IT Access Control Policy

ITP 119

Table of Contents

1.	POLICY INTRODUCTION	3
2.	SCOPE	3
3.	ROLES AND RESPONSIBILITIES	4
4.	POLICY STATEMENT	5
4.1.	ENTITY AUTHENTICATION	5
4.2	WORKSTATION ACCESS CONTROL SYSTEM	5
4.3	DISCLOSURE NOTICE (BANNER)	6
4.4.	SYSTEM ACCESS CONTROL	6
4.5.	LIMITING USER ACCESS	6
4.6.	NEED-TO-KNOW	6
4.7.	COMPLIANCE STATEMENTS	6
4.8.	AUDIT TRAILS AND LOGGING	6
4.9.	CONFIDENTIAL SYSTEMS	7
4.10	SEGREGATION OF NETWORKS	7
4.11	ACCESS FOR NON-EMPLOYEE	7
4.12	UNAUTHORISED ACCESS	8
4.13	REMOTE ACCESS	8
5.	VIOLATION OF POLICY	8
6.	RELEVANT LEGISLATION	8
7.	RELATED POLICIES & PROCEDURES	8
8.	FEEDBACK	9
9.	DOCUMENT CONTROL AND OWNERSHIP	9

1. POLICY INTRODUCTION

The purpose of the access control policy is to establish processes to control access and use of National Ambulance information resources. Access management incorporates role based access controls (RBAC), privileged user access, access definitions, roles, and profiles.
Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorized use. Information is an important, valuable asset of National Ambulance which must be managed with care. All information has a value to the Company. However, not all of this information has an equal value or requires the same level of protection. Formal procedures must control how access to information is granted and how such access is changed. This policy defines the control requirements surrounding the management of access to information on National Ambulance computers and communications systems.

2. SCOPE

This policy applies to all National Ambulance Departments, Partners, Employees (including IT System support staff with access to privileged administrative passwords), contractual third parties and agents of National Ambulance with any form of access to National Ambulance information and information systems.

This policy applies to all information technology (IT) / Security personnel and contracted vendors involved in activities that cause or require changes to technology solutions within the Information Technology Environments. Therefore the scope of the Access Control Policy includes the following:
•All IT Supported National Ambulance locations
•All environments subject to the Access Control Policy determined by the IT Department
Affected Systems: This policy applies to all computer and communication systems owned or operated by National Ambulance and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

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 Access Control Policy. • Shall develop, maintain, and publish standards, processes, procedures and guidelines to achieve compliance with this Access Control Policy. • Shall Annually review the Access Control processes, standards and procedures, to achieve compliance with this Access Control Policy and shall support the Access Control Strategy and provide security specific input and guidance where required.
System Administrator	• Creating users in the AD and assigning privilege based on Role and need to know. • Implementing user access control in line with this policy e.g. defining password complexity, password allowed lifetime etc.
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

TYPES OF ACCESS CONTROLS ADDRESSED BY THIS POLICY

Below are the various types of access control addressed by this policy:

4.1. Entity Authentication

Entity Authentication: Any User (remote or internal), accessing National Ambulance networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- ✓ Automatic logoff
- ✓ And unique user identifier
- ✓ At least one of the following:
  - Biometric identification
  - Password
  - Personal identification number
  - A telephone callback procedure
  - Token

4.2. Workstation Access Control System:

All workstations used for National Ambulance business activity, no matter where they are located, must use an access control system approved by National Ambulance In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOs. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly lock or log out of all applications and networks. Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 10 minutes). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

Exceptions to timed logout or screen loc exist for systems critical to timely patient care 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

4.3. Disclosure Notice (Banner):

A warning notice banner A notice warning on the other also called “Banner” that those should only access the system with proper authority will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network, system or application and those unauthorized users should disconnect or log off immediately.

4.4. System Access Controls:

System Access Controls: Access controls will be applied to all computer-resident information based on its’ Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

National Ambulance follows the Data Classification scheme as outlined in the Department of Health: Abu Dhabi Healthcare Information and Cyber Security (ADHICS) Standard as outlined in COP401

4.5 User Access:

User Access: National Ambulance approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized.

4.6 Need-to-Know:

Need-to-Know: Users will be granted access to information on a “need-to-know” basis. That is, Users will only receive access to minimum applications and privilege required performing their jobs.

4.7 Compliance Statements:

Compliance Statements: Users which access National Ambulance’s information systems must have a current NDA non-disclosure agreement from the (HR) prior to issuance of a user-ID. A signature on this compliance statement or NDA indicates the user understands and agrees to abide by these National Ambulance policies and procedures related to computers and information systems.

4.8 Audit Trails and Logging:

Audit Trails and Logging: Logging and auditing trails are based on the Data Classification of the systems.

4.9 Confidential Systems:

Confidential Systems: Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- ✓ Access time
- ✓ User account
- ✓ Method of access

All privileged commands must be traceable to specific user accounts
In addition logs of all inbound access into National Ambulance's internal network by systems outside of its defined network perimeter must be maintained.
Audit trails for confidential systems should be backed up and stored in accordance with National Ambulance back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis. Audit results should be included in periodic management reports.

4.10 SEGREGATION OF NETWORKS

National ambulance networks is segregated according to the confidentiality of information capable of being distributed with the said network:-

- NAC Corporate – Authorized to carry all NA information up to and including Confidential information both Wired and Wirelessly including IPT telephony information.
- NAC Mobile – Authorized to carry public access and restricted information under a SSL connection
- NAC Guest – No Access to non public systems, only authorized to carry public access information unless protected by SSL, VPN or other secure wrapper.

Internet Cloud – Public access information only, SSL protected restricted information SSL and VPN protected Confidential information from and two protected endpoints.

Communication between the different networks is controlled and restricted by firewall appliances.

4.11 Access for Non-Employees:

Access for Non-Employees: Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use the National Ambulance computers or information systems unless the written approval of the Department Head has first been obtained And a company NDA is in place. Before any third party or business partner is given access to National Ambulance computers or information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.

4.12 Unauthorized Access:

Unauthorized Access: Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. System privileges allowing the modification of 'production data' must be restricted to 'production' applications.

4.13 Remote Access:

Remote access must conform at least minimally to all statutory requirements including but not limited to ISO27001:2013, NESA, DOH-ADHICS etc.

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

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
1.0	07-11-2019	New Policy
2.0	23-09 2020	- Remove " info security" from Roles and Responsibility. - Add exceptions to timed logout - Tracked changes enable, all updates made to meet ADHICS requirement - Added "Segregation of Networks"

CEO Approval

Board Member Verification