CLEAN DESK POLICY

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS

DVD	Digital Versatile Disc
ISO	International Organization for Standardization
USB	Universal Serial Bus

DEFINITION OF CLEAN DESK

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee or a student leaves his/her workstation. This policy will reduce the risk of unauthorized access, loss of and damage to information during and outside of normal working hours or when workstations are left unattended. This policy can also increase students and employee's awareness about protecting sensitive information.

A Clean Desk Policy is an important security and privacy control and necessary for ISO 27001/17799 compliance.

BY THIS POLICY

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/confidential information about our students, employees, intellectual property, customers and other affiliates is secure in locked cabinets.

APPLIES TO

This policy applies to all {company} students, employees and affiliates.

POLICY GUIDELINES

Whenever a desk is unoccupied for an extended period the following will apply:

- All confidential or sensitive information must be removed from the desk and locked in a drawer or filing cabinet.
- File cabinets containing confidential or sensitive information must be kept closed and locked when not in use.
- Keys used for access to confidential or sensitive information should not be left unattended at a desk.

- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing confidential or sensitive information should be immediately retrieved from the printer.
- Upon disposal confidential or sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins. Under no circumstances should this information be places in regular wastepaper bins.
- Whiteboards containing confidential or sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as DVD or USB drives as sensitive and secure them in a locked drawer.
- Lock the computer screen or log off.

POLICY COMPLIANCE

Compliance Measurement

This policy will be monitored for compliance by information security team and may include random and scheduled inspections.

Exceptions

Any exception to the policy shall be approved by the information security manager in advance.

Non-Compliance

An employee or a student found to have violated this policy may be subject to disciplinary action.

RELATED STANDARDS, POLICIES AND PROCESSES

None

REVISION HISTORY

Version	Description	Date	Author	Approved By
1.0	Initial version	14/04/2025	ztothez	