VULNERABILITY MANAGEMENT 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 Vulnerability Management Policy is to outline the procedures put in place to identify new vulnerabilities in the Information Systems arising due to new threats or new product releases.

Scope

The vulnerability management policy applies to following

- All Information Systems of Veranda Learning.
- Internet and Intranet networks
- Cloud systems
- Personnel laptop / mobile devices
- Software procured

Background

Every day new threats sources try to take advantage of an organization's security vulnerabilities arising from

- Outdated software
- Missed patches/security updates
- New un-tested software release

With this policy, Veranda Learning aims to quickly identify these vulnerabilities and update security controls to mitigate these vulnerabilities.

Policy

Vulnerability assessment

- At Veranda Learning a vulnerability scan and assessment of all critical information systems are conducted at least once every 6 months. The scan includes
  - Network scan
  - Application scan
  - Server and computer scans
- The scan is conducted by a third-party vendor
- The scan tries to find vulnerabilities that are related to
  - Known vulnerabilities
  - Application vulnerabilities
  - Invalid configuration vulnerabilities
  - Others from the CVE database

Review of scan results

- Results of the scans are reviewed with the application teams, infrastructure team, and the InfoSec team
- The findings are categorized into High, Medium, and Low risk
- A mitigation plan for fixing the high and medium risk findings is immediately put in place.
- Patches are applied as per the Patch Management Policy

Vulnerability management

- A risk assessment must be conducted for all vulnerabilities discovered and appropriate controls must be put in place to mitigate and prevent the vulnerability from being exploited.

Mapping with Industry Standards

This policy addresses the following risks related to vulnerability management and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (confidentiality, Integrity, and Availability)	8.8 Management of technical vulnerabilities 8.9 Configuration management 8.19 Installation of software on operational systems C 10.1 Continual improvement
Data Breach	8.8 Management of technical vulnerabilities 8.9 Configuration management 8.19 Installation of software on operational systems C 10.1 Continual improvement
Unauthorized access	8.8 Management of technical vulnerabilities 8.9 Configuration management 8.19 Installation of software on operational systems C 10.1 Continual improvement
Information Leakage	8.8 Management of technical vulnerabilities 8.9 Configuration management 8.19 Installation of software on operational systems C 10.1 Continual improvement

Enforcement

Infosec team is responsible for conducting and scheduling regular vulnerability scans. Each application system is responsible to work with the Infosec team to conduct vulnerability scans for their application

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