Clear Desk and Clear Screen Policy

Objective and Scope

The objective of this document is to prescribe the clear desk and clear screen standards for the protection of personal information and sensitive data content. This applies to papers and removable storage media and clear screen protocols.

The scope of this policy covers the use of computer and digital screens and workspace practices that ensure sensitive information is protected. This includes both digital and paper based sensitive information. Assets include mobile phones, computers and other electronic devices that access data.

Roles, Responsibilities and Authorities

The Operations Director shall set the rules for workspace management, including clear desk and clear screen standards.

Individuals have an obligation to follow the policy directions and report to an IT delegate or ISMS representative if there is any suspected breach.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The Change Management Procedure may need to be enacted.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Equipment	8.0	11.2		6.4
Clear desk clear screen policy		11.2.9		7.7

Clear Desk and Clear Screen Policy

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	ISO 27001: 2022 Clause ID	ISO 27002: 2022 Control ID

Related Information

- Data Breach Notification
- Disciplinary process documentation

Policy

To reduce the risks of unauthorised access, loss of and damage to sensitive information on a workspace such as desks, screens and in other accessible locations during and outside normal working hours, Prevision Research has standard rules to be followed.

Sensitive information in any workspace in any form shall not be left unprotected or accessible to any person other than the designated user.

A workspace can be any of the following:

- Your desk or anywhere in the office
- In a motor vehicle or other forms of transport
- Accommodation outside the home
- Home office or anywhere at home
- In any other public space

Information and assets at any of the workplaces listed are vulnerable to either loss, disclosure or unauthorised use.

Mandatory Protective Measures

The risk of vulnerability of personal information or sensitive data is greatest when the asset owner is not in attendance. The following guidelines should be followed to limit this risk.

Workspace: General

- Use lockable areas such as a drawer, cabinet or room to store paperwork and devices.
- Do not use or create multiples of documents, multiple USB's with variation or versions of secure data, multiple files on desktop and laptop computers. The more versions and assets the greater the risk.
- Whiteboards shall not be used to display sensitive information.
- When presenting to an audience via a computer, ensure notifications of emails and other information is inactivated for the period of the presentation.

Clear Desk and Clear Screen Policy

Computers

- Computers and other devices should be positioned to avoid content being read off screens by people passing by.
- All devices should have a time activated screensaver, requiring password activation to reinstate the user.
- Always log off and close down computers at the end of day OR before travelling with portable devices.

Printing and Copying

- Restrict the use of photocopying or multiple printed technology and ensure any printed material is retrieved from the devices as soon as possible..
- DO NOT reuse or recycle paper that is commercially, privacy or otherwise contains sensitive information. When no longer required, shred or cross shred for highly sensitive content.
- A paperless office is a secure office.
    a. Less paper copies, the more secure the data
    b. Sticky notes with passwords left on monitors compromises information security
    c. White boards should be cleaned after use
    d. After finishing meetings, collect all paperwork not used and destroy according to classification of information

Travelling

Assets in vehicles may be lost or stolen.

- Don’t leave mobile phones in clothing pockets when getting in or out of vehicles
- Shut down computers before placing in a vehicle
- Place computers and other mobile assets out of sight in a car storage area such as a boot for larger assets and glove box for smaller assets. Where practical, don’t leave assets in the car
- Paperwork should be contained in a briefcase or bag, not as loose paper. Lockit in the boot and remove it from the vehicle as soon as possible. Do not leave paperwork in vehicle overnight or for extended periods of time

Working from Home

Home offices are a designated workspace in the home. This does not mean every room in the home is a workspace.

- Assign a designated only working area and contain assets and paperwork in this area
- Do not allow other members of the household to access work assets as this can compromise information security.
- Do not share passwords or allow games or non-work related Apps to be downloaded.
- Paperwork taken home must not be of a secure nature as home offices are rarely as secure as normal work premises

Clear Desk and Clear Screen Policy

A Clear Screen also means that no sensitive data is stored on the desktop of your computer.

- Do not keep secure data folders or files on the desktop
- All electronic data shall be contained in designated drives
- Work in Progress to be moved to secure drives at end of the work day
- Avoid working off desktops

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N