Logging Policy

This policy mandates continuous monitoring and logging to detect, evaluate, and respond to security events, thereby protecting the integrity, availability, and reliability of organizational systems and controls.

Executive Summary

Casper Studios must maintain continuous logging and monitoring aligned with SOC 2 Trust Services Criteria (CC4.1, CC6.5, CC7.2) using AWS CloudWatch, Splunk, and Google Workspace audit logs. The policy defines mandatory controls for log generation, aggregation, review, and incident detection, with monthly reviews and quarterly audits. It outlines the exception process and disciplinary actions to ensure compliance and readiness for external audits.

Table of Contents

A. Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third parties using company-provided laptops, AWS (us-east-1), Google Workspace, Slack, Linear, Figma, and Zoom. It covers all systems generating, transmitting, storing, or analyzing security-related logs to protect the integrity, availability, and confidentiality of employee data. System Owners, the InfoSec Officer, and the CTO shall enforce these requirements across hybrid and remote environments.

B. Controls

Security Monitoring & Detection

1. All AWS and Google Workspace audit logs must be aggregated into AWS CloudWatch Logs and Splunk within one hour of generation (CC6.5).
2. The InfoSec Officer shall review aggregated security event dashboards daily using AWS Security Hub and Slack alerts for anomalous activities (CC7.3).

3. The CTO and Internal Audit Team must analyze log trends quarterly to assess control effectiveness and refine security monitoring (CC4.3).
4. AWS CloudWatch Alarms and AWS Config rules shall detect unauthorized configuration changes and notify System Owners and the InfoSec Officer within two hours (CC6.5).

Security Logging

1. Company-provided laptops and AWS EC2 instances must forward OS and application logs (authentication, system, network) to AWS CloudWatch Logs with a retention period of 90 days (CC4.1).
2. Google Workspace Admin audit logs for user activity must be exported daily to AWS S3 (us-east-1) and retained for one year (CC4.1).
3. Splunk queries shall detect anomalous login patterns (e.g., more than five failed logins per minute) and alert the on-call Security Engineer via PagerDuty within 15 minutes (CC6.5).
4. All logs shall be encrypted at rest using AES-256 and in transit using TLS 1.2 or higher (CC7.2).

C. Exceptions Process

Requests to deviate from logging requirements must be submitted via a Linear ticket tagged “SOC2-Logging”. The ticket shall include business justification, compensating controls, and an expiration date. The InfoSec Officer and System Owner shall review and approve exceptions within five business days, with monthly reviews until closure.

D. Violations and Disciplinary Action

Automated and manual log reviews shall detect non-compliance. Suspected violations must be reported to the InfoSec Officer and HR within one business day. Confirmed violations result in disciplinary action—verbal warning, written warning, suspension, or termination—and may include access revocation and legal referral as appropriate.

E. Auditor Evidence Artefacts

- AWS CloudWatch Logs retention reports (screenshots)
- Splunk alert configuration and reports
- Linear tickets for exception requests and approvals
- Quarterly log review meeting minutes
- AWS S3 bucket audit log export records
- PagerDuty alert logs
- Internal Audit quarterly report on logging controls