Encryption & Cryptographic Control Policy

This policy establishes requirements for managing encryption, keys, and cryptographic protections to safeguard the confidentiality and integrity of customer and organizational data at rest and in transit.

Encryption & Cryptographic Control Policy

Executive Summary

Casper Studios must enforce encryption and cryptographic controls across all production and non-production environments to maintain confidentiality and integrity of organizational and customer data in alignment with SOC 2 CC6 and CC7 criteria. All encryption keys shall be managed within AWS KMS with automated rotation, strict access controls, and quarterly reviews. Data in transit and at rest must utilize FIPS 140-2 validated algorithms and industry-standard TLS 1.2+ encryption.

Table of Contents

Document Content Page

A. Applicability And Scope

This policy applies to all Casper Studios employees, contractors, and third parties who design, implement, or manage cryptographic solutions, keys, databases, and network services—whether in AWS production or non-production environments (e.g., us-east-1) or on company-provided laptops in home offices.

Full disk encryption shall be enabled on all company-provided laptops using FIPS 140-2 validated mechanisms (e.g., BitLocker, FileVault) and configured to integrate with Google Workspace authentication for key escrow.

The Information Security Officer and Data Owner must ensure compliance through quarterly audits and annual policy reviews.

B. Controls

1. Encryption Key Management

1. All cryptographic keys must be generated and stored in AWS Key Management Service (KMS) using FIPS 140-2 validated modules (SOC 2 CC6.1).
2. AWS KMS keys shall be automatically rotated every 90 days, with rotation events recorded in CloudTrail logs and reviewed monthly by the Information Security Officer (SOC 2 CC6.2).
3. Access to KMS keys must require IAM roles with least privilege and dual approval by the Information Security Officer and Data Owner (SOC 2 CC7.1).
4. Quarterly key inventory and usage reports must be generated and retained for at least one year (SOC 2 CC6.3).

2. Secure Data Transfer

1. All in-transit data shall be encrypted using TLS 1.2 or higher with certificates managed by AWS Certificate Manager and renewed at least 30 days before expiration (SOC 2 CC6.5).
2. Production databases in AWS RDS must enforce encryption at rest with AES-256 or AWS KMS-managed keys (SOC 2 CC6.4).
3. Non-production environments must implement identical encryption configurations as production, unless an exception is approved per Section C (SOC 2 CC6.6).

C. Exceptions Process

Any deviation from this policy must be requested through the Linear ticketing system with business justification, compensating controls, and a defined expiration date. The Information Security Officer and Data Owner shall jointly review and approve or reject each exception, and revalidate approved exceptions quarterly. All exception tickets must be documented and archived for auditor review (SOC 2 CC7.2).

D. Violations And Disciplinary Action

Automated AWS Config checks and monthly security audits shall detect non-compliance; any violations must be reported immediately to the Information Security Officer. Confirmed breaches of cryptographic controls may result in key revocation, access removal, and HR disciplinary action up to termination, in accordance with company policy (SOC 2 CC7.3).

Auditor Evidence Artefacts

- AWS KMS key policy snapshots and CloudTrail rotation logs
- Monthly IAM access review reports
- TLS certificate inventory and renewal screenshots
- Linear tickets for exception approvals
- Quarterly key management and audit meeting minutes