ANTIVIRUS 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 Antivirus Policy establishes requirements that must be met by all computers (laptops, desktops, mobile devices) and servers connected to Veranda Learning network to ensure effective detection and prevention of the virus, malware, and trojan.

Scope

The Antivirus Policy applies to all computers, mobile devices, and servers that Veranda Learning is responsible to manage. This policy also applies to any system that Veranda Learning has a contractual obligation to administer.

Background

New viruses are discovered almost every day. Therefore, it is necessary that organization adopt a standard approach to deploy anti-virus application across all computers and servers. The anti-virus solution or software should guard against malicious software or scripts by blocking or quarantining the malicious software that is identified, and alerting administrators that such action has taken place

Policy

Computers

- All Veranda Learning's computers must have the Company's standard and supported antivirus software installed and scheduled to run regularly. In addition, the antivirus software and the virus pattern files must be kept up to date. Virus-infected computers must be removed from the network until verified as virus-free.
- The IT team is responsible for establishing procedures to ensure that antivirus software is executed regularly, and computers are verified as virus-free. Different procedures must be implemented for Macintosh and Windows computers.
- Malicious code that is identified should be blocked, quarantined, and an alert is sent to the administrators.
- According to the Acceptable Use Policy, any activities to create and distribute malicious programs into Veranda Learning's networks (e.g., viruses, worms, Trojans, etc.) are prohibited.
- The end users cannot disable the antivirus software on their devices.
- Audit logs of the scans should be kept for future reference. (e.g., Audit)

Antivirus on Servers

All servers must have an antivirus application installed that offers real-time scanning protection to files and applications running on the target system. Following servers must have an antivirus software

- File servers

- HTTP/FTP servers open to the Internet
- Other risky protocols/applications on the network
- Systems with outbound web access

Mail Server

- If the target system is a mail server, it must have an external or internal antivirus scanning application that scans all mail destined to and from the mail server.

Internet Gateway

- Antivirus must be deployed at the perimeter of Veranda Learning's network to block viruses, worms, trojans, and spyware before they can infect internal systems.

Mapping with Industry Standards

This policy addresses the following risks related to Virus Management and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (Confidentiality, Integrity and Availability)	8.7 Protection against malware 8.15 Logging 6.7 Remote working
Security Breach	8.7 Protection against malware 8.15 Logging 6.7 Remote working

Enforcement

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

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

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 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.