Clear Desk, Clear Screen Policy

1. Introduction

1.1 A 'Clear Desk, Clear Screen Policy' will help ensure that all sensitive/confidential materials are removed from workspaces and locked away when the items are not in use or an employee leaves their workstation. The policy will help reduce the risk of security breaches within the workplace.

1.2 This document supplements Intech Centre's Information Security Policy and should be read in conjunction with it.

2. Responsibility

2.1 The responsibility for the production and maintenance of this document is with the Senior Manager as detailed within the Information Security Policy. He will also ensure that any substantive changes made will be communicated to all relevant personnel.

2.2 It is also the responsibility of the Senior Manager to ensure that the policy set is and remains internally consistent.

2.3 It is the responsibility of the Centre Manager to ensure that this policy is implemented and to ensure that regular clear desk, clear screen audits take place (see section 7).

3. Scope

3.1 This policy applies to all permanent, temporary or contracted staff employed by Intech Centre and to students and volunteers who can access information under supervision.

4. Purpose and Objectives

4.1 The purpose and objectives of this policy are in addition to those detailed within Intech Centre's overriding Information Security Policy.

4.2 The purpose of this policy is to establish the minimum requirements for maintaining clean desks and clear screens and to ensure that, where there is any confidential, restricted or sensitive Information that it is locked away and is out of site.

5. Clear Desk Policy

5.1 Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.

5.2 Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office doors must be locked if left unattended.

5.3 Hard copy documents containing any personal data, or confidential, restricted or sensitive information should only be stored if necessary. e.g. learner had copy work that needs to be scanned and sent to the prime contractor. Original paper copies should be securely stored in confidential shredding bags for destruction.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

5.4 Employees are required to ensure that all confidential, restricted or sensitive information in hardcopy or electronic form is secured at the end of the day and when they are expected to be away from their desk for an extended period.

5.5 Any confidential, restricted or sensitive information must be removed from desks and locked in a drawer when a desk is left unoccupied at any time.

5.6 Confidential, restricted or sensitive information, when printed, should be cleared from printers immediately. Where possible printers with a 'locked job' facility should be used.

5.7 It is good practice to lock office areas when they are not in use and it is safe to do so.

5.8 Any visit, appointment or message books should be stored in a locked area when not in use.

5.9 The reception area can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times. No personally identifiable information should be kept on desks within reach or sight of visitors.

5.10 It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.

5.11 Keys used for access to confidential, restricted or sensitive information must not be left in or on an unattended desk. Keys for desk drawers, cabinets and other secure areas must be stored in the dedicated key safe.

5.12 Upon disposal, any document containing any personal data or confidential, restricted or sensitive information should be placed in the confidential shredding bags which are stored in locked secure locations. Confidential waste must not be left on desks, in filing trays or placed in regular waste bins.

6. Clear Screen Policy

6.1 Computer terminals should not be left logged on when unattended and should always be password protected.

6.2 Computer screens should be angled away from the view of unauthorised persons.

6.3 Computer workstations must be logged off at the end of the working day, to allow security updates to be installed during the evening.

6.4 The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period of time.

6.5 The Windows Security Lock should be password protected for reactivation.

6.6 Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down and left in an accessible location.

6.7 Users should log off or lock their machines (by pressing the Windows key and L) when they leave the room.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

6.8 Whiteboards containing restricted and/or sensitive information should be erased.

6.9 Portable computing devices such as unused laptops, digital cameras and tablets must be locked away in a drawer or the server room.

6.10 Mass storage devices such as USB sticks should be treated as being sensitive data and must locked away in a drawer or the server room.

7. Maintaining Compliance

7.1 Regular and ongoing Clear Desk, Clear Screen audits will be undertaken to ensure continued employee compliance with this policy.

7.2 Clear Desk, Clear Screen audits will be documented and logged as per Intech Centre's documented 'Clear Desk Audit Process'. This process will be reviewed annually. It is the responsibility of the Senior Manager to ensure reviews take place.

7.3 The auditee must provide the relevant employees name, date of the audit and tick Pass or Weakness for each section. Any identified issues or areas of weakness should also be documented.

7.4 Where a weakness has been logged, the auditee must email that member of staff with the following example text.
'We conducted an audit on Thursday 2nd July and found a weakness.
Weakness Explained - Clients files and information left in tray on desk There is a requirement as part of your role to comply with GDPR Data Protection Act and as such this incident is classed as a breach. Please ensure at the end of each day all confidential information is locked away and the desk is left clear. This incident has been logged and I would therefore be grateful if you could sign and return the attached document to me by email which will then be saved in your staff file. Please note, as per the Clear Desk, Clear Screen Policy, persistent breaches of the policy will be regarded as a disciplinary incident and will be treated as such.'

7.5 Both the above email and the signed scanned audit report should then be logged in the relevant employees file under the disciplinary section and reported to the employee's line manager.

7.6 Further training will be provided when and where required.

7.7 Persistent and repeated breaches of the policy should be referred to the Senior Manager.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com