CloudServe Data Retention Policy

Effective Date: 9/09/2024
Last Updated: 9/09/2024
Version: 1.0

---

1. Purpose

The purpose of this Data Retention Policy is to define CloudServe's approach to retaining, archiving, and securely disposing of data. This policy ensures compliance with legal, regulatory, and business requirements, particularly with respect to SOC 2 Trust Service Criteria for Security, Availability, and Confidentiality.

---

2. Scope

This policy applies to all CloudServe employees, contractors, and third-party vendors who handle company data. It covers all forms of data storage, including physical servers, cloud platforms, databases, and removable media. The policy also addresses customer, employee, and business-related data.

---

3. Data Classification

Data at CloudServe is classified into three categories to facilitate appropriate retention and disposal procedures:

- **Confidential Data**: Highly sensitive information, including customer personally identifiable information (PII), financial data, system credentials, and intellectual property.
- **Internal Data**: Information related to the company’s operations, including internal communications, business strategies, and employee data.
- **Public Data**: Data intended for public dissemination, such as marketing material or press releases.

---

4. Retention Periods

CloudServe data retention periods are established based on legal and business requirements. Data will be retained for a specified period before being securely archived or deleted. Below are the guidelines for various data types:

Data Type	Retention Period	Description
Customer PII	7 Years	Retained for legal compliance (e.g., GDPR, CCPA).
Financial Records	7 Years	Required for tax, audit, and regulatory purposes.
Contracts and Agreements	5 Years	After the contract has been terminated.
Employee Records	5 Years	Following the end of employment.
Business Communications	3 Years	Retained for internal reference and audits.
Backups	1 Year	Monthly backups retained for business continuity.

Note: These retention periods may be adjusted based on regulatory updates.

---

5. Data Retention Procedures

- **Active Data**: During its active lifecycle, data must be maintained and managed by its designated owner and backed up regularly.
- **Archiving**: After its active use, data will be archived and retained for the specified retention period. Archived data should be stored securely and accessible only to authorized personnel.
- **Disposal**: Once the retention period has expired, data must be securely deleted or destroyed. This includes permanent deletion from electronic storage systems and physical destruction of any paper records.

---

6. Responsibilities

- **Data Owners**: Data owners are responsible for managing the retention, archiving, and disposal of data in their respective areas.
- **IT Department**: The IT team is responsible for securely managing backups, archiving systems, and ensuring proper deletion protocols are followed for electronic data.
- **Compliance Team**: The compliance team ensures that this policy adheres to relevant legal, regulatory, and contractual obligations, and conducts regular audits to verify compliance.

---

7. Security and Access Controls

- All data retention systems must be protected using access controls, encryption, and other security measures to ensure that data integrity is maintained.
- Only authorized personnel should have access to archived or retained data, and any retrieval of this data should be logged for audit purposes.

---

8. Policy Compliance

Compliance with this policy will be regularly monitored and audited. Failure to comply may result in disciplinary actions, including termination of employment or vendor contracts.

---

9. Review and Updates

This policy will be reviewed annually, or when required by significant changes in legal or regulatory requirements, to ensure that it remains current and effective.

---

10. Contact Information

For any questions or concerns regarding this Data Retention Policy, please contact the Compliance Team at CloudserverIT@CS.com.