AUB Password Standard and Guidelines

Version: V1-2017

Password Security Setting	Students	Faculty, Staff, Sponsored, and Other Accounts	Alumni Accounts
		Other accounts are the accounts that do not classify under any of the other user classes.	To be applied on Alumni users.
Minimum password length	8	8	8
Password Complexity Set of rules that forces the user to formulate a strong password	AD Complexity Rules In order to meet the password complexity requirement, passwords must contain characters from (for example) at least three (3) of the following four (4) classes: • English Upper Case Letters (A, B, C, ... Z) • English Lower Case Letters (a, b, c, ... z) • Westernized Arabic Numerals (0, 1, 2, ... 9) • Non-alphanumeric ("Special characters") (E.g., punctuation symbols)	AD Complexity Rules In order to meet the password complexity requirement, passwords must contain characters from (for example) at least three (3) of the following four (4) classes: • English Upper Case Letters (A, B, C, ... Z) • English Lower Case Letters (a, b, c, ... z) • Westernized Arabic Numerals (0, 1, 2, ... 9) • Non-alphanumeric ("Special characters") (E.g., punctuation symbols)	AD Complexity Rules In order to meet the password complexity requirement, passwords must contain characters from (for example) at least three (3) of the following four (4) classes: • English Upper Case Letters (A, B, C, ... Z) • English Lower Case Letters (a, b, c, ... z) • Westernized Arabic Numerals (0, 1, 2, ... 9) • Non-alphanumeric ("Special characters") (E.g., punctuation symbols)
Password Lifetime The period of time a password can be used before the system forces the user to change it	180 days (6 Months)	180 days (6 Months)	unlimited
Account Lockout Number of failed authentication attempts before an account is locked out	No Lockout	Threshold: 50 times Lockout Duration: 5 Mins Reset account lockout counter after:1 Mins	No Lockout
Password Reuse History: Determines how often old passwords could be reused. **Controlled by two variables:** - Number of Old Passwords - Time to Use an Old Password	#of old Pass=6 Passwords Time to use old Pass=0 days	#of old Pass=6 Passwords Time to use old Pass=0 days	#of old Pass=6 Passwords Time to use old Pass=0 days
Inactive Accounts Lockout Number of days an account is allowed to be inactive before it is locked by the system	1 Year	1 Year	No Inactive Accounts Lockout
Password Storage and Transfer Security	Hashed at Storage/Encrypted at Transfer	Hashed at Storage/Encrypted at Transfer	Hashed at Storage/Encrypted at Transfer
Second Factor	NO	NO	NO
Dictionary check	NO	NO	NO

Password Security Setting	Privileged Accounts	Service Accounts
	To be applied on users having elevated privileges.	To be applied on accounts running batch jobs and services + Privileged
Minimum password length	14	14
Password Complexity Set of rules that forces the user to formulate a strong password	AD Complexity Rules In order to meet the password complexity requirement, passwords must contain characters from (for example) at least three (3) of the following four (4) classes: • English Upper Case Letters (A, B, C, ... Z) • English Lower Case Letters (a, b, c, ... z) • Westernized Arabic Numerals (0, 1, 2, ... 9) • Non-alphanumeric ("Special characters") (E.g., punctuation symbols)	AD Complexity Rules In order to meet the password complexity requirement, passwords must contain characters from (for example) at least three (3) of the following four (4) classes: • English Upper Case Letters (A, B, C, ... Z) • English Lower Case Letters (a, b, c, ... z) • Westernized Arabic Numerals (0, 1, 2, ... 9) • Non-alphanumeric ("Special characters") (E.g., punctuation symbols)
Password Lifetime The period of time a password can be used before the system forces the user to change it	180 days (6 Months) (This is the only variable change done to compensate the change in lockout policy)	1 Year (Soft Limit for Service Accounts)
Account Lockout Number of failed authentication attempts before an account is locked out	Threshold: 50 times Lockout Duration: 5 Mins Reset account lockout counter after:1 Mins	No Lockout
Password Reuse History: Determines how often old passwords could be reused. **Controlled by two variables:** - Number of Old Passwords - Time to Use an Old Password	#of old Pass=6 Passwords Time to use old Pass=0 days	#of old Pass=6 Passwords Time to use old Pass=0 days
Inactive Accounts Lockout Number of days an account is allowed to be inactive before it is locked by the system	1 Year	1 Year
Password Storage and Transfer Security	Hashed at Storage/Encrypted at Transfer	Hashed at Storage/Encrypted at Transfer
Second Factor	NO	NO
Dictionary check	NO	NO

Security Controls to be implemented along with the Password Settings

Technical Controls
Notify the User at Failed Logins
Alert User after multiple lockouts
Alert admin upon Excessive login Failure
Notify the Users of logins activities from new machines
Monitor Abnormal Account Activities
Awareness Campaign

PASSWORD PROTECTION GUIDELINES

Outlined below are security guidelines recommended by AUB to protect your password:

- Passwords must not be included 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 sharing passwords with 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.
- Authentication devices should be kept with owners at all times and or stored in secure location

AUTHORING HISTORY

Original Issue Date: V1 - 28-Feb-2017

Contact Person: Ghassan Salem - Senior Information Security Engineer, gs37@aub.edu.lb or it.security@aub.edu.lb