PATCH 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
This policy defines the procedures to be adopted for technical vulnerability and patch management at Veranda Learning.

Scope
This policy applies to all information technology infrastructure components deployed and managed by Veranda Learning.

Background
Poor patching can allow viruses and spyware to infect the network and allow security weaknesses to be exploited. Without regular vulnerability scanning and patching, the information technology infrastructure could fall foul of problems that are fixed by regularly updating the software, firmware, and drivers. Therefore, it is necessary that organization adopt a standard approach to implementing patch management.

Policy

Discover

- The first step is to identify and categorize assets: taking a complete inventory of all workstations and servers on a network. The inventory report should involve the list of assets with the OS versions and installed applications. Once assets are identified, they need to be categorized based on exposure and risk. Risk Analysis should be an integral part of the Patch Management process.
- Veranda Learning is enrolled in all Security bulletin's distribution list of all Application and OS vendors in the inventory list to get the updates/patches release notifications in real-time.

Analyze

- In the analysis phase, current patch levels are assessed by a vulnerability or patch management system designed to scan the systems they discover for installed and missing patches. The operating system needs to be determined for a given device and which applications are installed on the machine. Based on that information, consult a master list of available patches for a given OS and application and determine which of these patches are installed and which are not.
- Patch Level Minimum Baseline a critical concept is the minimum patch level required on the network.

Research

- The Information Security team must research before deploying the patches in the environment. Before deploying the patch following points should be considered.
- Nature of the vulnerability
- Application or OS component affected by it
- How easy is it to exploit the vulnerability?
- The severity of the vulnerability
- If the vulnerability is exploited, then what's the damage?
- Level of exposure to vulnerability?

Test

- The testing phase of deployment includes applying patches to a test environment before deploying them to a production system. No patch or service pack should ever be deployed without being tested in a test environment first.

Deploy

- Patch the standby system (old production) after establishing confidence with the production unit. A patch must be deployed on a standby system, and the system's functionality should be validated. Swap the patched standby system into production and keep the previous unpatched system as a standby for emergency patch regression.

Report

- Reporting confirms the successful deployment of patches and verifies that there is no negative impact. Reporting should be used to review the patch management process and look for areas of improvement.

Mapping with Industry Standards

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

Risk	Mapping to ISO 27001:2022
Loss of CIA (Confidentiality, Integrity, and Availability)	5.17 Authentication Information
Data Breach	5.17 Authentication Information
Unauthorized access	5.17 Authentication Information
Information Leakage	5.17 Authentication Information
Theft	5.17 Authentication Information

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.

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