Veranda

Physical Security 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 Physical Security Policy is to outline the security controls in place to authorize, monitor, and revoke access to physical premises of Veranda Learning.

Scope

Physical Security policy applies to

- All Employees of Veranda Learning
- All Contractors of Veranda Learning
- All vendors / third-party / visitors who temporarily access Veranda Learning datacenter or offices.
- All locations including physical office spaces, data centers and remote offices of Veranda Learning.

Background

Physical security is a must to protect employees, contractors, and other personnel within the office premises from unlawful and harmful acts by malicious external actors. Proper physical security also prevents bad actors from having easy access to data, information, and other assets owned by the organization. This policy outlines all measures in place at Veranda Learning to prevent such incidents.

Policy

General physical security procedures

- The primary objective of Veranda Learning's physical security policy is to ensure the physical security of its employees and information assets.
- All physical access to premises is secured by electronic key cards (or other means such as security guards, front desk staff, etc.)
- ID badges are always required on the person when on the office premises
- Physical access is reviewed quarterly
- Access cards are not allowed to be shared or used by other than the person to who the card was issued to
- All in / out activity is logged and monitored
- Lost or stolen cards must be reported immediately
- All terminated employees must return their key cards/badges to human resources or the IT team.
- All physical access will be revoked as per the access management policy

Visitor and Guest Access

- Guests are always accepted to wear and correctly display a guest pass
- All visitors must request and receive written onsite authorization from a staff member.
- Visitor access is tracked with a sign-in/out log.
- The log contains the visitor's name; the firm represented the purpose of the visit and onsite personnel authorizing access.
- The log is retained for a minimum of 90 days.

Mapping with Industry Standards

This policy addresses the following risks related to physical security and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Data Breach	7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats 7.10 Storage media 7.9 Security of assets off-premises C 10.1 Continual improvement
Unauthorized access	7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats 7.10 Storage media 7.9 Security of assets off-premises C 10.1 Continual improvement
Information Leakage	7.1 Physical security perimeters 7.5 Protecting against physical and environmental threats 7.6 Working in secure areas 7.10 Storage media 7.9 Security of assets off-premises 7.14 Secure disposal or re-use of equipment 8.1 User endpoint devices 7.7 Clear desk and clear screen C 10.1 Continual improvement
Theft	7.1 Physical security perimeters 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats 7.6 Working in secure areas 7.10 Storage media 7.9 Security of assets off-premises 7.7 Clear desk and clear screen
Physical loss and damage	7.2 Physical entry 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats 7.8 Equipment siting and protection 7.11 Supporting utilities 7.12 Cabling security 7.13 Equipment maintenance

Risk	Mapping to ISO 27001:2022

Enforcement

Information security team and at times security staff are accountable for enforcing physical security policy requirements.

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