COMPUTER & INFORMATION TECHNOLOGY CENTER

Password Policy

Document Controls

This document is reviewed every six months

Document Reference	PAAET-PLCY-Password Policy
Document Title	Password Policy
Document Owner	Abdullah AlDousari
ISO 27001:2013 reference	A.9.4.3 – Password Management System A.9.4.2 – Secure log-on procedures A.9.2.4 – Management of secret authentication information of users.
Security Classification	Internal – Restricted
Stored	http://sp13.paaet.edu/sites/TecDep
Next Review Date	20th January 2017
Document Status	Final

Document Review and Approval History

Date	Version	Amended by	Reviewer / Approver	Remarks	RFC#
1st May, 2016	Draft v1.0	Reena Varghese			
19th May 2016	Draft v1.1	Reena Varghese	Jessy Sakariah	Updated based on reviewer comments	
16th June 2016	Draft v1.2	Abdullah AlDousari		Edited	
19th July 2016	Final v1.3	Rabie Al-Mejbas		Edited	

Document Distribution List

Sl.No.	Name and Department	Purpose
1	Dr. Jasem AlOstad, CIC Manager	For feedback
2	Ali Hussain, Technical Support Supervisor	Distribution to concerned staff responsible for creating maintaining and troubleshooting PC and Network problems.
3	Ammal AlQattan, PC & Servers section Head.	For her information
4	ISO team : • Rabie Al-Mejbas • Rajiv Prakash • Nadia AL Saleh • Shaikha AL Barak • Mai AlAbdulqader	Be aware of this policy start enforce it.
5	All CIC systems and servers administrators (Windows, PCs, Exchange, etc.	Apply passwords requirements to all systems and servers login

CONTENTS

CONFIDENTIALITY STATEMENT

This document includes confidential information related to the Computer and Information Technology Center (**CIC**) at the Public Authority for Applied Education and Training (**PAAET**), shall not be distributed to any persons other than those mentioned in the distribution list herein, and shall be used solely for **CIC'**s internal purpose.

1.0 INTRODUCTION

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of PAAET entire network. As such as all employees including contractors and vendors with access to systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 PURPOSE

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 change.

3.0 SCOPE

The requirements in this standard apply to passwords for any computing account on any PAAET computer resource, to the users of any such accounts, and to system administrators who manage or design systems that require passwords for authentication.

4.0 STANDARD

4.1. PASSWORD CONSTRUCTION

4.1.1 MINIMUM PASSWORD LENGTH

Passwords shall have a minimum of eight characters with a mix of alphanumeric and special characters; if a particular system will not support eight character passwords, then the maximum number of characters allowed by that system shall be used.

4.1.2 PASSWORD COMPOSITION

Passwords shall not be composed of one or more dictionary words in any language. Passwords shall not consist of well-known or publicly posted identification information.

4.2. PASSWORD MANAGEMENT

4.1.3 PASSWORD STORAGE

Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames.

Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.

4.1.4 PASSWORD AGING

Users must change their passwords before 120 days with the new password.

4.1.5 PASSWORD REUSE

Care shall be taken to prevent the compromise on the security of multiple systems or resources while using the same username and password for the access. This is a guideline to staff/users that one should not use the same matching password in various systems. If the password is hacked into, the security compromise is extensive.

4.1.6 PASSWORD SHARING AND TRANSFER

Passwords shall not be transferred or shared with others unless the user obtains appropriate authorization to do so. When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record. When communicating a password to an authorized individual orally, take measures to ensure that the password is not overheard by unauthorized individuals.

4.1.7 ELECTRONIC TRANSMISSION

Passwords shall not be transferred electronically over the Internet using insecure methods. Wherever possible, security protocols including IMAPS, FTPS, HTTPS, etc. shall be used.

5.0 REQUIREMENTS FOR SYSTEM ADMINISTRATORS

5.1. REQUIRE PASSWORDS FOR LOGIN

Systems shall not be configured to allow user login without a password.

5.2. PROTECT AGAINST PASSWORD HACKING

System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate “brute force” password attacks. For example, some systems will lock an account for a few minutes after several failed login attempts, or detect where the attack is coming from and block further attempts from that location.

5.3. CHANGING PASSWORD AFTER COMPROMISE OR DISCLOSURE

Systems administrators shall, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource. Examples of these situations include, but are not limited to, disclosure of a password to an unauthorized person; discovery of a password by unauthorized person; system compromise (unauthorized access to a system or account); insecure transmission of a password; replacing the user of an account with another individual requiring access to the same account; password is provided to IT support staff in order to resolve a technical issue; account password is communicated to a user by the system administrator. Also once the password is reset, the User is forced to change password at next logon.

5.4. DEFAULT PASSWORDS

System administrators shall not use default passwords for administrative accounts

5.5. APPLICATION DEVELOPMENT

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management; such that one user can take over the functions of another without having to know the other's password.

6.0 APPENDIX A: PASSWORD CONSTRUCTION GUIDELINES

6.1. ACCEPTABLE METHODS TO CREATE A STRONG PASSWORD

- Use a minimum of 8 characters. Generally, the more characters you can use, the harder a password is to be cracked or guessed.
- Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use a sentence or saying to create a “passphrase” by using the first letters, capitalization, and special characters as substitutes. For example, “One ring to rule them all, one ring to bind them” may be used to create a passphrase like “1R2rtAor2Bt” that can be used as a very strong password.
- Use mixed case (upper & lower)
- Use special characters and punctuation symbols (Example: +=!@%*&”:./)

6.2. UNACCEPTABLE METHODS TO CREATE A STRONG PASSWORD

- Do not use dictionary or actual words. Non-English words are no more secure than English words
- Do not use words, numbers, or known or public information associated with you. (e.g. Social security numbers; Names, family names, pet names; birthdays, phone numbers, addresses; etc.)
- Avoid using your login name or any variation of your login name as your password. If your login is ‘fredrick’, do not use substitution or letter reordering. Examples would be ‘fr3drick’, where the 3=e. alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).
- Do not use the same character for the entire password (e.g., ‘11111111’) or use fewer than five unique characters.
- Do not use common letter or number patterns for your password (e.g., ‘12345678’ or ‘abcdefgh’).
- Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=I, 0=O, etc).

- When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.

6.3. PASSWORD REQUIREMENTS (SUBJECT TO CHANGE)

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password, which an attacker with the old password could guess. The following password requirements will be set by the IT security department:

1. Minimum Length - 8 characters recommended
2. Maximum Length - 14 characters
3. Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
    1. Lowercase
    2. Uppercase
    3. Numbers
    4. Special characters such as !@#$%^&*(){}[]
4. Passwords are case sensitive and the user name or login ID is not case sensitive.
5. Password history - it can remember 4 old passwords
6. Password age - 120 days
7. Account lockout threshold - 5 failed login attempts

7.0 ENFORCEMENT

An employee found to have violated this policy may be subject to disciplinary action and may include termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with PAAET.

8.0 GLOSSARY

Password history	The number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.
Password Aging	After a specified period, the user is prompted to create a new password.

9.0 REFERENCES

1) ISO/IEC 27001:2013 - [A.9.4.3] – Password Management System
2) ISO/IEC 27001:2013 - [A.9.4.2] – Secure log-on procedures
3) ISO/IEC 27001:2013 - [A.9.2.4] –Management of secret authentication information of users.

10.0 ASSOCIATED DOCUMENTS

1) Information Security Policy
2) Access Control Policy