Clean Desk Clear Screen Policy

Wood must adopt a clean desk and clear screen policy for papers, and digital removable media in order to reduce the risk of unauthorised access, unauthorised viewing, loss of and damage to information at all times.

Purpose:

The purpose of this policy is to establish the minimum requirements for maintaining a clean desk and clear screen to ensure confidential, sensitive, and secret information about our employees, our intellectual property, our customers, and our vendors is secure and out-of-sight.

Scope:

This policy applies to all employees, contractors, third-parties, or other agents (hereafter referred to as "users") who access Wood information on any device with a screen, have a physical workplace or work remotely.

Policy Requirements:

Users must:

- Ensure all data other than public classified data is not exposed to unauthorized individuals at all times.
  - When not present at their desk, users must lock their workstation.
- Use security screens on devices if accessing or processing sensitive/secret data.
- Ensure the physical security of portable computing devices (such as phones, laptops, or tablets), and removable media (such as CDROM, DVD, or USB drives) in accordance with the Removable Media Policy and Remote Working practices (see IT Acceptable Use Policy).
  - At the end of the working day, users must take their portable devices home and keep them in a safe location.
  - Unattended portable computing devices in the office must be secured and locked away to prevent damage, theft and data breach.
- Ensure electronic information displayed on their screens when working remotely outside of the privacy of a Wood location (restaurant, train, plane, airport, etc.) is protected from others' sight.
- Store working papers in a locked drawer or filling cabinet if going to be away for extended periods of time, such as a lunch break:
  - Wood provides locking desks and filing cabinets to enable this policy.
  - Keys used to access such desks and cabinets must secured to prevent access by unauthorized individuals.
- Erase whiteboards containing Wood information.
- Remove printouts containing Wood information immediately from the printer.
- Ensure appropriate safeguards are in place when processing all data not classified as public data at home.
- Irrespective of location, dispose Wood information by shredding in official shredder bins or using confidential waste bins.

Any exceptions to this policy are subject to approval by the SRC team in advance via Service Desk "Request an exception."

If you observe others violating this policy, intervene and suggest corrective action or report it to your line manager, HSSE, or raise a security incident.

Reference Documents:

- Information Security Policy
- IT Acceptable Use Policy
- Data Protection Policy
- Password Policy
- Removable Media Policy
- Data Classification Guideline

Name	Andrew Thom
Position	VP Security Risk & Compliance
Date	30 April 2024