Clear Desk and Clear Screen Policy

1 INTRODUCTION

1.1 Purpose

Equipment and information assets are always to be safeguarded appropriately, especially when left unattended.

1.2 Goals & Objectives

The goal is to ensure the security of all sensitive information. It outlines the user's role and responsibilities for compliance with this policy. The primary goal is to ensure consistency and integrity of all SYBRID informational resources and protect them from unauthorized access, loss and damage. The policy will apply to both working and non-working hours.

2 POLICY

2.1 Policy Statements

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted according to which:

1. Clean desk policy means only published documents on desk e.g. Books, Magazines etc. No other paper document can be left unattended at work areas.
2. Although published materials are acceptable on the desks, it will be a good practice to keep the desk completely clean (no unattended material on the desk)
3. Sensitive information in any form (processes electronically, on paper or removable storage media) should not be left unattended.
4. Sensitive or critical business information e.g. on paper or on electronic storage media should be locked away (ideally in your safe or cabinet) when not required, especially when the office is vacated.
5. All documents should be properly organized and filed to avoid any loss.
6. Computers and terminals should be left logged off / locked and protected with a screen and a keyboard locking mechanism controlled by a password when unattended.
7. Never leave your system unattended and don't allow the shoulder surfers to gain access to secret/ confidential information. Lock your system when someone tries to look at your screen intentionally.

8. Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras etc.) should be prevented.

9. Don't leave the papers unattended at the printer tray.

10. Use paper thresher to destroy the documents you no longer need and don't just throw them in dustbins.

11. Incoming and outgoing mail points and unattended facsimile machines should be protected.

12. Classification of information should be done to identify the sensitivity of information.

13. Photocopier should be password protected and rights to be granted only to authorized user(s) identified by Head of Department following the Access Control Policy

2.2 Roles and Responsibilities

The information security manager shall be responsible for monitoring compliance with the policy. The following measures will be followed by the Information Security Officer to monitor compliance:

1. Visually examine desks on a fortnightly basis (every two weeks)

2. Examine a sample of desks. These shall be spread out over both floors, evenly spread across the entire floor.

3. Desks that do not comply with the policy shall be photographed. The photograph along with the name of the person using the desk shall be recorded. A compiled risk of all photographs and names for non-compliant desks shall be emailed to the HR Manager.

4. Each non-compliant desk discovered shall be logged as a *security incident* by the Information Security Manager.

5. The admin officer will be responsible for reminding the offenders of the details of the policy.

6. Any SYBRID employee found to have violated the policy two times in a quarter shall be deemed a "Repeat Offender". Repeat offenders may be subjected to disciplinary action or as suggested otherwise by their managers