Asset Management Policy

This policy ensures that all organizational assets are identified, assigned ownership, and protected according to their value and risk, reducing the likelihood of loss, misuse, or inadequate accountability.

Document Content Page

Executive Summary

This Asset Management Policy defines the identification, classification, ownership, and protection of Casper Studios assets to meet SOC 2 security criteria. It mandates quarterly inventory reviews, assigns clear roles and responsibilities, and enforces mandatory controls across AWS, company laptops, and cloud services. Compliance will be audited annually, with evidence artifacts maintained for verification.

Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third parties who handle organizational assets, including AWS resources, company-provided laptops used in home offices, Google Workspace accounts, and related cloud services. It covers physical hardware, virtual machines, data repositories, and SaaS applications. All assets must adhere to SOC 2 Trust Service Criteria for Security (CC1, CC6, CC7).

Asset Management Controls

Asset Inventory

1. CS-AM-1: The IT Administrator must maintain an up-to-date inventory of all organizational assets (physical and virtual) in AWS (e.g., EC2, S3) and laptops in a centralized CMDB. This inventory shall be reviewed quarterly.
2. CS-AM-2: The Asset Owner must classify assets according to SOC 2 sensitivity levels (e.g., Confidential, Internal) upon acquisition and record the classification in the inventory. Classifications

shall be validated quarterly.

Asset Ownership

1. CS-AM-3: The Information Security Officer must assign and document ownership responsibilities for each asset, specifying owner role, responsibilities, and contact information. Ownership assignments shall be validated quarterly.

Asset Protection

1. CS-AM-4: The IT Administrator must implement logical and physical controls (e.g., disk encryption on laptops, AWS IAM policies, VPC configurations) aligned with SOC 2 CC6 and CC7 to protect assets based on classification. Controls shall be tested annually.
2. CS-AM-5: The IT Administrator shall ensure automated monitoring for asset integrity and unauthorized changes, with alerts configured in AWS CloudWatch and Google Workspace logs. Alerts and logs shall be reviewed monthly.

Exceptions Process

Employees must submit asset-related exception requests via Linear ticketing, including business justification, compensating controls, and requested duration. The Information Security Officer and Asset Owner shall approve, document, and time-limit each exception in the ticket, and review at or before expiry on a quarterly basis. Exceptions must be revoked immediately if expiration occurs without formal renewal.

Violations and Disciplinary Action

Automated monitoring and quarterly audits shall detect non-compliance with this policy. Suspected violations must be reported to the Information Security Officer and HR. Confirmed violations shall result in disciplinary actions—ranging from written warnings to termination—and may include revocation of access and legal action.

Auditor Evidence Artefacts

- Asset inventory export from CMDB with timestamps.
- Quarterly review meeting minutes signed by the Information Security Officer.
- Linear tickets for asset exception requests with approvals.
- AWS CloudWatch and Google Workspace audit logs.
- Screenshots of IAM policy configurations and encryption settings.