Clear Desk & Clear Screen Policy

Version 1.0

Revision History

Version #	Date (DD-MMM-YYYY)	Details of the Changes	Modified By	Reviewed & Approved By
1.0	16 Jan 2024	First Release	Manu Mitragotri	Sridhar Reddy

Introduction

Quadrant is committed to ensuring the security of its information assets and complying with all applicable laws and regulations in its handling of sensitive data. It is important that all employees and others with access to classified information take care to ensure that unauthorised people do not have access it through being able to view it either on paper, on removable media or on a user's screen.

This policy sets out the actions that should be taken to ensure that this information remains secure, both during the working day and out of hours.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Quadrant systems.

The following policies and procedures are relevant to this document:

- *Information Classification Procedure*
- *Physical Security Policy*
- *Procedure for Working in Secure Areas*
- *Mobile Device Policy*
- *Teleworking Policy*
- *Procedure for the Management of Removable Media*
- *Acceptable Use Policy*

Clear desk and clear screen policy

This policy applies to information that has been defined as Confidential and Restricted in accordance with Quadrant Information Classification Procedure.

The following actions must be taken to ensure the security of information displayed on a computer or device screen:

- Screens must be locked when unattended, so that classified information is not displayed, and no access is available to restricted systems
- Screen locks must be protected by a password (or other approved mechanism) that meets organization policies on strength
- Care must be taken that screens are not sited such that the information displayed on them can be easily seen by unauthorised people
- Users must remain aware of situations in which their screen may be overlooked by unauthorised people, including visitors
- Cameras or other recording devices must not be used in the vicinity of screens which may display classified information

Creation and handling of printed materials containing classified information must conform to the following controls:

- Where possible, the printing of classified information must be avoided
- When classified information is printed, care must be taken that printouts are not accessible to unauthorised people

- PIN-protected facilities (or similar) must be used where available when printing classified information
- When unattended, classified printed information must be locked away and appropriate control exercised over the key or other security mechanism
- Classified printed materials must not be left on desks (or other unsecured areas) outside of office hours
- Use of photocopiers must be subject to access controls to prevent their use by unauthorised people

In general, use of removable media must be subject to the controls described in Procedure for the Management of Removable Media. Approved media that is used in an office environment must be subject to the following additional controls:

- Removable media, such as memory sticks and storage cards, that contain classified information must not be left unattended e.g. on desks
- Outside of working hours, removable media must be secured appropriately e.g. in a locked drawer or cabinet

In addition to the above, care must also be taken over classified information that may be displayed on other media, such as whiteboards, flip charts, and sticky notes. These must be wiped or removed after use so that the classified information is no longer displayed.