It's your future too

EDUCATION

POL/IT/0019: Password Policy

Policy Title:	GEMS Education MENASA ICT – Password Policy
Policy Number:	POL/IT/0019
Version:	1.0
Effective date:	27 January 2023
Scheduled review date:	26 January 2024
Policy approver:	Chief Disruption Officer
Policy owner:	ICT
Policy reviewer:	IT Security Manager
Relevant related policies:	• Refer Section 7
Other relevant documents:	• None

It's your future too

EDUCATION

Table of Contents

It's your future too

EDUCATION

1. Policy Statement

Access to all GEMS Education systems shall be granted after user authentication, in order to prevent unauthorized access and enforce user accountability.

2. Purpose

The purpose of this policy is to establish a standard for the selection and maintenance of strong passwords.

3. Scope

- All GEMS Education IT systems and portals;
- All GEMS Education employees and contractors;
- All ICT engineers at schools and ICT team at corporate offices;
- All GEMS Education students and parents.

4. Requirements

4.1 All users shall be responsible for selecting and maintaining passwords according to the requirements of this document;

4.2 All users shall adhere to the following practices to safeguard their system/application credentials:

4.2.1 Shall not use a common password across GEMS system/application accounts and their personal accounts;

4.2.2 Shall not share passwords with anyone including colleagues, administrative assistants or secretaries;

4.2.3 Shall not reveal passwords in emails, chats or other forms of digital or verbal communications;

4.2.4 Shall not provide hints on the password format;

4.2.5 Shall not store/save passwords in text files, note books, emails or web browsers;

4.2.6 Shall treat passwords as company confidential information;

4.2.7 Shall decline the use of the "Remember Password" feature on web applications;

4.2.8 Shall not transmit passwords over a network in clear text or publicly display them.

4.3 All questions or support issues shall be addressed to the corporate ICT team.

4.4 All ICT team members shall utilize a password manager to store and generate passwords for all administrative and service accounts;

Password requirements:

CATEGORY	MINIMUM LENGTH	MINIMUM COMPLEXITY	REUSE	ACCOUNT LOCKOUT	INACTIVE SESSION
User account - Administrator	14 characters	Lower case, upper case, special character and numeric digit	Expires after 90 days No re-use of previous 6 passwords	Duration: 30 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account – Staff (except teachers)	8 characters	Lower case, upper case, special character and numeric digit	Expires after 90 days No re-use of previous 4 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account – Teachers	8 characters	Lower case, upper case, special character and numeric digit	Expires after 90 days No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 50 minutes of inactivity
User account - Junior Students (03 and	3 characters (CVC words)	Any three characters	Expires after 180 days No re-use of previous 3	Duration: 15 min After 5 consecutive failed authentication	Terminate after 15 minutes of inactivity

CATEGORY	MINIMUM LENGTH	MINIMUM COMPLEXITY	REUSE	ACCOUNT LOCKOUT	INACTIVE SESSION
04)			passwords	attempts	
User account - Mid-level Students (05 and 06)	5 characters (dictionary words)	Any five characters	Expires after 180 days No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account - Senior Students (07 and above)	8 characters	Any eight characters	Expires after 180 days No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account - Parents	6 characters	Lower case, upper case, special character and numeric digit	Expires after 180 days No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity

5 Guidance on selection of strong passwords

- You can choose one or two lines from a poem, song or your favourite phrase or quotation and use the first letter of each word. For e.g. '**T**hing **O**f **B**eauty **I**s **J**oy **F**orever' becomes "Tobijf1#".
- Replace letters with numbers or characters. For e.g. "tobijf" becomes "T0b1jf#s".
- Use short unrelated words and concatenate them together with special symbol and number.

6. Policy Compliance

6.1 Compliance measurement:

It's your future too

GEMS EDUCATION

6.1.1 Information security team shall be responsible to monitor compliance with this policy;

6.2 Exceptions:

6.2.1 None.

7. Related Standards, Policies and Processes

- Information security policy;
- Acceptable Use Policy
- Password Standard

Signed..... **Date**.....March 2023

Principal/CEO