CONFIGURATION 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 the Configuration Management Policy is to ensure that all IT Assets are documented with their known interdependencies and relationships so that change management, impact analysis, and compliance activities can be executed. The policy ensures that configuration items and components on Veranda Learning network are effectively documented, and subsequent changes are controlled and tracked.

Scope

Configuration Management policy applies to the following personnel

- All Employees of Veranda Learning
- All Contractors of Veranda Learning
- All vendors / third-party / visitors who temporarily access Veranda Learning's IT assets
- IT assets & Information System that are owned, operated, or leased by Veranda Learning

Background

Information systems are typically dynamic causing the system state to change frequently as a result of upgrades to hardware, software, firmware, or modifications to the surrounding environment in which a system resides. Organizations must document and assess the potential impact that proposed system changes may have on the operational processes and security posture of the system. Information Technology (IT) industry best practices recognize this as an essential aspect of effective system management.

Policy

Baseline Configuration

- Develop, document, and maintain a current baseline configuration of each platform (operating systems, databases, middleware, enterprise applications) within Veranda Learning's environment.
- Review and update the baselines annually and as needed due to system upgrades, patches, or other significant changes.
- Retain at least 1 previous configuration to support rollback.
- Establish a minimum baseline configuration for information systems or components with elevated security controls.

Configuration Change Control

- Determine the types of changes to an information system that is configuration controlled.
- Review proposed configuration changes and approved or disapproved with explicit consideration for security impact analysis and document change decisions.
- Test, validate, and document planned changes before implementation of approved changes.
- Retain records of changes for the system's life and retain audit and review activities associated with changes.

Configuration Settings

- Establish, document, and implement configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements.
- Periodically, review the use of functions, ports, protocols, and services. Identify and disable or eliminate those deemed unnecessary, unused, or detrimental to the system or business.
- Employ an allow-all, deny-by-exception policy to prohibit unauthorized software execution.
- Identify and document software programs prohibited or restricted from execution on the information system. Periodically review and update the list.

Information System Component Inventory

- Develop and document an inventory of information system components that:
  - Accurately reflects the current systems
  - Includes all components within the authorization boundary of the system
  - Provides information necessary to achieve effective infrastructure component accountability
  - It is at the level of granularity deemed essential for tracking and reporting.
- Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware when unauthorized components are detected, such as disabling network access for such components, isolating the components, or notifying authorized points of contact.

Configuration Management Plan

- Addresses configuration management roles, responsibilities, processes, and procedures.
- Establishes a process for identifying configuration items throughout the system development life cycle (SDLC) and ensures they align with established processes and procedures
- Protects the Configuration Management Plan from unauthorized disclosure and modification.

Software Usage Restrictions

- Use software (and associated documentation) in accordance with contractual agreements and copyright laws; and track the use of software protected for quantity licenses.
- Strictly prohibit the use of peer-to-peer file-sharing technology.
- Establish restrictions on the use of open-source software (OSS).

Mapping with Industry Standards

This policy addresses the following risks related Secure Configuration and Information Security standards, frameworks:

Risk	ISO 27001:2022

Insecure and incorrect functioning of organization's hardware and software assets.	8.9 Configuration management 8.27 Secure system architecture and engineering principles
Loss of Availability or System mis-behave	8.8 Management of technical vulnerabilities.
Information Leakage	8.19 Installation of software on operational systems

Enforcement

Configuration Management policy is enforced by the Information Security team. All exceptions to the policy should be brought to the attention of the information security team along with the executive management of the company.

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.