Veranda

BUSINESS CONTINUITY 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 this policy is to outline objectives, plans, and, procedures put in place by Veranda Learning to ensure that it minimizes disruption to the Company's key business activities caused by a major security incident or a natural disaster.

Scope

Business Continuity policy applies to following

- All Information Systems
- Operation teams and support personnel
- Senior management

Background

Veranda Learning continuously aims for the preservation of critical business operations and essential functions to deliver key products and services. This policy outlines how Veranda Learning ensures this continuity.

- This policy puts in place a structure and authority to ensure business resilience of operations and information systems.
- This policy puts in place a plan to manage business operations through the disaster period and the effort it will take to get back to normal operations
- This policy defines a disaster recovery plan containing a set of human, physical, technical, and procedural resources to return to a normal level of operation, within a defined time and cost, in case of an emergency or disaster.

Policy

Veranda Learning must establish, implement and maintain procedures for the continuity of operations and ensure the availability of information systems and resources during adverse conditions. As a result, the company must create a **contingency and recovery plan** which must

- Identify essential information systems and critical business functions that must operate normally or in a limited fashion despite a system disruption, compromise, or failure
- List associated contingency requirements for each one of the identified systems.
- Provide recovery objectives, restoration priorities, and metrics for each system.
- Define roles, responsibilities, and assigned individuals with contact information for each system.
- Create procedures for obtaining access to sensitive data during other-than-normal or emergency conditions.
- Create an inventory of recovery documents and operation procedures for each system. The steps should contain
  - Assets impacted
  - Custodian
  - Backup procedures
  - Restoration procedures
  - Testing / Validation steps
  - Recovery time and recovery point objectives for each asset
  - Escalation structure during the disaster period
  - Communication steps
- The recovery steps must be in the following order of priority.

- Critical operations during disaster
- Minimal operations after recovery
- Full recovery and normal operations

Reviewing and maintaining the plan

- The contingency plan must be reviewed at least annually.
- The contingency plan must be reviewed and approved by company management.
- After each review, the necessary changes must be applied to the plan
- Key personnel must be notified of the changes
- Distributing copies of the contingency plan to key contingency personnel.
- Asset custodians and data owners are required to be trained in their contingency roles and responsibilities for systems.

Testing the plan

- A contingency plan must be tested once per year
- The contingency plan test results are document
- Asset owners and custodians of the information systems are responsible for the testing of the plan.
- Asset owners and custodians of the information systems are responsible for making any corrective actions in the plan as a result of the test exercises.

Mapping with Industry Standards

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

Risk	Mapping to ISO 27001:2022
Data Breach	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
System failure	5.29 Information security during disruption 5.30 ICT readiness for business continuity 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
Natural Disaster (earthquake)	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
Man-made hazards (war, terrorism)	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control
Physical Loss or damage	5.29 Information security during disruption 8.14 Redundancy of information processing facilities C 8.1 Operational planning and control

Enforcement

Business Continuity policy is enforced by the Senior Management team along with information security team and in some cases the business operation teams such as IT support teams.

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.