

## CLEAN DESK POLICY

Effective Date	
Reviewed by	
The next scheduled review date	
Supersedes	All previous similar policies
Approved by	
Date Approved	

**1.1 Purpose** This policy establishes the minimum requirements for maintaining a "clean desk," ensuring that sensitive and critical information about our employees, intellectual property, customers, and vendors is secure in locked areas and out of sight. This Clean Desk policy is ISO 27001/17799 compliant and part of standard privacy controls.

A clean desk policy is an important tool for ensuring that all sensitive or confidential materials are removed from an end-user workspace and securely stored when they are not in use or when an employee leaves their workstation. Implementing this policy reduces the risk of security breaches in the workplace and increases employee awareness about protecting sensitive information. **2.0 Clean Desk Policy**

- ☐ Employees must ensure that all sensitive or confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are away for an extended period. **Computer workstations** must be locked
- ☐ when the workspace is unoccupied. **Computer workstations** must be fully shut
- ☐ down at the end of the workday. Any **Restricted** or **Sensitive** information must
- ☐ be removed from desks and
- ☐ locked in a drawer when the desk is unoccupied and at the end of the workday. **File cabinets** containing Restricted or Sensitive information must be closed
- ☐ and locked when not in use or not attended. **Keys** used to access Restricted or Sensitive information must not be left at an
- ☐ unattended desk. **Laptops** must be secured with a locking cable or in a drawer.
- ☐ **Passwords** must not be left on sticky notes posted on or under a computer or
- ☐ in an easily accessible location.

- **Printouts** containing Restricted or Sensitive information should be immediately removed from the printer.
  - Upon disposal, Restricted or Sensitive documents must be shredded in the official shredder bins or placed in locked confidential disposal bins.
- **Whiteboards** containing Restricted or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat **mass storage devices** such as CD-ROMs, DVDs, or USB drives as sensitive and secure them in a locked drawer.
- All **printers and fax machines** should be cleared of papers as soon as they are printed to ensure sensitive documents are not left in printer trays for the wrong person to pick up.

## 3.0 Policy Compliance

### 3.1 Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback from the policy owner.

### 3.2 Exceptions

The Infosec team must approve any exception to this policy in advance.

### 3.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Maintaining a clean desk is a key component of our company's commitment to protecting sensitive information, and adherence to this policy is essential in ensuring that confidential materials remain secure at all times.