Backup And Restoration 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 Backup Policy is to maintain data integrity and availability of the Veranda Learning's information system, to prevent loss of data, and to facilitate the restoration of the information system and business processes.

Scope

The backup policy applies to the following personnel

- All databases of **Veranda Learning**
- All data created by the information systems of **Veranda Learning**
- All vendors / third-party creating / managing data for **Veranda Learning**

Background

The purpose of a data backup is to create a copy of data that can be recovered in the event of a failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data. Backup copies allow data to be restored from an earlier point in time to help the business recover from an unplanned event.

Policy

Performing a backup

- Loss of data must be prevented by performing regular backups to meet the RPO (Recovery Point Objective) and RTO (Recovery Time Objective). Refer to the Data Retention Policy for RTO and RPO.
- For **Veranda Learning** data for critical information systems must be backed up at least 2 times a day.
- The appropriate team/system owners must perform backups for the data and information systems they are responsible for protecting.
- Backup schedules must be maintained for all information systems centrally.
- The extent (e.g., full or differential backup) and frequency of backups should reflect the organization's business requirements, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization.

Backup storage

- All backup data must be stored encrypted with the AES-256 symmetric encryption algorithm.
- Backup copies must be stored in an environmentally protected and access-controlled secure location offsite from the site of the originating asset.
- For highly critical data, more than one copy in a geographically distributed location must be considered.
- A record of the physical and logical movements of backup media must be maintained.

Restoring a backup

Backup copies must be tested every quarter for recovery capability.

Mapping with Industry Standards

This policy addresses the following risks related to Backup & Restoration and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Loss of CIA (Confidentiality, Integrity and Availability)	8.13 Information backup C 10.1 Continual improvement
Malware	8.13 Information backup C 10.1 Continual improvement
Data Loss	8.13 Information backup C 10.1 Continual improvement
Theft and Physical Damage	8.13 Information backup C 10.1 Continual improvement

Enforcement

The backup policy is enforced by the Infosec team and system owners of respective information systems whose data is backed up. All exceptions to the policy should be brought to the attention of the Infosec 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.