ITP 123

IT Malicious Software Management Policy

Table of Contents

1. POLICY INTRODUCTION

This policy concerns computer viruses, network worms, Trojan horse programs, rootkits, key loggers, trapdoors, backdoors, adware, crimeware, scareware, ransomware etc., collectively known as "Malware" (A Contraction of Malicious Software).

Malware poses a serious threat to the organisation because it is commonplace, highly variable and surreptitious. It is difficult to detect and block. Modern malware is technically advanced, making it difficult to eradicate and capable of undermining or negating many forms of control. Worse still, Malware incidents can be highly damaging, affecting the security of business information leading to serious consequences such as business interruption, privacy breaches and other compliance failures/ loss/ theft/ devaluation of intellectual property and safety failures.

Malware is being actively developed, traded and used by:

- Individuals for personal reasons (such as spying on their partners and work colleagues or accessing confidential proprietary information);
- Criminals to commit fraud, identity theft, information theft, coercion, blackmail, sabotage etc.
- Unethical adversaries to commit industrial espionage, steal intellectual property, sabotage, business process and commercial bids etc.; and
- Hackers, journalist, private investigators, law enforcement, the security services, government agencies and others for various reasons including national security and potentially, cyberwar.

2. SCOPE

This policy applies to everyone who has access to National Ambulance information, information assets or IT equipment. This may include, but is not limited to employees of the National Ambulance, Executives of the Company, temporary workers, partners and contractual third parties.

All those who use or have access to National Ambulance information must understand and adopt this policy and are responsible for ensuring the security of the Company's information systems and the information that they use or handle.

3. ROLES AND RESPONSIBILITIES

ROLE	FUNCTIONAL RESPONSIBILITIES
Information Security Specialist /Management	• Responsible for maintaining this policy and advising generally on information security controls. • Assigning task for mitigations and countermeasures, following up and ensuring that all identified GAPS are closed. • Works in conjunction with other corporate functions, it is also responsible for running the activities to raise awareness and understanding of the obligations identified in this policy.
IT Department	• Responsible for determining requirements, reviewing, approving, installing, configuring, monitoring, and maintaining antivirus software and other technical antivirus controls.
Employees	• Employees are personally accountable for complying with applicable policies, laws and regulations at all times. • Employees who use cooperate IT systems or their own IT systems under the BYOD (Bring Your Own Devices Scheme) are responsible for using and not interfering with the antivirus controls outlined in this policy. • Prior to any official disclosure, Employees must not disclose or discuss malware incident outside the organisation unless explicitly authorized to do so. • It is also a responsibility of all individuals and handlers of National Ambulance information Technology Services, data and information to ensure that all policies and procedures dealing with all Information Technology (IT) & security, integrity of information and data are followed.
Internal Audit (IT/IS Staffs)	• Internal Audit is conducted periodically like weekly and quarterly depending on type by the Information Security Specialist and IT Staffs where applicable and is authorized to access compliance with this and other corporate policies at any time. • Anti-Virus Vulnerability Status (Weekly • All Systems and Networks Vulnerability Assessment (Quarterly)

4. POLICY STATEMENT (DETAILED REQUIREMENT)

4.1. ANTIVIRUS DEPLOYMENT:

- Antivirus Software Deployment - Antivirus software must be deployed and executing on all National Ambulance computer and communications systems commonly affected by malicious software, e.g., personal computers and servers, where applicable anti-virus technology exists.
- Virus Software Installation - Virus screening software must be installed and enabled on all National Ambulance firewalls, FTP servers, mail servers, intranet servers, and desktop machines.
- Antivirus Software Capabilities - All antivirus software that is deployed on National Ambulance computer and communications systems must be capable of detecting, removing, and protecting against all known types of malicious software.

4.2 Antivirus Configuration

- Antivirus Software Updates - All antivirus programs deployed on National Ambulance computer and communications systems must be configured to accept automatic updates of the software.
- Antivirus Software Scans - All antivirus programs deployed on National Ambulance computer and communications systems must be configured to periodically scan all systems for malware.
- Antivirus Software Logs - All antivirus programs deployed on National Ambulance computer and communications systems must be configured to log all antivirus activity.

4.3 Approved software list

- Approved software: National Ambulance shall maintain an approved software list that contains all software and business applications that is allowed to be installed on the organisation Desktop, Laptops and Servers. Software that is not included in this list would be subject to approval of the IT Department/Security before being allowed to be installed.

5. PROCEDURES

• Systems Network Access - Systems without the required software patches or systems that are virus-infested must be disconnected from the National Ambulance network.

• Virus Test System - Whenever software or files are received from any external entity, this material must be tested for viruses, worms, and other malicious software on a stand-alone non-production machine before it is used on National Ambulance information systems.

• Outbound Software And Executables - All files containing software or executable statements must be certified as virus free prior to being sent to any third party.

• Decrypting Files For Virus Checking - All externally-supplied computer-readable files must be decrypted prior to being subjected to an approved virus checking process.

• Weekly report of the Antivirus vulnerabilities status and maintenance activities must be generated and sent to the IT Manager.

• Any new software that is required by an employee for business purpose must be requested through and approved by the information Security of the IT department before the installation of such software. And the software updated in the National Ambulance approved software list.

6. BREACHES OF POLICY

Any violation of this policy may result in disciplinary action, up to and including termination of employment. National Ambulance reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Accordingly, to the extent permitted by law, National Ambulance reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Compliance to this policy can be verified through various methods, including but not limited to, periodic audits trails, internal and external audits, and feedback to the policy owner.

7. RELEVANT LEGISLATION

National Ambulance Privacy

International, federal or local legislation and circulars relevant to this Policy. Full detail on this legislation can be found in QHP109 Legal Register.

8. RELATED POLICIES AND FORMS

Policy & Procedure /Form

9. FEEDBACK

Any feedback or suggestions for improvement to this Policy, Processes or Procedures can be submitted to qhse@nationalambulance.ae

10.DOCUMENT CONTROL AND OWNERSHIP

A review and update of this document will take place as necessary, when changes occur that identify the need to revise this Policy such as changes in roles and responsibilities, release of new legislative or technical guidance, or identification of a new policy area.

This document ownership for editing is identified as:

IT Manager

_____

Change Brief

Version No.	Date	Change
1.0	December 2019	New Document
2.0	August 2022	Due to review no changes

CEO Approval

Board Member Verification