
COMPUTER & INFORMATION TECHNOLOGY CENTER

# Removable Media Handling Policy

# Document Controls

***This document is reviewed every six months***

| | |
|---|---|
| **Document Reference** | PAAET-CIC-PLCY-Media Handling |
| **Document Title** | Media Handling Policy |
| **Document Owner** | Abdullah AlDousari |
| **ISO 27001:2013 reference** | A.8.3 Media Handling |
| **Security Classification** | Internal - Restricted |
| **Stored** | http://sp13.paaet.edu/sites/TecDep |
| **Next Review Date** | 25th Mar 2017 |
| **Document Status** | Final |

## Document Review and Approval History

| Date | Version | Amended by | Reviewer / Approver | Remarks | RFC# |
|---|---|---|---|---|---|
| 21st April, 2016 | Draft v1.0 | Reena Varghese | | | |
| 24th October, 2016 | Draft v1.1 | Abdullah AlDousari | | | |
| 25th October, 2016 | Final v1.2 | Abdullah AlDousari | Rabie Al-Mejbas | | |
| | | | | | |

## Document Distribution List

| Sl.No. | Name and Department | Purpose |
|---|---|---|
| | ***Will be published on PAAET website for all PAAET employees*** | ***To ensure that all users read the policy of removable media handling and know how to deal with this policy to get the maximum security within the organization*** |
| | | |

# CONTENTS

# CONFIDENTIALITY STATEMENT

This document includes confidential information related to the Computer and Information Technology Center (**CIC**) at the Public Authority for Applied Education and Training (**PAAET**), shall not be distributed to any persons other than those mentioned in the distribution list herein, and shall be used solely for **CIC'**s internal purpose.

# 1.0 INTRODUCTION

Removable Media is being used by staff who has access to the information, information systems and IT equipment within the IT Division of **Public Authority for Applied Education & Training (PAAET)** to store and transfer information.

# 2.0 OBJECTIVE

The objective of Media Handling policy is to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of PAAET's computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Confidential and Internal - Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

# 3.0 SCOPE

This policy applies to all users in PAAET, including contractual third parties who have access to PAAET's information, information systems or IT equipment and intends to store any information on removable media devices.

# 4.0 REMOVABLE MEDIA LIST

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- External Hard Drives.
- USB Memory Sticks (also known as flash drives).
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- Backup Tapes

# 5.0 POLICY

### 5.1 Restricted Access to Removable Media

- It is PAAET's policy to prohibit the use of all removable media devices. The use of removable media devices shall only be approved if a valid business case for its use is developed.
- Requests for access to, and use of, removable media devices shall be made to IT Service Desk. Approval for their use must be given by Head of IT.

### 5.2 Procurement of Removable Media

- All removable media devices and any associated equipment and software must only be purchased and installed by IT Services. Non-PAAET owned removable media devices must not be used to store any information used to conduct official PAAET business, and must not be used with any PAAET owned or leased IT equipment.
- The only equipment and media that should be used to connect to PAAET's equipment or the network is equipment and media that has been approved by the Head of IT or has been sanctioned for use by the Head of IT.

### 5.3 Security of Data

- Removable media should not be the only place where data obtained for PAAET's purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.
- All storage media shall be stored in an appropriately secure and safe environment in order to minimize physical risk, loss, theft or electrical corruption.
- Each user shall be responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.
- All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all Confidential or Internal - Restricted data held must be encrypted.
- Virus and malware checking software shall be used when the removable media device is connected to a machine.
- Special care shall be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data shall consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Damaged or faulty removable media devices shall not be used. It is the duty of all users to contact IT Service Desk should removable media be damaged.

### 5.4 Disposing of Removable Media Devices

- Removable media devices that are no longer required, or have become damaged, shall be disposed of securely to avoid data leakage.
- Any previous contents of any reusable media that are to be reused, either within the PAAET shall be erased. This shall be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools.
- All removable media devices that are no longer required, or have become damaged, must be returned to IT Service Desk for secure disposal.

## 6.0 REFERENCES

1) ISO/IEC 27001:2013 - [A.8.3] – Media Handling

## 7.0 ASSOCIATED DOCUMENTS

1) Information Security Policy

# 8.0 GLOSSARY

| | |
|---|---|
| **Removable media** | Removable media are data storage devices capable of computer system removal without powering off the system. Removable media devices are used for backup, storage or transportation of data. |
| **Malware** | Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission. |