APPLICATION 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 Application Security Policy is to define the security framework and requirements for the security of applications, notably web applications, within the Veranda Learning's production environment.

Scope

the Application Security Policy applies to following.

Software Applications

- All in-house applications built by Veranda Learning and running in LIVE / Production environment
- All third-party software applications which store sensitive customer or organizational data

Background

Software Application vulnerabilities, especially web applications are the largest source of threats and data breaches for any organization. In Veranda Learning it is important that applications are designed with security in mind, and that they are scanned and continuously monitored for malicious activity that could lead to larger security or a data breach incident.

The policy is intended to facilitate the discovery and mitigation of application vulnerabilities in order to limit the company's attack surface. This policy defines technical requirements and procedures to ensure that applications are properly hardened in accordance with the practices and procedures defined by Veranda Learning's information security team.

Policy

Secure application

- All applications must require a secure login process per access management policy and password policy.
- Web applications must adhere to OWASP Top 10 to address the common security issues.
- All applications which store sensitive data must perform a quarterly vulnerability scan.
- Application development must strictly adhere to the Application Development Lifecycle (aka, SDLC) policy.
- Changes to the application must be per the Change Management Policy document.
- The information security team must conduct a formal security risk assessment for all new applications.
- Conduct a security risk assessment following all significant changes
- A periodic security risk assessment must be performed for legacy or other applications to assess against the latest threats and vulnerabilities.
- All applications must adhere to Log Management Policy for storing and disposing of application logs.
- All applications must follow security best practices for managing configuration and documenting the secure configurations for the application.

Data Handling

- Data handled and managed by the application must be classified in accordance with the Data Classification Policy.
- If the application processes confidential information, a confidential record banner must be prominently displayed, which highlights the type of confidential data being accessed (e.g., personally identifiable information (PII), protected health information (PHI))
- Sensitive data, especially data specifically restricted by law or policy (e.g., social security numbers, passwords, and credit card data) should not be displayed in plaintext.

Secure Processes for Application Development Lifecycle

- All application development must be per the Software Development Lifecycle document
- All changes to the application must be per the Change Management policy

Third-Party Software

- Updates, patches, and configuration changes issued by the vendor shall be implemented as soon as possible.
- Security reports & policy assessments of 3rd party software must be performed annually.
- Application provided by 3rd party vendors must be procured in accordance with vendor management policy.
- No custom modifications may be applied to the application without confirmation that the vendor can continue to provide support.

Mapping with Industry Standards

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

Risk	Mapping to ISO 27002:2022
Non-Compliance with the standards and regulations	5.31 Legal, statutory, regulatory and contractual requirements 5.32 Intellectual property rights 5.36 Compliance with policies, rules and standards for information security
Non-Compliance fees	5.35 Independent review of information security 8.19 Installation of software on operational systems 5.36 Compliance with policies, rules and standards for information security
Reputational Damage	5.33 Protection of records 5.34 Privacy and protection of PII

Enforcement

Application security policy will be enforced by the information security team and all applications must follow it. Exceptions are allowed upon formal approval from the information security team.

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.