POL/IT/0037: Removable Media Policy

Policy Title:	GEMS Education MENASA ICT – Removable Media Policy
Policy Number:	POL/IT/0037
Version:	1.0
Effective date:	21 September 2022
Scheduled review date:	20 September 2024
Policy approver:	Chief Disruption Officer
Policy owner:	SSC IT
Policy reviewer:	IT Heads of Department
Relevant related policies:	• Refer Section 6
Other relevant documents:	• None

Table of Contents

1. Policy Statement 3
2. Purpose 3
3. Scope 3
4. Requirements 3
5 Policy Compliance 5
6 Related Standards, Policies and Processes 5
7 Appendix – I (Exceptions Form) 6

1. Policy Statement

No personal removable storage devices will be authorized to be used in GEMS Education.

2. Purpose

The purpose of this policy is to define the term for the use and security of removable media devices/equipment on GEMS' corporate devices as SSC and schools.

3. Scope

All removable media for use on information systems owned or operated by GEMS are covered by this policy.

Removable media refers to computer storage devices that are not fixed inside a computer and include:

- Solid state memory devices including memory cards, pen drives, memory sticks (USB) etc.
- Removable or external hard disk drives
- Optical disks i.e., DVD and CD
- SD cards

4. Requirements

4.1 No Personal data storage devices are authorized to be used in GEMS. Any deviation to this shall be handled as per the exception handling policy;

4.2 Actions of installing unauthorized software or intentionally tampering with the integrity of the device to bypass GEMS portable device security would not be allowed;

4.3 Access to removable media, by default, shall be blocked on all portable devices (laptops, tablets, and mobiles), servers, desktops, endpoints, information display panel, printers, fax machines, magnetic tapes and any other device;

4.4 Where a need has been identified and the request is approved by the authorized department heads and Chief of Strategy, Operational Transformation and PPP and then Group Chief Disruption Officer, the request shall be evaluated and approved by the information security team after considering the risk of possible data loss or leakage. On approval, an encrypted GEMS removable media will be allocated to the respective user by the local ICT team;

4.5 All such business request shall be made through service desk portal or via an email sent to service desk portal;

4.6 It is a mandatory requirement that Restricted, Confidential and Internal data shall not be stored or carried on non-encrypted removable media; Details pertaining to data classification can be found in GEMS Data Classification Policy document.

4.7 Use of removable media access shall be permitted for a limited time and is subject to business requirement. Enabling of this access will require a user to follow the Exception Handling process/steps elaborated in the Exception Handling Section;

4.8 GEMS IT to ensure that only identified GEMS removable media shall be provided to the user while provisioning the removable media device;

4.9 GEMS IT shall ensure that all removable media allocated to end-users are formatted, securely erased, encrypted and free from any malware before allocation;

4.10 GEMS IT to ensure that auto-run feature of removable media is disabled;

4.11 GEMS IT shall configure the endpoint protection system to scan any removable media for malware, every time they are connected to the GEMS information systems;

4.12 Records shall be maintained and asset register need to be updated regularly for all GEMS encrypted removable media devices;

4.13 All removable media/encrypted memory devices remain the property of GEMS and shall be returned when the staff leaves employment from GEMS and/or no longer needs to use such a device;

4.14 GEMS Information security team shall continuously monitor possible data leakage through removable media by configuring a use-case in SOC monitoring;

4.15 Line Managers to ensure that access to removable media are revoked and the device is returned if,

i. Allocated removable media is no longer required due to role change;
ii. Change in business needs;
iii. Any case of misuse of the allocated removable media is reported against the staff;
iv. Usage request Duration of lease is expired.

4.16 In case of loss of allocated removable media, the end-user shall report to the department head and also to the GEMS information security team. The loss of removable media shall be reported as an "Incident" created on IT Service Desk Portal. Please refer security incident management policy for more details.

5 Policy Compliance

5.1 Compliance - Information security team shall be responsible to monitor compliance with this policy by conducting a bi-annual review of all assigned encrypted removable media devices and associated exceptions.

5.2 Exceptions:

- Exceptions to this policy shall be documented and recorded in service desk portal. Exception shall include:
  - Clear Business Justification,
  - Impact / risk resulting
- Exceptional approval process will be initiated once a request from Heads of Department with business justification is received by information security team either by service desk portal or by an email. Once the exception request is created on service desk, it must be approved by Chief of Strategy, Operational Transformation and PPP and then Group Chief Disruption Officer
- Technology Steering Committee will be used to decide on the final decision in case of an escalation.

6 Related Standards, Policies and Processes

- Information Security Policy;
- Acceptable Use Policy
- Security incident Management Policy
- Data Classification Policy

7 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	
Department Head:	
Employee Name and Designation:	
Employee ID:	
Approval Date:	
Status:	☐Approved ☐Rejected
Enterprise Business Data Owner	
Employee Name and Designation:	
Employee ID:	
Approval Date:	
Status:	☐Approved ☐Rejected
Technology Owner	
Employee Name and Designation:	
Employee ID:	
Approval Date:	
Status:	☐Approved ☐Rejected