جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Antivirus and Antimalware	Last Review date	19/5/2021
	Policy Number	IT-03	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

This policy is designed to prevent viruses, malware, or malicious code from infecting University of Sharjah's computing devices and network. By preventing virus infections, data and files damages to UoS processing facilities will also be protected. This policy shall be reviewed for content and compliance on annual basis.

Scope

This policy is applicable to all systems, and information processing facilities, personnel as well as all third party personnel who are using information and systems.

Purpose

Virus, worm, Trojan, spyware or collectively called as malware are potential risk to the confidentiality, integrity and availability of UoS systems. The antivirus policy is for the successful prevention, detection and removal of virus and malware.

Definitions

1. A computer virus is a computer program that can copy itself and infect a computer.
2. A computer worm is a self-replicating computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.
3. A Trojan is non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.
4. Adware, or advertising-supported software, is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used
5. Spyware is a type of malware that is installed on computers and collects little bits of information at a time about users without their knowledge.
6. For the purpose of this document, malware term is used to define virus, worm, Trojan, adware, spyware or any other malicious software program that can cause harm to the users, systems, network or organization's IT infrastructure. However, antivirus software term is used to refers to the application installed on the computer system to prevent any malware infecting the system or prevent the spreading of such malicious software from spreading.

Policy

Anti-Malware / Anti-Virus

1. All possible and practicable measures shall be taken to prevent the introduction of malware into University of Sharjah's information systems.
2. Any information systems including servers, laptops and desktops, storage, High performance computing systems IoT devices, Lab machines must have approved Antivirus solutions installed.
3. Mobile devices, where technically possible shall have anti-virus installed. Malware detection infrastructure shall be implemented at points where Malware can be introduced into University of Sharjah's information network.
4. The anti-virus shall be operated in real time on all servers and client computers
5. The virus scanner shall be scheduled to auto run scans at regular intervals. Frequency for scanning shall be defined.
6. Both inbound and outbound email messages along with the attachments shall be scanned for viruses.
7. The Malware detection infrastructure will be updated with the latest product and virus signature updates as soon as these updates are released by the Antivirus vendor.
8. The antivirus software and clients on the University of Sharjah's systems must not be disabled or stopped while connected to the network.
9. All files downloaded or transferred within the University of Sharjah's network and information systems shall be scanned for malware at the gateway level.
10. All network traffic entering and leaving University of Sharjah's network including Internet, email, file transfer etc. shall be scanned for malware.
11. All University of Sharjah's information system users shall be provided with appropriate awareness on the antivirus best practices and policies.
12. All users are responsible for reporting any malware/virus incident to IT Service Desk / Information Security Team immediately.
13. Email systems must be enforced with appropriate malware and phishing controls. Email attachments from unreliable sources should not be opened.
14. Mobile codes such as ActiveX controls should not be activated unless it is acceptable and from a trusted source.
15. Software from untrustworthy sources when required to be tested, must be tested on an isolated system with proper approval from the Information Security Team
16. The Anti-virus solution shall be configured to do the following
    a. Scan for all files including compressed files.

b. Clean the Malware detected automatically.

17. Quarantine / Delete the infected file in case it cannot be cleaned.

Antivirus Standards:

1. University of Sharjah approved antivirus shall be installed on desktops, laptops, mobile devices, and servers with the latest definitions updated.

Exceptions

Exceptions if any to this policy shall be explicitly reviewed by the information security team and approved by the ITC director. The exceptions if any shall be approved and valid for a specific time period and shall be reassessed and re-approved if necessary.

Policy Compliance, Enforcement and Violations

1. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from Information security team.
2. All Users shall report any known or suspected information security incidents immediately.
3. Anonymity of User reporting a suspected incident shall be maintained, unless the matter is referred to a court of law.
4. Violations of this policy and supporting policies shall result in corrective / disciplinary action by Management.
5. An Internal audit shall be carried out once a year and a report on the compliance shall be submitted to the IT Information Technology Committee.

Reference

Standard	Control Ref
ISO 27001:2013	A.12.2.1