
COMPUTER & INFORMATION TECHNOLOGY CENTER

# Anti-Malware Policy

# Document Controls

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

| | |
|---|---|
| **Document Reference** | PAAET-PLCY-Anti-Malware Policy |
| **Document Title** | Anti-Malware Policy |
| **Document Owner** | Abdullah AlDousari |
| **ISO 27001:2013 reference** | A.12.2.1 Controls against Malware |
| **Security Classification** | Internal – Restricted |
| **Stored** | http://sp13.paaet.edu/sites/TecDep |
| **Next Review Date** | 20th January 2017 |
| **Document Status** | Final |

## Document Review and Approval History

| Date | Version | Amended by | Reviewer / Approver | Remarks | RFC# |
|---|---|---|---|---|---|
| 19th May, 2016 | Draft v1.0 | Reena Varghese | | | |
| 19th May 2016 | Draft v1.1 | Reena Varghese | Jessy Sakariah | Updated on reviewer comments | |
| 16th June 2016 | Draft v1.2 | Abdullah AlDousari | | Edited | |
| 20th July 2016 | Final 1.3 | Rabie Al-Mejbas | Rabie Al-Mejbas | Updated reviewer comments and final review. | |

## Document Distribution List

| Sl.No. | Name and Department | Purpose |
|---|---|---|
| 1 | Dr. Jasem AlOstad, CIC Manager | For feedback |
| 2 | Ali Hussain, Technical Support Supervisor | Distribution to concerned staff responsible for creating maintaining and troubleshooting PC and Network problems. |
| 3 | Ibtisam Shaban, Development Supervisor | Distributions to the Development team members who are responsible creating computer systems to start enforce it. |
| 4 | Ammal AlQattan, PC & Servers section Head. | For her information |
| 5 | ISO team :<br>• Rabie Al-Mejbas<br>• Rajiv Prakash<br>• Nadia AL Saleh<br>• Shaikha AL Barak<br>• Mai AlAbdulqader | Be aware of this policy start enforce it. |
| 6 | All CIC employees and technical supports contractors | Enforce this policy by reporting any violation by any employee connected to PAAET network |

# 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

Malicious software, commonly known as malware is a general expression used by many within the information security to describe software created and/or used for the purpose of harming and damaging various systems such as computer code, files, applications and other relevant information technology platforms and utilities. This policy is designed to provide PAAET with a formalized anti-malware policy that is to be adhered to and utilized throughout the organization at all times.

# 2.0 SCOPE

This policy encompasses all system resources that are owned, operated, maintained and controlled by PAAET and all other system resources, both internally and externally, that interact with these systems.

# 3.0 POLICY

- All PAAET personal computers and servers that are connected to the PAAET's network or otherwise using the IT facilities must run an approved and up-to-date anti-virus product that continually monitors for malicious software (viruses, worms, Trojan horse, rootkits, adware, spyware, logic bombs, etc.).
- All personal computers, devices and servers connected to PAAET's network must run the latest available patches applied on the Operating System as well as on the applications.
- Removable devices such as USB Drives, CDs, etc. shall be scanned before being connected to the PAAET network.
- The anti-virus product shall be operated in real time on all servers and client computers.
- The anti-virus library definitions shall be updated at least once per day.
- Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.
- Any non-PAAET owned devices that require connection to the PAAET network must run an appropriate anti-virus product, which is approved and compliant to the standard followed by PAAET.

- Do not try to uninstall or disable anti-virus software. Any messages suggesting that anti-virus protection has been disabled should be investigated immediately.
- PAAET's IT Regulations prohibit any activity intended to create and / or distribute malicious code (viruses, worms, etc.) on the network or IT facilities.
- PAAET reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.
- If you suspect that a device is infected with a virus, report the incident to the Helpdesk staff who shall follow the standard incident handling procedures.
- Email attachments must be scanned by an anti-virus product before delivery.
- Check the authenticity of attachments / software to be installed from internet sources. Do not install applications that arrive on unsolicited media.
- Reports shall be generated to identify the systems that have not received the latest anti-virus updates. The updates shall be run either remotely or on site for such systems.

## 4.0 ENFORCEMENT

An employee found to have violated this policy may be subject to disciplinary action and may include termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with PAAET.

# 5.0 GLOSSARY

| | |
|---|---|
| **Internal System resources** | Resources owned, operated, maintained and controlled by the organization and include all network devices (firewall, routers, switches, load balancer, other network devices). Servers (both physical and virtual server, along with the operating systems and applications that reside on them) and any other system resources deemed in scope. |
| **Malware** | Software created and/or used for the purposes of harming and damaging various systems, such as computer code, files, applications and other relevant information technology platforms and utilities. |
| **Antivirus** | Software used for the purposes of preventing, detecting and removing malicious software. |
| **Worm** | A standalone, independent program that has the ability to replicate itself and spread to other computes, ultimately infiltrating programs and destroying data. |
| **Trojan Horse** | A harmful piece of malware that facilitates unauthorised access on a computer system by way of social engineering tactics and strategies. |
| **Rootkits** | Software that enables unauthorised access to a computer system and that is also hidden from detection. Rootkits can conceal the altering of files, data, etc. and are a serious form of malware. |
| **Spyware** | Software that collects vital information form a computer system regarding data on such system and the associated user activities. It is |

| | |
|---|---|
| | considered malware when it is “unauthorised” as there are legitimate use of spyware. |
| **Adware** | Programs that facilitate delivery of advertising content and related material to a user through their browser while on the internet or through some other type of interface. It is considered a malware when it is “unauthorized” as there are legitimate uses of adware. |
| **Logic Bomb** | Code that is intentionally inserted into a software system that initiates a malicious function when specified conditions are met. |

# 6.0 REFERENCES

1) ISO/IEC 27001:2013 - [A.12.2.1] –Controls against Malware

# 7.0 ASSOCIATED DOCUMENTS

2) Information Security Policy