مدرسة جيمس متروبول الواحة
GEMS Metropole School
AL WAHA

Logical Access Control

Approved by:	Jeremy Hallum (Principal)
Last reviewed on:	August 2023
Next review due by:	August 2026

MISSION

Lead, nurture and succeed.

VISION

A sustainable and inclusive community hub, nurturing future leaders.

Nurturing LEADERSHIP

This policy is applied at MTW alongside our school's vision, mission and values. Alongside the principles of High Performance Learning; VAA and A.C.P. characteristics.

Policy Title:	GEMS Education MENASA ICT – Logical Access Control Policy
Policy Number:	POL/IT/0014
Version:	1.0
Effective date:	January 2023
Scheduled review date:	January 2024
Policy approver:	Chief Disruption Officer
Policy owner:	ICT
Policy reviewer:	IT Security Manager
Relevant related policies:	• Refer Section 12
Other relevant documents:	• None

1. Policy Statement

Access to GEMS Education systems shall be restricted to authorized users, based on theprinciple of need to know and least privilege.

2. Purpose

The purpose of this policy is to standardize the user life-cycle management process andprovide controlled access to users.

3. Scope

- All employees, contractors and associated third parties of ICT department;
- GEMS Education ICT department information systems and applications.

4. Authentication

4.1 Each user shall be assigned a unique User-ID and password;
4.2 User-ID shall be permanently decommissioned when the user leaves GEMSEducation;
4.3 Reuse of User-ID shall not be permitted;
4.4 Use of anonymous User-ID (such as "Guest") shall not be permitted;
4.5 User-ID shall be created as per GEMS Education standards;

- Asian – [First name without spaces or special characters].[First characterof Last name/ Middle name(if Last name is blank)]
- International – [First character of first name].[Last name/ Middle name(ifLast name is blank) without spaces or special characters]

- Corporate - [First name without spaces or special characters].[Last name/Middle name(if Last name is blank)]

4.6 Generic or shared user-IDs shall not be utilized;

- Exception to generic or shared user-IDs shall be documented withbusiness justification;
- Access request shall be approved by Head of Department and Informationsecurity team;
- Ownership of the generic or shared user ID shall be defined.

4.7 Vendor specific default user-IDs and passwords on systems / applications or devices shall be disabled or the default password shall be changed to comply withGEMS password policies;

4.8 User shall be responsible for all activities that occur, from use of their accounts.

5. Authorisation

5.1 Access to information systems shall be assigned based on business requirementsand relevant approvals;

- Allocated access shall be in accordance with the least privilege principles.

6. Segregation of Duties

6.1 Segregation of duties shall be maintained for the assigned access rights inaccordance with business roles;

Example:

- *System administration and system auditing shall be performed by differentpersonnel;*
- *System operations and system security administration shall be performedby different personnel.*

7. Change of User Responisiblities

7.1 Access shall be modified when a user:

- Moves departments or job roles internally;
- No longer requires the level of access that has been granted.

8. User Access Reviews

8.1 Periodic review of access shall be performed bi-annually;

8.2 Review shall be performed by ICT/ Information security operations;

8.3 Discrepancies identified shall be recorded and corrected;

9. Revocation

9.1 Revocation of access shall be performed in event of the following -

- Change in position, deputation or responsibilities;
- Transfer to another site/ school or department;
- Termination/Resignation;
- Absconding;
- Deceased.

10. Privilege Access Management

10.1 All privileges shall be allocated as per "business requirements" and "need toknow" basis;

- Privileged access shall be revoked as soon as they are deemed notrequired.

10.2 Privileges allocated shall be authorized, tracked and recorded.

11. Policy Compliance

11.1 Compliance measurement

11.1.1 Information security team shall be responsible to monitor compliance with thispolicy.

11.2 Exceptions

11.2.1 Exceptions to this policy shall be documented. Exception shall include:

- Justification,
- Impact / risk resulting and
- Approval from information security team, Application/ System owner andLine Manager;

12. Related Standard, Policies and Processes

- Information security policy
- Change management policy
- Password policy
- Application specific user access management process documents

13.Monitoring and review

This policy is monitored by MTW Senior Leaders and will be reviewed every three years or earlier if necessary.