**Contact Person**

Ghassan Hitti  
Chief Information Security Officer  
American University of Beirut  

[ghassan.hitti@aub.edu.lb](mailto:ghassan.hitti@aub.edu.lb) | +961-1-350-000 ext. 2247 | +961-71-079939

---

**Note:** When this document is released, it is to be followed and adhered to, and is subject to document AUB-IT-000001 “IT Document Control Policy”.
TABLE OF CONTENTS

1. PURPOSE 3
2. SCOPE 3
3. INTRODUCTION 3
4. DEFINITIONS 3
   4.1. Identification 3
   4.2. Authentication 3
   4.3. Authenticator 3
5. AUTHENTICATION SECURITY LEVELS 4
6. AUTHENTICATION MECHANISM FOR STANDARD AUTHENTICATION 4
7. REINFORCED STATIC PASSWORD 4
   7.1. Definition Rules 4
   7.2. Management 5
   7.3. Protection Guidelines 6
   7.4. Creation and Modification 7
8. VIOLATION OF THIS POLICY 7
9. AUTHORING HISTORY 9
1. Purpose

The purpose of this policy is to protect American University of Beirut (AUB) confidential data through the proper identification of users and their authentication on relevant systems.

2. Scope

The scope of this policy includes all persons with any type of account access (e.g., passwords) to any AUB Information System, including the AUB network, and internal, restricted, or confidential AUB information.

3. Introduction

This System Authentication Policy is part of the documentation of the American University of Beirut (AUB) security policies. This document describes the rules for authenticating user identities (i.e., physical persons) to access the AUB information technology (IT) assets.

4. Definitions

4.1. Identification

Identification is an operation that determines the identity of a user, a user group, or a service. The identifier is the information that allows identification. Every physical person in the scope of this policy has at least one identifier. The identifier does not change throughout the user’s lifetime.

4.2. Authentication

Authentication is an operation that ensures, without ambiguity, the reality of identification. Its main goal is to prevent identity theft and/or to draw attention to any attempt at identity theft. Once the authentication is carried out, the authorization control mechanisms can be implemented, for which a successful authentication is a prerequisite and necessary.

4.3. Authenticator

The authenticator is the personal information that is known only by one person and by the information system. The authenticator makes it possible to authenticate the identity of the person. For example, a password is an authenticator.
5. Authentication Security Levels

Authentication is bound to three (3) security levels including Low, Standard, and High. The assignment of the security level correlates with the security criticality of the assets being accessed. In turn, security criticality is defined in terms of Confidentiality and Auditability.

The following Confidentiality-related rules apply:

- If confidentiality of the asset is described as Secret, then the authentication security level must be, at a minimum, High.
- If confidentiality of the asset is described as Internal, Restricted, or Confidential, then the authentication security level must be, at a minimum, Standard.
- If confidentiality of the asset is described as Public, then the authentication security level is Low or Is Not Subject to Authentication.

The following Auditability-related rules apply:

- If auditability of the asset requires Simple or Detailed Tracking, then the authentication security level must be, at a minimum, Standard.
- If auditability of the asset does not require any tracking, then no authentication is required.

6. Authentication Mechanism for Standard Authentication

- A fixed password linked to an identifier; and
- Used by a system or an application that complies with the rules of the reinforced static password.

7. Reinforced Static Password

7.1. Definition Rules

The following rules apply when defining a reinforced static password:

- Minimum password length is eight (8) characters
- Password includes two (2) or more numerical digits (i.e., [0-90])
- Password includes two (2) or more special characters (i.e., $ & @ # % * ~ ` ^ ? ! ; , . ) > < + = - _ { } [ ] \ /)
• Password includes one or more uppercase letters

The following additional rules apply:

• Password does not include common words found in English and non-English dictionaries, including slang, dialect, and jargon.
• Password does not include surnames, first names, and dates of birth of people as well as any information that may be easily associated with the user (e.g., telephone number, ID number, or address)
• Password does not include the user or machine name
• Password does not include familiar names (e.g., colleagues, family, friends, pets, and more)
• Password does not include words related to companies, computer lingo and terms, websites, software and/or hardware
• Password does not include the words “AUB”, “AUBMC”, “Beirut”, “Lebanon”, and/or any derivation
• Password does not include character and/or number patterns (e.g., azerty, qwerty, eeerrr, 123321, or more)

7.2. Management

• Passwords are personal and classified as Confidential; they should never be shared
• The use of a password is the responsibility of the person it was assigned to
• The password is to be changed and managed privately by the person it was assigned to
• The password must be entered discretely
• The password must be changed every ninety (90) days
• The password must be encrypted when stored and transferred on the AUB network
• Automatic mechanism for password management (controls, validity periods, monitoring violations) must be implemented.
• Any account must be automatically temporarily locked for at least ten (10) minutes if more than three (3) repeated failed login attempts occur. The User Accounts IT Administrator is notified when such a lock occurs.
- Passwords must be protected against any automatic information backup recovery mechanism, e.g. keylogger.

- The Information Security Team (IST) from the Office of Information Technology may attempt to breach user passwords to validate the effectiveness of the chosen password. If a password is identified, then the password owner is notified and is required to change the former.

- End of validity period: the authentication mechanism must be obligatorily invalidated as soon as possible after the user leaves their function and there is no longer need for the authenticators. The invalidation procedures are indicated in the document “Security requirements for people leaving AUB”, which concerns any physical and logistical elements (recovery, invalidation, archiving, etc.) related to AUB departures.

### 7.3. Protection Guidelines

All AUB staff and students, including contractors and vendors with access to AUB systems, are responsible for taking the appropriate steps, as outlined below, to secure their passwords:

- Do not type in passwords in emails or other electronic (e.g., questionnaires and security forms) and non-electronic (e.g., over the phone) communication forms.

- Do not use the same passwords for AUB and non-AUB accounts (e.g., ISP account, emails, games, social networking, etc.).

- Do not share or reveal passwords. This includes assistants, helpdesk support, managers, family, colleagues, etc. Passwords are confidential and must be treated as such.

- Do not share passwords with co-workers who will replace you during a leave.

- Do not share or reveal password formats to anyone (e.g., “a combination of my family name and a website name”).

- Do not use the “Remember Password” feature hosted by some software applications (e.g., Internet Browsers or Microsoft Outlook).

- Do not write passwords on notepads and papers and store the latter in your office.

- If you keep passwords saved in a file on a computer, mobile phone, or similar, then make sure that the file is encrypted.
• If you suspect your or any other account or password is compromised, then report this to the Office of Information Technology and change your passwords immediately. If anyone requests your passwords, reference this Policy and/or have them communicate with the Office of Information Technology.

7.4. Creation and Modification

• The initially-generated password must not be generic, that is, it must not be associated with easily determined patterns (e.g., username followed by sign up date).

• The initially-generated password must be changed by the user on first system access. The user must not be allowed to proceed before changing the initially-generated password.

• The initially-generated password must be communicated to the requestor confidentially, as per the below:
  
  o Face to face if the two people know each other;

  o Face to face by verification of the user’s identity. The administrator can either use a badge with a photo or an official identify card for this verification process;

  o Remotely by sending an electronically signed message from the email box of the person requesting the password change. A response to this email will be returned in the same manner, signed and encoded.

8. Violation of this Policy

All users are advised that, in addition to being a violation of University rules, certain computer misconduct is prohibited under Lebanese laws and is therefore, subject to criminal penalties. Such misconduct includes gaining unauthorized access to controlled documents by breaking through a security measure, falsely obtaining electronic services or data, destroying of electronically processed, stored, or in-transit data, and using the Internet or an information technology device to threaten or blackmail another to act or not.

Any violation of this policy or applicable Lebanese laws will be subject to investigation and/or disciplinary action, up to and including termination of studies and referral to the appropriate law enforcement authorities in the appropriate cases. Any faculty, staff, students, and other authorized individuals breaching this policy are subject to disciplinary action which may result in employment termination. Questions concerning any aspect of this policy should be directed to the Office of Information Technology.
Office of Information Technology reserves the right to take appropriate action at any time to maintain and protect the confidentiality and integrity of the University’s documents.
9. Authoring History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date (DD-MM-YYYY)</th>
<th>Author</th>
<th>Reason for Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>17-06-2012</td>
<td>Ghassan Hitti</td>
<td>Initial document authoring</td>
</tr>
<tr>
<td></td>
<td>22-10-2012</td>
<td>Joe Hage</td>
<td>Updated Doc ID and Cover Page date</td>
</tr>
<tr>
<td>1.1</td>
<td>07-12-2012</td>
<td>Sharif Shahine</td>
<td>Update content</td>
</tr>
</tbody>
</table>