Cloud Storage Encryption and Security Measures Document

1. Introduction

This document outlines the encryption practices and security measures implemented for protecting data stored within our cloud storage environment.

2. Scope

The measures described herein apply to all data stored, transmitted, or processed within the cloud storage system under the responsibility of [Organization Name].

3. Roles and Responsibilities

Role	Responsibility
Cloud Administrator	Managing access controls, encryption settings, and regular audits.
Data Owner	Classifying data and requesting encryption policies.
Security Officer	Monitoring security events and incident response.

4. Encryption Measures

4.1 Data at Rest

- All stored data is encrypted using AES-256 standard by default.
- Encryption keys are managed and rotated regularly.

4.2 Data in Transit

- Data transferred between client devices and cloud is protected using TLS 1.2 or higher.
- Regular audits are conducted to verify secure transmission configurations.

5. Access Control

- Role-Based Access Control (RBAC) is enforced.
- Multi-factor authentication is required for all administrative accounts.
- Access logs are audited on a regular basis.

6. Key Management

- Encryption keys are stored in a managed Key Management Service (KMS).
- Keys are rotated every 90 days, or immediately upon suspicion of compromise.
- Access to the KMS is restricted to authorized personnel only.

7. Compliance and Monitoring

- Regular security audits are performed to ensure compliance with standards.
- Security events are monitored 24/7 with automated alerting.
- Incident response procedures are established and periodically tested.

8. Review and Updates

This document is reviewed biannually or upon significant changes to cloud storage technologies or security requirements.

9. Document Control

Version	Date	Author	Change Description
1.0	YYYY-MM-DD	[Author]	Initial document release.