

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



GFM Anti-Virus and Malware 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/0017: Anti-Malware Policy

Policy Title:	GEMS Education MENASA ICT – Anti-Malware Policy
Policy Number:	POL/IT/0017
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:	<ul style="list-style-type: none">Refer Section 13

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 Anti-Virus and Malware Policy

Other relevant documents:

- None

Table of Contents

1.	<u>Policy Statement.....</u>	3
2.	<u>Purpose.....</u>	3
3.	<u>Scope.....</u>	3
4.	<u>Installation.....</u>	3
5.	<u>Anti-Malware Signature Update.....</u>	4
6.	<u>Maintenance.....</u>	4
7.	<u>Documentation.....</u>	4
8.	<u>Backup.....</u>	4
9.	<u>Incident Management.....</u>	4
10.	<u>Change Management.....</u>	5
11.	<u>Vendor Support.....</u>	5
12.	<u>Policy Compliance.....</u>	5
13.	<u>Related Standards, Policies and Processes.....</u>	5
14.	<u>Appendix - I (Exceptions Form).....</u>	6

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 Anti-Virus and Malware Policy

1. Policy Statement

GEMS Education systems shall be protected against malicious code. The protection measure shall ensure early detection, efficient containment and eradication of malicious code.

2. Purpose

To ensure all servers, desktops, and laptops are protected against intrusion from malware.

3. Scope

This policy applies to all desktops, laptops, and servers connected to GEMS network and personnel responsible for managing Anti-Malware controls.

4. Installation

- 4.1 All GEMS owned and managed desktops, laptops and servers connected to the network shall host an enterprise managed, anti-malware product that continually monitors for malicious software;
- 4.2 Anti-malware solution shall be configured to:
 - 4.2.1 Perform a full system scan on a fortnightly basis;
 - 4.2.2 Perform a real-time scan of files, folders or drives when invoked;
 - 4.2.3 Automatically clean infected files and quarantine files that cannot be cleaned;
 - 4.2.4 Scan user mail for malicious content;
 - 4.2.5 Prevent end-users from disabling or tampering the anti-malware agent settings;
- 4.3 Anti-Malware servers shall be:

4.3.1 Securely

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 Anti-Virus and Malware Policy

configured and shall comply with GEMS security baselines;

Installed in a secure location.

5. Anti-Malware Signature Update

- 5.1 Anti-Malware solution shall be:
 - 5.1.1 Maintained updated to the recent definitions;
 - 5.1.2 Configured to update signatures from vendor portal, when not connected to GEMS network.

6. Maintenance

- 6.1 ICT administrators shall perform the following maintenance activities on a monthly basis:
 - 6.1.1 Review and ensure the end-points count is reconciled with the system inventory under their care;
 - 6.1.2 Review and ensure all end-points agents are able to communicate with the anti-malware server;
 - 6.1.3 Monitor end-points under their care for missed updates and apply corrective actions.

7. Documentation

- 7.1 The ICT team shall maintain documents on installation and configuration for the anti-malware solution.

8. Backup

- 8.1 Anti-malware server configuration shall be periodically backed up;
- 8.2 Anti-malware event logs shall be retained for a period of six months.

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 Anti-Virus and Malware Policy

9. Incident Management

9.1 Refer "Security incident management policy".

10. Change Management

10.1 Changes regarding anti-malware solution and configuration settings shall follow change management process (Refer "Change Management Policy").

11 Vendor Support

11.1 Service Level Agreements shall be maintained with vendors for software upgrade and technical support.

12 Policy Compliance

12.1 Compliance measurement

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

12.2 Exceptions

12.2.1 Exceptions to this policy shall be documented. Exception shall include

- Justification,
- Impact / risk resulting and
- Approval from information security team and VP – Technology;

13 Related Standards, Policies and Processes

- Change management policy
- Monitoring policy

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 Anti-Virus and Malware Policy

- Backup policy
- Security Incident management policy
- Acceptable use policy

Monitoring and review is annual.

Signed

IT Manager

Date

Signed

Principal/CEO

Date *February 2023*

Policy review date: **February 2024**

Please read this policy alongside:

IT Exception Form: Form# Entity-Location/Department-FOR-EX0001 Date: DD/MM/YYYY	
To be filled by Requester(System owner)	
School:	
Department:	
Employee Name:	
E-mail ID:	
Employee ID:	
Designation:	
Contact Number:	
Exception	

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 Anti-Virus and Malware Policy

14 Appendix – I (Exceptions Form)

Description				
Risk				
Asset/Polices Impacted				
Justification				
Impact:	Critical	High	Medium	Low
Approval				
VP – Technology				
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		

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.'