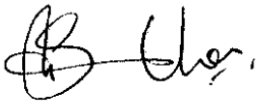
Aga Khan University Hospital

Document Title:	Password Policy		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		Document Reference / Policy No.:	ADM-P-005
Chief Information Officer		Issuance Date:	01 February 2015
		Revision Date:	25 May 2024
		Revision No.:	4.0
		Number of Pages:	3

1.0 **Policy Statement**: This document delineates AKU's policy on passwords, emphasizing their critical role in information security. This policy also defines expected user behaviors, mandating adherence to guidelines for selecting and securing passwords when using AKU ICT resources.

2.0 **Terms and Definitions**: No specific terms or definitions required for this document.

3.0 **Purpose**: The intent of this document is to ensure security of information assets and access control for the rightful users.

4.0 **Scope**: This policy is applicable to all AKU users. This includes all students, faculty members, employees, trainees, and consultants/volunteers.

5.0 **Responsibilities**: The users need to be aware of this policy, their responsibilities, and legal obligations. All users are required to comply with this policy, in order to protect themselves and the institution from any legal action.

6.0 **Process / Procedure / Policy Content:**

6.1. All AKU owned electronic devices must have password protection enabled.

6.2. Sharing or allowing another person to use an individual account password is a violation of this policy. Departmental account passwords should be shared only with appropriately designated departmental personnel.

6.3. User credentials should not be shared through written communication. In case it is inevitable to do so separate mediums or emails should be used.

6.4. The ICT department will never request a password via phone or email.

6.5. User IDs and passwords may only be shared by a group of employees for generic accounts including but not limited to collection points, department specific accounts and wireless access network for guests and for publicly accessible computer systems such as those connected to projectors in meeting rooms.

6.6. Passwords that provide access to University's confidential resources must not be stored on personal computers and must not be displayed on sticky notes or scraps of paper on or by computers.

6.7. If necessary, personal assistants and secretaries to executives may be permitted to send emails on behalf of their supervisor.

6.8. Passwords should be 8 or more characters long, and include alphabets numbers, and punctuation characters. They should not be names, or permutations of personal data (birth dates, anniversaries, etc.).

6.9. All passwords must be changed at least every three months (90 days).

6.10. An exception to this is for service accounts where passwords are set as never expiry by design. Different services are configured to run through these accounts and a password expiry can result in service interruptions.

6.11. User accounts must be locked after five (5) unsuccessful login attempts.

6.12. Password reuse is not encouraged. Restrictions should be implemented where permissible in the system.

6.13. Remote access to privileged accounts (e.g., root, enable, Windows admin, application administration accounts, etc.) must not be attempted from insecure locations e.g., open access cluster systems or public terminals.

6.14. All default passwords shall be changed to meet the current password requirements. No default passwords shall remain in effect after the required initial usage. Default passwords are those that are vendor supplied with hardware or software, or are system generated.

7.0 Disciplinary Actions:

7.1. The failure by the users to comply with this policy may result in loss of access to some or all of ICT resources and/or loss of access privileges to ICT resources. In addition, violators of these policies may be subject to disciplinary action, up to and including termination.

8.0 Compliance Reference: None

9.0 Measures of Compliance: None

10.0 Reference: No Specific references provided

11.0 Related Institutional Documents: No related documents applicable

12.0 Annexure: No additional documents provided

13.0 Author(s): Shumail Khalid, Senior Manager Service Delivery

14.0 Key Searchable Terms: Password

15.0 Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change
04	25-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-