DATA RETENTION 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

This data retention policy defines the objectives and requirements for data retention within the organization. This Policy covers all information and data/information in the Company's possession, custody, or control, including data/information in electronic, paper, or other forms, and including both original documents and reproductions. This Policy is not restricted to the information contained in paper documents but includes data/information contained in an electronically readable format. For the purposes of convenience, in this Policy, any medium which holds information and/or data is called a Record.

Scope

The data retention policy applies to following

Personnel

- All Employees of Veranda Learning
- All Contractors of Veranda Learning
- All vendors / third-party / visitors who temporarily access Veranda Learning's Information Systems of Veranda Learning

- All Information Systems
- All Information

Background

The Company is bound by various obligations with regard to the data/information that we retain or that is in our custody or under our control. These obligations include how long we may retain data/information and when and how we can destroy it. The obligations may arise from local laws or regulations or from contracts and promises that we have made to our employees, customers, regulators, goods and service providers, and partners. As a result, Records may need to be archived and stored for longer than the data/information that may be needed for day-to-day operations and business processes. Broadly, when the Record Retention Period has ended and we no longer need the Record, we must ensure that the Record is destroyed in an appropriate proper manner.

Further, the Company may be involved in unpredicted events such as litigation or disaster recoveries that require us to have access to the original Records in order to protect the Company's interests or those of our employees, customers, goods, and service providers, and our partners. There may be legal, regulatory, contractual, or policy requirements that may extend the duration for which information must be retained beyond its useful life. Before disposing of any Records, please review this Policy. In addition, do not destroy Records if you have received a "hold notice" from the Company's Legal department concerning actual or threatened litigation or investigation or if you have reason to believe that documents relate to a dispute that may result in litigation or investigation. If you have any questions, please contact the Legal department before you destroy any Records.

Policy

***** If this Policy applies to you, please consult your legal department for retention records and retention schedules***

What to retain

Application & Services data

- Customer, application & transactional data generated by products and services
- Audit log data generated by products and services
- Data created in 3rd party applications and services

Other data to retain

- Corporate / Company data (Articles of incorporation etc)
- Electronic Mail
- Physical correspondence
- Customer contracts etc
- Financial records / receipts / invoices etc
- Website / CRM data
- Call recordings

Retention schedule

A Record shall be considered active so long as Record is in use by a business unit or division("Function") or referenced in an external document.

Customer data shall be retained for the duration set in the contracts and SLAs. For example, application data

- Will be maintained during the full duration of the relationship
- Will be maintained till 45 days after the duration of the relationship
- Will be maintained during the duration of the trial
- Will be deleted between 7- 14 days after the trial or the relationship ends

Retention in 3rd party application

All data created in different 3rd party systems must be retained for the duration of the relationship with those 3rd party applications.

After termination of the relationship,

- If a new system is being established, then migrate the data from the current third-party system to the new system.
- If no system replaces the existing system, then the export of the data must be taken and maintained in an accessible format as per the data retention guidelines for the type of data

Destruction and disposition

- Each employee shall be responsible for returning Records in their possession, custody, or control to the Company upon separation or retirement.
- The final disposition of such Records shall be determined by their immediate supervisor in accordance with this Policy.
- Each head of Function shall be responsible for enforcing the retention, archiving, and destruction of records in their respective Function and communicating these periods to the relevant employees.
- Each employee shall be responsible for following and implementing the policies related to the Records they create, maintain, or access.

Mapping with Industry Standards

This policy addresses the following risks related to data retention, data disposal and Information Security standards, frameworks

Risk	ISO 27001:2022
Loss of CIA (confidentiality, Integrity and Availability)	5.12 Classification of information 5.10 Acceptable use of information and other associated assets 7.10 Storage media 8.13 Information backup 8.15 Logging 5.14 Information transfer 5.33 Protection of records 8.10 Information deletion
Non- adherence to laws and regulations	5.14 Information transfer 5.33 Protection of records
Unauthorized access	5.12 Classification of information 5.10 Acceptable use of information and other associated assets 8.15 Logging 5.33 Protection of records 8.10 Information deletion
Information Leakage	5.12 Classification of information 5.10 Acceptable use of information and other associated assets 7.10 Storage media 8.13 Information backup 8.15 Logging 5.14 Information transfer 5.33 Protection of records
Theft	5.10 Acceptable use of information and other associated assets 8.13 Information backup 8.15 Logging 5.14 Information transfer 5.33 Protection of records
Fraud	5.12 Classification of information 5.10 Acceptable use of information and other associated assets 7.10 Storage media 8.13 Information backup 8.15 Logging 5.14 Information transfer 5.33 Protection of records

Enforcement

Each head of Function shall be responsible for enforcing the retention, archiving, and destruction of records in their respective Function, and for communicating these periods to the relevant

employees. Each employee shall have the responsibility of following and implementing the policies as it relates to the Records they create, maintain or access.

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.