PASSWORD POLICY

Document ID: AUD/IT/Policy/03
Version No: 1.0
Release Date:
Document Classification: Internal

55

Document Release Note & Control Sheet

Document History					
Ver. No.	**Revision date**	**Description of Change**	**Authored / Revised by**	**Reviewed By**	**Approved By**
1.0	01.08.2019	Initial version	IT Services	IT Policy Review Committee	Vice Chancellor, AUD

1.0 POLICY:

The Objective of this policy is to ensure users have credentials (username and password) to access the authorized IT services to their work area.

2.0 PURPOSE:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords in the University.

3.0 ABBREVIATIONS:

IT: Information Technology

AUD : Ambedkar University Delhi

4.0 SCOPE:

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the AUD domain. These include Students, Faculty and Staff member of the University. The requirements in this standard apply to passwords for any computing account on any university computer resource, to the users of any such accounts, and to system administrators and developers who manage or design systems that require passwords for authentication.

5.0 RESPONSIBILITY:

IT Services Divison, End Users of IT Services

6.0 DISTRIBUTION:

University Wide Internally

53|c

7.0 PROCESS DETAILS:

7.1 DEFINITION:

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.

7.2 USER ACCOUNTS AND PASSWORDS

a) For users having accounts for accessing systems/services. Users shall be responsible for all activity performed with their official user IDs. Users are advised not to share their own credentials with others to access any of the IT services.

b) The active directory passwords to access desktop / laptop / network is required to be changed periodically (at least once every three months).

c) Password may be enforced to be of a minimum length and comprising of mix of alphabets, numbers and special characters.

d) Passwords shall not be stored in readable form (plain text) in batch files, automatic logon scripts, in computers without access control, or in any other location where unauthorized persons might discover or use them.

e) All access codes including user ID passwords, network passwords, PINs (if any) etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.

f) Passwords must not be communicated through email messages or other forms of electronic communication such as phone to anyone.

g) Passwords shall not be revealed on questionnaires or security forms.

h) Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.

i) It is advised that the "Remember Password" feature of applications is not used.

j) It is preferred that the credentials which are created for the first time login, should force changing of password by the end user.

k) The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

l) For Password Change Control, both the old and new passwords are required to be given whenever a password change is required, wherever technically feasible.

   I. **Policy for constructing a password**: All equipment passwords are required to be kept complex by IT services division for critical server room devices. It is recommended that critical equipment passwords shall be a combination of characters, integers, special characters etc.