ITP 102

IT ACCEPTABLE USE OF ASSET POLICY

Table of Contents

1. POLICY INTRODUCTION

National Ambulance is committed to the highest standards for the security of its Information Assets. National Ambulance has published this Policy to develop, implement and maintain appropriate safeguards to protect National Ambulance Personnel and Information, including personal and consumer information, and comply with applicable laws, regulations, customer contracts, and industry standards relating to information security. This Policy establishes consistent National Ambulance-wide requirements, which apply to all Information Assets owned or operated by or for National Ambulance whether located on National Ambulance's HQ premise, Warehouse or at other offsite location and those individuals who have access to them. The purpose of this policy is to outline the acceptable use of computer equipment and applications of the company. These rules are in place to protect the employee and the company. Inappropriate use exposes National Ambulance to risks including virus attacks, data leakage, compromise of network systems and services, compliance and legal issues.

2. SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at the company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the company.

3. ROLES AND RESPONSIBILITIES

ROLE	FUNCTIONAL RESPONSIBILITIES
Responsible Executives	• Approve and formally support this policy
IT Department	• Educate and Train users through formal and informal process to ensure compliance with this Acceptable use of Asset Policy. • Shall develop, maintain and publish standards, processes, procedures and guidelines to achieve compliance with this Acceptable use of Asset Control Policy.
Line Managers	• Approve the Asset assignment to individual members of their department.
HR	• Shall inform the IT department of users starting, moving and leaving National Ambulance
NA Employees / Users	• Adhering to the requirements of this policy and any associated policies, guidelines or procedures

4. POLICY STATEMENT

4.1 General Use and Ownership

While National Ambulance's network administration desires to provide a reasonable level of privacy, users should be aware that the data information they create on the corporate systems remains the property of the company. Because of the need to protect company's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the company.

It is recommended that any information that users consider sensitive or vulnerable be encrypted and password protected.

For security and network maintenance purposes, authorized individuals within the company may monitor equipment, systems and network traffic at any time. Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

In addition to the above:

1. Personnel are held responsible for all activity performed under their National Ambulance Personnel ID;
2. Personnel with accounts will only access systems, applications, files and data to which they have been granted access. Access must only be granted on a need to know basis. The ability to inadvertently read, execute, modify, delete or copy information does not imply permission to do so;
3. All National Ambulance information must only be stored, transmitted or shared through organisational approved information systems;
4. Only approved and authorized Mobile Devices may be connected to National Ambulance's Information Assets. Mobile Devices like Mobile Phones should only be connected to the Mobile Wireless SSID: "NAC-MOBILE" and may be required to perform certain remediation actions based audit and IDS logs on device compromised or possible threats;
5. Personnel are provided access to National Ambulance's Information Assets to assist them in performing their duties, which are to be used for business purposes only; however, reasonable personal use is permissible provided that such personal use does not interfere with the performance of their duties, is consistent with National Ambulance policies and is not for personal business ventures;
6. National Ambulance reserves the right to filter or restrict access to sites deemed to be inappropriate, including but not limited to: sites that promote, display or disseminate Offensive Material, gambling, alcohol, pornography, file and photo sharing, media streaming and sites known for distributing harmful viruses;
7. Personnel must ensure their use of Information Assets is appropriate, lawful and in compliance with applicable corporate and IT / information security policies;
8. Only authorized Personnel may post content or create the impression that they are representing, stating opinions, or otherwise making statements on behalf of National Ambulance on social networking sites, blogs or other Internet sites;
9. Personnel who are aware of any event which threatens the availability, integrity or confidentiality of National Ambulance's Information Assets, or which breaches National Ambulance's policies, or is contrary

to applicable law, must immediately contact National Ambulance's IT Department/information Security Operations or report the violation through his manager or top management.

10. Personnel must obey all applicable intellectual property rights (e.g., copyright, patent, trademark, license agreement) governing the download, distribution or use of items such as text, graphics, music or software accessed on the Internet or in Digital Communications;

11. Personnel must exercise caution when opening e-mail attachments and avoid opening unsolicited attachments, which may contain viruses, e-mail bombs, or Trojan horse code; and

12. Personnel, including remote access Personnel, must take reasonable precautions to safeguard corporate systems by having up-to-date anti-virus software installed on connected laptops /computers.

4.2 Security and Proprietary Information

The user interface for information contained on Internet, intranet, Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed every 90 calendar days. Passwords must be a minimum of 8 characters with one number, one upper one lower and one special character.

All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or by logging-off when the computer will be unattended.

Password history will be maintained, and new passwords may not be reused for at least six previous passwords. Entering an incorrect password 5 times will result in the account being locked for atleast 5minutes.

Exception

Including but not restricted to:

- AEDs / Defibrillators
- Radios and Mobile communications devices
- Mobile Data Terminals (MDTs) / Ambulance data terminals
- 998 Response communication, call logging and dispatch equipment

Note: CAMO agrees that having screens lock automatically in a second is not appropriate while treating patients, call taking or dispatching are required. However, if a user leaves the screen at any time they must log off to ensure security.

Because information contained on portable computers is especially vulnerable, special care should be exercised outside of company's premises. Encryption should be used for mobile devices to prevent data dissemination.

4.3 Users Own Devices (BYOD)

Use of personal data equipment is usually restricted to connection to the public access networks or NA Guest or NA Mobile. Managers own devices may be registered to access the National Ambulance network if it complies with the systems baselines described in ITP125 System Baselines in that it has a current supported OS and hardware, has a current recognized Malware protection and is Patched and secure. Own devices must have a secure password in place to access them and not cache National Ambulance credentials for more than one login session.

Postings by employees from a company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties.

All hosts used by the employee that are connected to the company's Internet / Intranet / Extranet, whether owned by the employee or company, shall be continually executing approved virus scanning software with a current virus database. Unless overridden by departmental or group policy.

4.4 Removable Media / USB Storage

Use of users own or company provided USB sticks or other removable media to store or transport restricted, or confidential information is prohibited unless approved by the data owner and encrypted by the use of BitLocker or other AES256 algorithm encryption with a complex password / key. Copies of the primary key will be provided to the IT team for storage and retrieval of information if it becomes necessary.

All Removable media / USB Storage devices must be scanned for malware using a current malware detection system when in use, in compliance with ITP123 Malicious Software Management policy

4.5 Unacceptable Use of Assets

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the company authorized to engage in any activity that is illegal under UAE or international law while utilizing company's resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.6 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the company.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the local or international jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any company's account.

8. Making statements about warranty, expressly or implied, unless, it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, using additional resources for personal gain (e.g. BitCoin Mining) and forged routing information for malicious purposes.

10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job / duty.

11. Circumventing user authentication or security of any host, network or account.

12. Interfering with or denying service to any user other than the employee's host (e.g. denial of service attack).

13. Using any program / script / command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet/ Extranet.

14. Providing information about or lists of the employees / customers to parties outside of the company.

15. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

16. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

17. Unauthorized use, or forging, of email header information.

18. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

19. Creating or forwarding "chain letters", "Ponzi'' or other "pyramid" schemes of any type.

20. Use of unsolicited email originating from within company's networks of other Internet / Intranet / Extranet service providers on behalf of, or to advertise, any service hosted by the company or connected via company's network.

21. Posting the same or similar non-business-related messages to large numbers of Usenet news groups, blogs or email-based discussion group.

5. VIOLATIONS 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. National Ambulance does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. 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.

6. 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.

7. RELATED POLICIES AND FORMS

List related policies and procedures to the created/updated policy.

Policy & Procedure /Form
ITP123 Malicious Software Management policy
COP401 Information Management Policy
COP402 Document Retention Policy and Procedure
COP403 General Confidentiality Policy
ITP119 Access Control Policy
PUP203 Asset Management Policy

8. FEEDBACK

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

9. 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
2	January 2014	Document Re-write
3	September 2014	Spelling Mistakes
4	November 2019	Policy updated and management for Smart Pc Exception added
5	September 2020	Tracked changes enable, all updates made to meet ADHICS requirement

		Password history will be maintained, and new passwords may not be reused for at least three previous passwords. Removable Media / USB Storage Use of users own or company provided USB sticks or other removable media to store or transport restricted, or confidential information is prohibited unless approved by the data owner and encrypted by the use of BitLocker or other AES256 algorithm encryption with a complex password / key. Copies of the primary key will be provided to the IT team for storage and retrieval of information if it becomes necessary. All Removable media / USB Storage devices must be scanned for malware using a current malware detection system when in use, in compliance with ITP123 Malicious Software Management policy
6	March 2022	Updated as per CISO review of Deloitte audit comments. Added reference to ITP125 Updated User Account Password retention to 6 times Added timeout on the incorrect password entered 5 times

CEO Approval

Board Member Verification