مدرسة جيمس متروبول الواحة
GEMS Metropole School
AL WAHA

Anti-Virus and Malware

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 – Anti-Malware Policy
Policy Number:	POL/IT/0017
Version:	1.0
Effective date:	January 2023
Policy approver:	Chief Disruption Officer
Policy owner:	ICT
Policy reviewer:	IT Security Manager
Relevant related policies:	• Refer Section 13
Other relevant documents:	• None

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:
4.3 Perform a full system scan on a fortnightly basis;
4.4 Perform a real-time scan of files, folders or drives when invoked;
4.5 Automatically clean infected files and quarantine files that cannot be cleaned;
4.6 Scan user mail for malicious content;
4.7 Prevent end-users from disabling or tampering the anti-malware agent settings;
4.8 Anti-Malware servers shall be:
Securely 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:
Maintained updated to the recent definitions;
Configured to update signatures from vendor portal, when not connected to GEMS network.

6. Maintainance

6.1 ICT administrators shall perform the following maintenance activities on a monthly basis:

Review and ensure the end-points count is reconciled with the system inventory under their care;

Review and ensure all end-points agents are can communicate with the anti- malware server;

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.

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

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

12.2 Exceptions

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

14. Monitoring and review

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