THE AMERICAN UNIVERSITY of PARIS 55 YEARS

PASSWORD MANAGEMENT

Policy Number: IT004EN
Last Review: July 2019

1. PURPOSE
Passwords are an important aspect of computer security. They are the front line of protection for user accounts and ultimately for AUP's computer systems. A poorly chosen password can compromise the security and integrity of AUP's network and result in unauthorized access to confidential data. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of changing these passwords.

2. WHO IS AFFECTED BY THIS POLICY
Anyone (students, faculty, staff, administrators, guests, volunteers, vendors, contractors, temporary workers, alumni, etc.) who has access to the AUP network and/or has been granted or is responsible for an account (or any form of access that supports or requires a password).

3. POLICY STATEMENT
All AUP faculty, students, staff, and administrators (including contractors, guests, volunteers and vendors with access to AUP systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. It is important to set a strong password and change it regularly.

1. As a general rule of thumb, change your password every 90 days.

2. A strong password consists of:
    - A minimum of eight characters
    - A mix of upper and lower case letters
    - At least one numeric, and
    - At least one special character
    - See Password Chart below for further details
    - A suggestion is to create a strong password phrase and then develop your password for it. This might be easier than trying to remember a random combination of characters. Remember, however, to use special characters as well.

3. Password Best Practices:
    - Do not reveal a password over the phone to anyone.
    - Do not reveal a password in an email message without encryption.
    - Do not reveal a password to your boss or administrative assistant.
    - Do not talk about a password in front of others.
    - Do not hint at the format of a password.
    - Do not use passwords that could be easily identifiable or easy for someone to guess such as your name or school name.
    - Do not use dictionary words in any language.
    - Do not reuse old passwords.
    - Do not reveal a password on questionnaires or security forms.
    - Do not share a password to co-workers while on vacation.
    - Do not write down a password and store it in an easily accessible location, i.e. under your keyboard.
    - Do report to the ITS Help Desk immediately if you suspect that your user account or password has been compromised.

4. Password Expiration
Changing passwords regularly is an important security measure. Network account passwords are configured to expire six months after they were last changed. Users are thus required to change their passwords at least every six months, to avoid losing access to their accounts. Users receive notifications prior to password expiry.

5. Password Chart:

Password Properties	Applicants, Current Students, Staff	Alumni
Password Expiration (days)	90	180
Minimum length (characters)	8	8
Account Locking / Failed Logins	5	5
Password History	2	2
Password Grace Period (days)	None	None
Account Inactivity Locking	After 6 months	After 6 months
Minimum password complexity	Password must contain three of the following four categories: - Upper Alpha (A-Z) - Lower Alpha (a-z) - Numeric (123…) - Special character (ex: !, ^, *, %, +, ?, -). Note that not all symbols are allowed	

6. Password Standards for Administrators and for Users of Enterprise Systems

Additional password standards apply to users with administrator privileges (such as Domain Administrators and campus-wide machine Local Administrators), and to users whose accounts grant them back-end or administrative access to Enterprise Systems (including but not limited to AUP's Student Information System and the Accounting, Finance and Human Resources systems).

- All system level passwords (e.g. root, Windows Administrator, application administration accounts, etc.) are changed every 90 days.
- Default passwords are not used.
- Where SNMP is used, the community string must be defined as something other than the standard defaults of "public", "private", and "system" and must be different from the passwords used to log in interactively.
- Passwords are at least eight characters in length.
- Passwords contain at least three of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - Special characters (e.g. @#$%^&, etc.)

4. RESPONSIBILITIES

The Director of Information Technology Services is responsible for the interpretation, administration, and enforcement of this policy. Individuals are responsible for setting their own passwords according to the policy.

5. DEFINITIONS

AUP The American University of Paris

ITS Information Technology Services

6. APPROVALS & HISTORY

January 29, 2019	Approved by the Leadership Team.
July 2019	Updates to Password Chart.
November 1, 2022	Next review.

7. ISSUING OFFICE AND CONTACT

Director of Information Technology Services
69 Quai d'Orsay
75007 Paris
+33 1 40 62 06 96
helpdesk@aup.edu