CloudServe Data Encryption Policy

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

---

1. Purpose

The purpose of this Data Encryption Policy is to protect sensitive and confidential data stored, transmitted, and processed by CloudServe. Encryption safeguards the security and confidentiality of data, ensuring that it is only accessible to authorized parties. This policy is aligned with SOC 2 Trust Service Criteria to ensure the protection of data integrity and availability.

---

2. Scope

This policy applies to all CloudServe employees, contractors, and third-party vendors who handle CloudServe's data, including data stored in the cloud, data in transit, and data on physical devices. It covers all systems, applications, networks, and databases that store or process sensitive information, including Personally Identifiable Information (PII), financial data, and customer information.

---

3. Data Classification

CloudServe classifies data based on its sensitivity and impact if disclosed. The following categories are used:

- **Confidential Data**: Highly sensitive data, including customer data, financial records, employee PII, intellectual property, and system credentials. Encryption is mandatory.
- **Internal Data**: Business operations data that is not publicly available but may not require the same level of encryption as confidential data.
- **Public Data**: Information that is intended to be shared publicly, which does not require encryption.

---

4. Encryption Requirements

CloudServe enforces encryption for all confidential data as follows:

4.1 Data at Rest

- **Encryption Standards**: All data at rest must be encrypted using industry-standard encryption algorithms, such as AES-256.
- **Scope of Encryption**: Encryption must be applied to:
  - Databases (e.g., customer data stored in cloud databases)
  - File systems containing sensitive data
  - Backups stored either locally or in the cloud
- **Encryption Key Management**:
  - Encryption keys must be stored and managed securely using a Key Management Service (KMS).
  - Access to encryption keys must be limited to authorized personnel only.

4.2 Data in Transit

- **Encryption of Network Traffic**: All data transmitted over public and private networks must be encrypted using secure protocols such as TLS 1.2 or higher.
- **VPN Encryption**: Remote access to internal systems must be done via a secure, encrypted VPN connection.
- **API and Application Traffic**: All application programming interfaces (APIs) that transmit sensitive data must use HTTPS with strong encryption to ensure data confidentiality.
- **Email Encryption**: Sensitive information sent via email must be encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME) or similar technologies.

4.3 Encryption for Mobile Devices and Endpoints

- **Device Encryption**: All company-issued laptops, smartphones, and tablets used to access CloudServe's systems must have full-disk encryption enabled.
- **External Storage Devices**: USB drives, external hard drives, or any other removable media used to store confidential data must also be encrypted.
- **Encryption for BYOD**: Employees using personal devices to access sensitive data must comply with CloudServe's BYOD (Bring Your Own Device) encryption standards.

---

5. Encryption Key Management

To ensure the secure use of encryption keys, CloudServe implements the following procedures:

- **Key Rotation**: Encryption keys must be rotated regularly and upon any suspicion of compromise.
- **Key Storage**: Encryption keys must be stored in a secure Key Management System (KMS) such as AWS KMS or Azure Key Vault.
- **Key Access Control**: Access to encryption keys is restricted to authorized personnel only, and permissions must be reviewed quarterly.
- **Key Backup and Recovery**: Encryption keys must be backed up in secure locations to ensure recovery in case of loss or corruption.

---

6. Encryption of Backups

CloudServe ensures that backups of confidential data are encrypted both during storage and transmission:

- **Backup Encryption**: All backups must be encrypted using AES-256 or higher.
- **Cloud Backup Encryption**: Cloud-based backups must use secure storage services that enforce encryption of both data at rest and in transit.
- **Backup Access Control**: Access to backup data must be restricted to authorized personnel, with logs maintained for all access.

---

7. Policy Enforcement

CloudServe enforces this encryption policy through the following methods:

- **Monitoring and Auditing**: Regular audits of encryption practices will be conducted to ensure compliance. This includes monitoring encryption configurations, key management systems, and data transfer protocols.
- **Training**: All employees will receive annual security training on the importance of data encryption and how to comply with this policy.
- **Non-Compliance**: Employees found to violate this policy may face disciplinary actions, including termination. Third-party vendors found in violation may have their contracts terminated.

---

8. Incident Response and Breach Reporting

If any encrypted data is compromised or a key is lost, the following steps must be taken:

- **Immediate Action**: Notify the IT Security Team within 24 hours of discovery.

- **Incident Response**: The Incident Response Team (IRT) will follow the established Incident Response Plan to contain and mitigate the breach.
- **Customer Notification**: In the case of a data breach involving customer information, customers must be notified within 72 hours in compliance with regulatory requirements (e.g., GDPR, CCPA).

---

9. Policy Review and Updates

This policy will be reviewed and updated annually, or when significant changes to encryption technologies or security threats are identified.

---

10. Contact Information

For questions or further information regarding this Data Encryption Policy, contact the IT Security Team at CloudserverIT@CS.com.