

Encryption Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy supports the SOC 2 common criteria CC6.1 and CC6.7 by defining encryption and key management requirements for data at rest and in transit.

This policy applies to all production systems, backups, and data transmissions that store, process, or transmit company or customer data.

2. Encryption standards

- Data at rest: Databases, object storage, backups and laptops that hold Company or customer data are encrypted with [Encryption standard at rest].
- Data in transit: Data crossing a public network is encrypted with [Encryption standard in transit]. Transport Layer Security (TLS) 1.2 is the minimum, and older protocols are disabled.
- Algorithms: Only current, widely reviewed algorithms from the cloud provider and standard libraries are used. Custom cryptography is not permitted.

3. Key management

- Where keys live: Encryption keys and secrets are held in [Secrets manager] and never in source code, chat or tickets.
- Rotation: Keys are rotated [Key rotation frequency], and at once when compromise is suspected or someone who could read them leaves.
- Access: Only named administrators can manage keys, and every use of a key is logged.
- Retirement: A retired key is disabled before it is deleted, so data it protects can still be read during the change.

4. Certificates

Public certificates come from a trusted certificate authority, renew automatically where the provider supports it, and are tracked with their expiry dates so none lapses unnoticed.

5. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.
Key administrators	[Engineering owner role]	Configure encryption and key rotation, and approve access to keys.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

6. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Encryption configuration	Evidence of at-rest and in-transit encryption settings.	[Cloud provider]
Key management settings	Key service or secrets manager settings, including rotation.	[Secrets manager]
Certificate inventory	Each certificate, where it is used, and when it expires.	[Documentation system]

7. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

8. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

9. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[Cloud provider]	Where production runs, for example AWS, Google Cloud or Azure.

Field	What to enter
[Secrets manager]	Where keys and secrets are stored, for example a cloud key management service.
[Encryption standard at rest]	For example AES-256, the Advanced Encryption Standard with 256-bit keys, through the cloud provider key service.
[Encryption standard in transit]	For example TLS 1.2 or higher.
[Key rotation frequency]	How often keys are replaced, for example every 12 months.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[Engineering owner role]	The role that owns production systems, for example engineering lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/encryption-policy (CC BY 4.0).