

PDS INFOTECH PVT LTD

Clear Desk, Clear Screen & Device Decommissioning Policy

Ref No: ISMS/PDS/5.2/6.1

1. Purpose

This policy establishes the requirement to secure sensitive and confidential information at workstations, desks, and screens, whether attended or unattended, and to ensure that decommissioned or reassigned devices do not retain residual data.

2. Scope

This policy applies to all employees, contractors, and third parties working from PDS Infotech Pvt Ltd's ("the Company") premises or accessing Company information resources remotely.

3. Policy

3.1 Clear Desk

- Confidential or sensitive documents must not be left unattended on desks, printers, fax machines, or common areas.
- Documents containing confidential information must be stored in a locked drawer or cabinet when not in use and at the end of the workday.
- Whiteboards, notice boards, or meeting room screens containing confidential information must be cleared after use.
- Passwords, access codes, or authentication details must never be written down or left visible at a workstation.

3.2 Clear Screen

- Personnel must lock or log off their workstation or laptop whenever it is left unattended, even briefly.
- All workstations must be configured to auto-lock after a defined period of inactivity, as set by IT Management.
- Confidential information must not be left open or visible on-screen in shared or publicly accessible areas.

3.3 Device Decommissioning and Reassignment

- Where a computer or laptop is to be retired or reassigned, all relevant data must first be backed up and/or transferred to the new system, and the transfer verified.
- Once verified, the original device must be securely wiped (hard formatted, or equivalent secure erasure) to ensure no residual data remains.
- Upon an employee's exit, the allotted desktop or laptop must be returned to IT Management. All irrelevant data must be removed and relevant business content archived, following due diligence to confirm no sensitive or extraneous information remains before reassignment to the next user.

4. Roles and Responsibilities

- IT Management: Configures auto-lock settings, performs secure data wipes, and manages device reassignment.
- All Personnel: Maintain a clear desk and locked screen at all times when away from their workstation.

5. Review

This policy shall be reviewed at least annually, or upon significant organizational or regulatory change, to ensure continued alignment with ISO/IEC 27001:2022.