Clear Screen Clear Desk Policy

ITP121

Table of Contents

1. POLICY INTRODUCTION

The clear desk and clear screen policy refers to practices related to ensuring that sensitive information, both in digital and physical format, and assets (e.g., notebooks, cellphones, tablets, etc.) are not left unprotected at personal and public workspaces when they are not in use, or when someone leaves his workstation, either for a short time or at the end of the day.

Information is an asset. Like any other business asset it has a value and must be protected. Systems that enable us to store, process and communicate this information must also be protected in order to safeguard information assets. 'Information systems' is the collective term for our information and the systems we use to store, process and communicate it.
This document should be read in conjunction with the National Ambulance Corporate COP403 General Confidentiality Policy – which is also stored in the N: Drive

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure and damage. By ensuring that staff securely lock away all papers at the end of the day, when they are away at meetings and over lunchtime this risk can be reduced.
Security risks of unauthorised access to electronic records are also prevalent when PC screens are left unattended.
Clear desks and clear screens also ensure that National Ambulance projects a professional and efficient image to visitors, members of the public and colleagues.

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.
This policy sets out National Ambulance's requirements for each member of staff to protect any documents or records which are kept at their desk/workstation either temporarily or permanently and covers records in all formats including:

- Paper
- Electronic documents
- Patient Care Record (Paper or Electronic)
- Emails
- Visual images such as work related photographs

- Audio and video tapes, CDs, DVDs and cassettes
- Memory sticks and portable hard drives
- Databases

3. ROLES AND RESPONSIBILITIES

ROLE	FUNCTIONAL RESPONSIBILITIES
Responsible Executives	• Approve and formally support this policy
IT Department & Information Security	• Educate and Train users through formal and informal process to ensure compliance with this Clear Desk Clear Screen Policy. • Shall develop, maintain and publish standards, processes, procedures and guidelines to achieve compliance with this Clear Desk Clear Screen Policy.
NA Employees / Users	• Adhering to the requirements of this policy and any associated policies, guidelines or procedures

4. POLICY STATEMENT

PRACTICES OF CLEAN DESK/CLEAR SCREEN POLICY

4.1 Use of locked areas:

Lockable drawers, archive cabinets, safes, and file rooms should be available to store information media (e.g., paper documents, USB flash drives, memory cards, etc.) or easily transportable devices (e.g., cellphones, tablets, and notebooks) when not required, or when there is no one to take care of them. Beyond the protection against unauthorized access, this measure can also protect information and assets against disasters such as a fire, earthquake, flood, or explosion.

4.2 Protection of devices and information systems:

Computers and similar devices should be positioned in such a way as to avoid people passing by to have a chance to look at their screens, and configured to use time-activated screen savers i.e. lock after 10 mins idle time and password protection to minimize chances that someone takes advantage of unattended equipment. Additionally, information systems should be logged off when not in use. At the end of the day the devices should be shut down, especially those network-connected (the less time a device is on, the less time there is for someone to try to access it).

4.3 Restriction on use of copy and printing technology:

The use of printers, photocopiers, scanners, and cameras, for example, should be controlled, by reducing their quantity (the fewer units available, the fewer potential data leak points) or by the use of code functions that allow only authorized persons to have access to material sent to them. And, any information sent to printers should be retrieved as soon as practicable.

4.4 Adoption of a paperless culture:

Documents should not be printed unnecessarily, and sticky notes should not be left on monitors or under keyboards. Remember, even little pieces of information may be sufficient for wrongdoers to discover aspects of your life, or of the organizations' processes, that can help them to compromise information.

4.5 Disposal of information remaining in meeting rooms:

All information on white boards should be erased and all pieces of papers used during a meeting should be subject to proper disposal (e.g., by using a shredder).

5. PROCEEDURES FOR CLEAN DESK/CLEAR SCREEN

5.1 Clean Desk Procedure

Personal confidential information must be locked away when not in use and never left unattended. Ideally, all staff should leave their desk paper free at the end of the day. Ensure that you select an appropriately located printer where you are able to retrieve your printing immediately. Do not leave personal confidential information for others to find. An easy way to comply with the clear desk procedure is to work with electronic documents whenever possible – "do you need to print it"?

Ensure documents are disposed of securely. Never put documents containing sensitive, personal or corporate sensitive information in the general waste bins. Use the confidential paper shredding boxes.

All Portable Computing & Data Storage Devices (PCDs) such as USB data sticks, mobile phones and laptops should be placed out of sight, preferably locked away at the end of the working day.

5.2 Clear Screen Procedure

Always lock the desktop when leaving the workstation/desk unattended. If using a shared workstation/desk log off rather than lock it. If anticipating an absence of 30 minutes or more log off or shutdown the computer. This also applies when using a laptop. Pressing CTRL+ALT+DEL and clicking 'Lock this computer' is straight forward and simple. However, a windows key combination is even simpler. Press windows key + L and your computer will lock automatically.

(The windows key can usually be found in the bottom left of the keyboard and looks like a flag/window.)
To unlock press CTRL+ALT+DEL and log back in.
Always be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by unauthorised people while in use.

6. BREACHES OF POLICY

Compliance to this policy can be verified through various methods, including but not limited to, periodic walkthroughs, internal and external audits, and feedback to the policy owner. An employee found to have violated this policy may be subject to disciplinary action.

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

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

Policy & Procedure /Form

9. FEEDBACK

Any feedback or suggestions for improvement to this Policy, Processes or Procedures can be submitted to ghse@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:

Ahmed Alkindi
IT manager

_____

This controlled document is managed / overseen by IT Manger

Change Brief

Version No.	Date	Change
1	18/12/2019	*Created the initial draft of this document*

CEO Approval

Board Member Verification