Cloud Storage Encryption Strategy Document

1. Purpose

This document outlines the encryption strategy for securing data stored in cloud storage environments. It aims to define procedures, standards, and responsibilities for protecting data confidentiality, integrity, and availability.

2. Scope

This strategy applies to all data classified as sensitive or confidential that is stored, processed, or transmitted through organization-managed cloud storage services.

3. Encryption Objectives

- Ensure all sensitive data at-rest and in-transit is encrypted using industry standards.
- Maintain data confidentiality, integrity, and regulatory compliance.
- Limit access to encryption keys and enforce robust key management.

4. Encryption Standards

Data Type	Encryption Method	Standard
At-Rest	Server-side encryption	AES 256-bit
In-Transit	Transport Layer Security	TLS 1.2 or higher

5. Key Management

- Encryption keys must be stored in a managed Key Management Service (KMS).
- Implement role-based access control for key usage and management.
- Rotate keys on a regular schedule (annually or upon staff turnover).
- Monitor and audit key usage.

6. Roles and Responsibilities

Role	Responsibility
IT Security Team	Manage encryption protocols, monitor compliance, and maintain documentation.
Cloud Administrators	Implement and configure encryption settings and key management.
All Users	Ensure sensitive data is stored and accessed per encryption policy.

7. Compliance

Ensure all encryption and key management practices adhere to applicable legal, regulatory, and contractual requirements (e.g., GDPR, HIPAA, PCI-DSS).

8. Review and Updates

This document will be reviewed annually or upon significant changes to cloud technology, organizational requirements, or applicable regulations.