Policy Name	**Password Policy**
Policy Number	**AKU-K/ICT/002**
Approved by	**Academic Council**
Date of Original Approval	**1st February 2015**
Date of revisions	**Revision Date: 10th April 2020**
Contact	**Office of the Registrar**

1.0 Preamble

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or compromise of the entire AKU network. All users with access to AKU systems and networks are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Organizational Scope

This policy is applicable to all users of AKU's IT facilities. This includes all students, faculty members, employees and other staff (the users). They 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 AKU from any legal actions.

3.0 Policy Content

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

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

3.3 Passwords should never be shared via e-mail, chat or other electronic written communication. The IT (Information Technology) department will never request a user name or password by e-mail.

3.4 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.

3.5 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.

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

3.7 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.).

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

3.8.1 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.

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

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

3.8.4 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.

3.8.5 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.

3.8.6 All other exceptions to the above stated clauses must be approved by the management and recorded.

4.0 Disciplinary Actions

1.1. The failure by the users to comply with these Policies may result in loss of access to some or all of IT Resources and/or loss of access privileges to IT Resources. In addition, violators of these Policies may be subject to disciplinary action, up to and including termination.