Veranda

CHANGE 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 Change Management Policy is to outline the appropriate procedures put in place at Veranda Learning for managing change without impacting SLAs or adding risk to the system.

Scope

Change Management policy applies to the following:

- All infrastructure hosted in house and in the cloud
- Information systems and applications that contain company data
- Customer data, regardless of location.
- Source code
- Configuration managed by Veranda Learning

Background

Change management refers to a formal process for making changes to company software. Change management aims to increase awareness and understanding of proposed changes across the company and ensure that all changes are made in a thoughtful way that minimizes negative impact to services and customers. Unplanned changes can introduce unknown risks to the information systems either directly as security vulnerabilities or indirectly due to inadequate planning communication and un-preparedness to handle the transition. The change management policy defines how change is managed to maximize the success of that change.

Policy

Veranda Learning's change management policy requires that all information systems changes, including changes to applications, databases, and servers, are formally requested. All changes are approved and adequately communicated to stakeholders with appropriate training and awareness.

Types of Changes

There are four types of changes based on approvals needed through the change management process.

Standard Change: A relatively low risk change with well-understood outcomes regularly made during the business. A Standard change follows pre-determined processes, is pre-approved by change management processes, and may be made at the discretion of an individual employee, provided it has been defined as a Standard Change per the change management assessment process. Examples of standard changes are day-to-day changes to infrastructure, application releases, and any other change not expected to impact the availability of the Company's application or system.

Backward Incompatible Change: Backward incompatibility is a system property that disallows interoperability with an older system or with an input designed for such a system. It has medium to high risk for critical services and involves less understood risks. Because of the ability to affect downstream or upstream services, any proposed Backwards, Incompatible Change must be reviewed and authorized by Company's management, including engineering and product managers or lead developers.

Significant Change: A Significant Change has a high risk for critical services, has less predictable outcomes and is a change that is not regularly made during the business. An example of a Significant Change would be moving hosting from AWS to another cloud services provider, such as Google Cloud Platform. Because of the ability to affect downstream or upstream services, any proposed Significant Change must be reviewed and authorized by Company's management.

Emergency Change: An Emergency Change must be executed with utmost urgencies, such as when responding to an Incident. Few people may be involved in the change management process review, and the change assessment may involve fewer steps. However, any Emergency Change must still be authorized by Company's management, even in cases where management cannot review the change in advance.

Change management process

Change requests are initiated through a ticketing system (such as JIRA). Each change request has the following information at the minimum.

- Change for (Application, Infrastructure, etc.)
- Change Title
- Change Description
- Change type (Standard, Emergency, etc.)
- Requestor Name
- Approval By
- Priority
- Impact
- Change Reason
- Risk Type
- Affected systems/Services
- Start date, End date
- Backout Plan

All changes are required to go through an approval process. The information systems are free to pick the approval process depending on the magnitude of change and the development process they follow (automated CI / CD pipeline).

In some cases, approval is required from Chief Product Officer, Chief Information Officer (CIO), and Chief Operating Officer (COO)

Enhanced monitoring of all changes is required for at least a week, followed by a retrospective meeting.

All significant changes must go through a mandatory security assessment of change.

Change communication plan

A list of stakeholders is maintained by the operations manager of each information system. The stakeholders are kept in the loop and are informed of the changes from the very initial stages of the change.

Change Awareness

Change awareness is a top priority for changes that require a significant shift in how different stakeholders consume products and offerings in the organization. Change awareness is performed using newsletters, internal and external training, webinars, etc.

Application/source code changes

Only authorized Company employees can deploy code to company production systems.

Before deployment, all code requires the following steps.

- Peer review using Git pull requests by at least one other engineer (two-person rule)
- Peer reviewer signs off on pull request.
- Unit tests and static analysis checks are run on code in a pull request and must pass for code to be merged.
- Pull requests require at least one Jira ticket associated with the change explaining why it was made.
- Once a pull request passes peer review, code is merged to the development branch and is deployed to an internal staging environment.
- The Project Manager can request deployment to Production via a ticket in Jira.
- The same 2-person process is followed by merging development code to master for Production deployment.
- "Must have" test cases are run against Production after release
- All tickets in Jira that were pushed to Production are marked as "Closed."
- Versions of all deployed services are maintained in Git
- Deployment history is stored in our deployment database.

Infrastructure changes

Like application changes, infrastructure changes can only be done by authorized employees. The process for implementing changes is as follows:

- A need for change is initiated because of
  - A planned update to support future growth or development requirements
  - A change in response to a monitoring alert or pattern that should be addressed
  - A platform level issue that requires an immediate infrastructure change to remedy
- A ticket is raised regarding the requested change or issue requiring remedy and assigned to the appropriate employee.
- The employee evaluates the ticket and either address or escalates it to the Chief Technology Officer for approval.
- If it is approved or does not require approval, the change is made
- The ticket is then marked as resolved

Mapping with Industry Standards

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

Risk	Mapping to ISO 27001:2022
System failure	8.32 Change Management 5.3 Segregation of duties C 6.3 Planning of changes C 8.1 Operational planning and control C 10.1 Continual improvement
Data Loss	8.32 Change Management 5.3 Segregation of duties C 6.3 Planning of changes

Risk	Mapping to ISO 27001:2022
	C 8.1 Operational planning and control C 10.1 Continual improvement

Enforcement

Change management policy is enforced by the Operations Manager, Engineering Manager or the Chief Information Officer (CIO).

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.