CLEAN DESK POLICY

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

Purpose

The purpose of the Clean Desk Policy is to increase awareness amongst employees of Veranda Learning about protecting sensitive and classified information by keeping their work areas clean of sensitive documents and information.

Scope

The clean desk policy applies to following

- All Employees of Veranda Learning.
- All Contractors of Veranda Learning.
- All vendors/third-party/visitors who temporarily access Veranda Learning's equipment.

Background

Information theft and accidental exposure of sensitive information can lead to large scale data breaches and other attacks on the information systems. By keeping their work areas and desks clean all employees can contribute towards protecting confidential information of the company.

Policy

Laptops, computers, and other electronics

- All laptops and computers are locked when not used, and the user is not at their desk.
- Physical devices such as laptops will not be left unattended in public places or places not adequately protected by the company, such as user conferences and client meetings.
- Laptops to be kept in a drawer or secured by a locking cable when left unattended for more extended periods in the office, such as overnight

Work area (personal and shared)

- Personal work areas must be free of all confidential papers, reports, and printouts.
- No sticky notes or written down papers for passwords
- Remove sensitive printouts from the printer as soon as the print job completes
- Drawers and other restricted file cabinets must always be locked, and the keys must not be left in plain sight
- Employees must not leave sensitive notes or drawings on the whiteboard
- Employees must ensure that sensitive information is disposed of in reliable shredders and not left in disposal/trash baskets

Public events, common areas

- Whiteboards containing Restricted or Controlled data must be thoroughly erased.
- Printouts containing Restricted or Controlled information should be immediately removed from standard printers
- File cabinets containing Restricted or Controlled information must be kept closed and locked when not in use or when left unattended.
- Storage devices with sensitive information must be secured in a locked drawer.

Mapping with Industry Standards

This policy addresses the following risks related to Clean Desk and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (Confidentiality, Integrity and Availability)	7.7 Clear desk and clear screen
Non-adherence to the laws and regulations and Compliance	7.7 Clear desk and clear screen
Unauthorized access	7.7 Clear desk and clear screen
Information Leakage	7.7 Clear desk and clear screen
Theft	7.7 Clear desk and clear screen
Physical Loss or damage	7.7 Clear desk and clear screen 7.8 Equipment siting and protection

Enforcement

Clean desk policy is enforced by information security team. Information security team conducts regular audits of work areas by conducting walk throughs or with the help of building and floor admins.

Non- Compliance

Violations of the policy may subject employees to disciplinary action, including removal of privilege to the systems, up to and including termination of employment. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable Veranda learning policies.
- Termination of employment.
- Legal action according to applicable laws and contractual agreements.

Validity and Document Management

The owner of this document is the management, who must check and, if necessary, update the document at least once every 12 months.