Clear Desk and Clear Screen Policy

Version History

Ver. No.	Release Date	Description of Change	Authored / Revised By	Reviewed By	Approved By
0.1	16nd Aug 2013	First Draft	Saket Madan	Dhananjay Kumar	Ajay Kr. Zalpuri
1.0	22nd Aug 2013	Initial Release	Saket Madan	Dhananjay Kumar	Ajay Kr. Zalpuri
1.1	12th July 2017	Update in policy for shredder	Rahul Raj	Dhananjay Kumar	Ajay Kr. Zalpuri
1.2	14th Aug 2018	Update in policy for viewing sensitive information	Rahul Raj	Dhananjay Kumar	Ajay Kr. Zalpuri
1.3	10th June 2020	Update section 3.0 for clear desk clear screen and separate the policy term for clear desk and clear screen. Also add section4 for policy compliance	Rahul Raj		

1. Introduction

A ‘Clear Desk Clear Screen Policy’ will 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 to reduce the risk of security breaches within the workplace.

2. Objectives

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.

3. Clear Desk and Clear Screen Policy

Clear Desk Policy

- Where appropriate, paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.
- Hard copy documents containing any personal data, or confidential, restricted, or sensitive information should only be stored if necessary.
- 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.
- Any visit, appointment or any logbooks should be stored in a locked area when not in use.
- The reception area can be particularly vulnerable to visitors. This area should always be kept as clear as possible. No personally identifiable information should be kept on desks within reach or sight of visitors
- 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.
- 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
- Incoming and outgoing mail points and unattended fax and telex machines shall be protected.

- Personal computers and computer terminals and printers shall not be left logged on when unattended and shall be protected by key locks, passwords or other controls when not in use.
- Photocopiers shall be locked (or protected from unauthorized use in some other way) outside normal working hours.
- Paper containing sensitive or classified information must be removed from printers and faxes immediately. Faxes and printers used to print sensitive information should not be in public areas. Any time a document containing sensitive information is being printed the user must make sure they know the proper printer is chosen and go directly to the printer to retrieve the document.
- Sensitive information on paper or electronic storage media that is to be shredded must not be left in unattended boxes or bins to be handled at a later time, and must be secured until the time that they can be shredded

Clear Screen Policy

- Computer terminals should not be left logged on when unattended and should always be password protected.
- Enable screen saver password if you are going to be away from the system for more than 5 minutes.
- While switching off the desktop, log off from all the applications shut down the PC and power-off properly.
- Always protect the sensitive files by using passwords.
- 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.
- Whiteboards containing restricted and/or sensitive information should be erased.
- When viewing sensitive information on a screen, users should be aware of their surroundings and should ensure that third parties are not permitted to view the sensitive information.
- Portable computing devices such as unused laptops, Mobile devices and tablets must be locked away in a drawer or the server room.
- Mass storage devices such as CDROM, DVD or USB drives should be treated as being sensitive data and must locked away in a drawer or the server room

4. Maintaining Compliance

- Regular and ongoing Clear Desk Clear Screen audits will be undertaken to ensure continued employee compliance with this policy.
- Persistent and repeated breaches of the policy should be referred to the Chief Information Security Officer