
 جامعة الإمارات العربية المتحدة United Arab Emirates University  	<b>Information Technology Policies Manual</b>	Policy Number	IT-07
		Effective Date	02-Mar-2014
	<b>Subject</b> Password	Most Recent Review Date	01-Dec-2013
	<i>Responsible Office:</i> Chief Information Officer	Due Date for Next Review	01-Sep-2016
		Pages of this Policy	1 of 1

## 7. Password

### Overview

Provides standards for defining passwords for UAEU applications.

### Scope


Applies to all personnel who have, or are responsible for, an account or any form of access that supports or requires a password. This includes any system that resides at UAEU, has access to UAEU network, or stores any non-public UAEU information.

### Objective

Effective password management will protect UAEU data and reduce the risk of unauthorized applications access. The policy is to establish a secure information technology environment by enforcing the use of strong passwords.

### Policy

1. Passwords are an important aspect of computer security. These are the front line of protection for user accounts. A poorly chosen password may result in the compromise of UAEU's entire network.
2. All UAEU faculty members, staff members, students, alumni, and contractors are responsible for taking the appropriate steps to select and secure their passwords.
3. All system passwords must be kept and maintained in a predefined secure location.
4. All passwords are to be treated as sensitive and confidential UAEU information.
5. The password policy is enforced by default.

 <b>UAEU</b>	<b>Information Technology Procedures Manual</b>	Related Policy	IT-07
		Effective Date	01-Sep-2014
	<b>Subject</b> Password	Most Recent Review Date	01-Dec-2013
		Due Date for Next Review	01-Sep-2016
<b>Responsible Office:</b> Chief Information Officer		Pages of these Procedures	1 of 1

## Procedures of Policy No. (7) - Password

1. When a password reset request is made by the user, a valid verification is required.
2. All user and system-level passwords must conform to the standards described below.
3. Users should communicate with the IT Helpdesk to unlock their accounts.

Setting	Description	User Configured Setting	Admin Configured Setting
Minimum Password Length	Defines the minimum number of characters a password can contain.	8	8
Maximum Password Age in Days	The period of time a password can be used before the system forces the user to change it. The value can be between 1 and 999 days. A value of 0 means that the password will never expire. A password that never expires is a security risk as it can be compromised over time.	90 days	90 days
Password History Size	Determines whether old passwords can be reused. It is the number of new passwords that must be used by a user account before an old password can be reused.	6	6
Password complexity	Passwords must contain the following four (4) classes: <ul style="list-style-type: none"> <li>▪ English Upper Case Letters (A, B, C, ... Z)</li> <li>▪ English Lower Case Letters (a, b, c, ... z)</li> <li>▪ Numeric Numerals (0, 1, 2, ... 9)</li> <li>▪ Special characters (., !()": %#@*^)</li> </ul>	Enabled	Enabled
Lockout Threshold	Indicates the number of failed log-on attempts for a user account before the account is locked out.	5	3
Lockout Duration	Lockout duration required for locked accounts to be unlocked.	30 min	15 min
Password Reset	Enforce change password on next log-on for password reset or new accounts passwords.	Enable	Enable