 Lower case letters.

3-2-2-3 Numbers (12345).

3-2-2-4 Special characters (@*%#).

3-2-3 Users must be notified prior to the expiration of their passwords, so as to remind them to change the password before it expires.

3-2-4 The settings of all informational and technical assets must be configured to require the changing of temporary passwords when users log in for the first time.

3-2-5 All default passwords for all informational and technical assets must be changed before they are installed in the production environment.

3-2-6 Default community string passwords (such as “public”, “private”, and “system”) pertaining to the Simple Network Management Protocol (SNMP) must be changed, and must be different from the passwords used for logging in to specific technical assets.

3-3 Password Protection

3-3-1 All passwords for King AbdulAziz University informational and technical assets must be encrypted in an unreadable format during login, transmission, and storage, in accordance with the Cryptography Policy.

3-3-2 Passwords must be masked as they are entered onto the login screen.

3-3-3 The “remember password” feature must be disabled on King AbdulAziz University systems and applications.

3-3-4 Use of well-known (dictionary) words in their usual forms for passwords is prohibited.

3-3-5 User passwords must be transmitted in a secure and reliable manner.

3-3-6 When a user requests to reset his password using a phone, the Internet, or any other medium, his identity must be verified before the password is reset.

3-3-7 Passwords for accounts with important and critical privileges must be stored securely in an appropriate place (inside a sealed envelope in a safe), or techniques for preserving and managing important and critical privileges (privileged access management solutions) must be used.

4– Other Requirements

4-1 Key Performance Indicators (KPI) must be employed to ensure the continual development of identity and access management.

4-2 The implementation of cyber-security requirements pertaining to identity and access management must be reviewed periodically.

4-3 This policy must be reviewed yearly, at least, or in the event that changes are made to the relevant legislative or regulatory requirements or standards.

Roles and Responsibilities

–Responsible Party and Owner of the Document: Director of the Cyber-Security Center.

–Updating and Review of the Document: The Cyber-Security Center.

–Implementation and Application of the Document: The Deanship of Information Technology, the Cyber-Security Center, and the General Office for Human Resources.

Compliance with the Policy

1– The Director of the Cyber-Security Center must ensure the compliance of King AbdulAziz University with this policy periodically.

2– All employees of King AbdulAziz University must comply with this policy.

3– Any violation of this policy may subject the offender to disciplinary action, in accordance with the procedures followed by King AbdulAziz University.