Cloud Storage always encrypts your data on the server side, before it is written to disk, at no additional charge. This page discusses the standard encryption that Cloud Storage performs. For other encryption options, see Data Encryption Options (/storage/docs/encryption).

Cloud Storage manages server-side encryption keys on your behalf using the same hardened key management systems that we use for our own encrypted data, including strict key access controls and auditing. Cloud Storage encrypts user data at rest using AES-256 (https://en.wikipedia.org/wiki/Advanced_Encryption_Standard). There is no setup or configuration required, no need to modify the way you access the service, and no visible performance impact. Data is automatically and transparently decrypted when read by an authorized user.

To protect your data as it travels over the Internet during read and write operations, use Transport Layer Security, commonly known as TLS or HTTPS.