Mission Statement:
Creating tomorrow's successful and caring citizens today.

GFM Logical Access Control Policy

Policy Updated By	Latest Publish Date	Monitoring Cycle
IT Security Manager	January 2023	Annually

Schedule for Development / Monitoring / Review

This policy was approved by the Governing Body on:	January 2023
The implementation of this policy will be monitored by the:	**Principal and Senior Leadership Team**
The Policy will be reviewed annually, or more regularly in the light of any significant new developments. The next anticipated review date will be:	**January 2024**
Should serious incidents take place, the following external persons/agencies should be informed:	**Akram Tarik (Principal) and in his absence (Vice Principal)**

This policy is applied at GFM alongside our school's vision, mission and values. Interwoven with the principles of High Performance Learning; values, attitudes, attributes and A.C.P. Characteristics.

POL/IT/0014: Logical Access Control Policy

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

Vision

'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

Mission Statement:
Creating tomorrow's successful and caring citizens today.

GFM Logical Access Control Policy

Policy reviewer:	IT Security Manager
Relevant related policies:	• Refer Section 12
Other relevant documents:	• None

Table of Contents

1. Policy Statement

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

Vision

'At GFM we empower students to have the heart to celebrate uniqueness and the mind to be innovative, creative problem solvers, bringing a positive change to the world in which we live.'

GFM Logical Access Control Policy

2. Purpose

The purpose of this policy is to standardize the user life-cycle management process and provide 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 GEMS Education;

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(if Last 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 with business justification;
- Access request shall be approved by Head of Department and Information security team;
- Ownership of the generic or shared user ID shall be defined.

GFM Logical Access Control Policy

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. Authorization

5.1 Access to information systems shall be assigned based on business requirements and 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 in accordance with business roles;

Example:

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

7. Change of user responsibilities

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.

GFM Logical Access Control Policy

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 to know" basis;

- Privileged access shall be revoked as soon as they are deemed not required.

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 this policy.

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 and Line Manager;

12.Related Standard, Policies and Processes

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

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

Principal/CEO

Policy review date: February 2024

Please read this policy alongside:

13.Appendix – I (Exceptions Form)

Form# Entity-Location/ Department-FOR-EX0001				Date: DD/MM/YYYY
To be filled by Requester				
School:				
Department:				
Employee Name:				
E-mail ID:				
Employee ID:				
Designation:				
Contact Number:				
Exception				
Description				
Risk				
Assets/ policy Impacted				
Ownership of generic ID (if applicable)				
Justification				
Impact:	Critical	High	Medium	Low
Approval				
Application/ System Owner:				
Employee Name and Designation:				
Employee ID:				
Approval Date:				
Status:	Approved		Rejected	
Line manager				
Employee Name and Designation:				
Employee ID:				
Approval Date:				
Status:	Approved		Rejected	
Information Security Team				
Employee Name and Designation:				
Employee ID:				
Approval Date:				
Status:	Approved		Rejected	