Security Awareness & Training Policy

This policy promotes a security-conscious culture by setting behavioral expectations and ensuring all personnel possess the knowledge and qualifications necessary to safeguard organizational assets.

Table of Contents

Executive Summary

This Security Awareness & Training Policy establishes mandatory training, acceptable use, and personnel security controls to safeguard Casper Studios' AWS-hosted systems and data in strict alignment with SOC 2 requirements. It applies to all employees, contractors, and third parties accessing cloud and home-office environments. The policy is reviewed quarterly and audited annually to ensure continued compliance and mitigate risks to employee data and organizational assets.

A. Applicability & Scope

This policy applies to all Casper Studios employees, contractors, and third-party vendors accessing or managing information systems, including AWS cloud resources, Google Workspace accounts, company-provided laptops, and home-office networks.

B. Controls

1. Acceptable Use

1. (SOC2-TC-1) Personnel must use only approved devices and authenticated Google Workspace or company credentials to access corporate resources; use of personal devices for sensitive operations is prohibited without documented exception.
2. (SOC2-TC-2) All access to AWS consoles and related systems must occur over secure VPN or approved secure home-office networks, with multi-factor authentication enabled.
3. (SOC2-TC-3) Personnel shall comply with company guidelines for acceptable technology use on Slack, Linear, Figma, and Zoom; violations must be reported to the Information Security Officer.

4. (SOC2-CT-4) All staff must acknowledge this policy and complete annual SOC 2 security awareness training by electronic signature; reminders are sent quarterly.

2. Personnel Security

1. (SOC2-PS-1) Background checks must be completed for all new hires before granting access to corporate or AWS resources.
2. (SOC2-PS-2) Information security roles and responsibilities shall be defined in job descriptions; only qualified personnel may fulfill security-related duties.
3. (SOC2-PS-3) Security and privacy training tailored to job functions must be delivered during onboarding and refreshed annually.
4. (SOC2-PS-4) Training completion records shall be retained in Linear training tickets and reviewed quarterly.

C. Exceptions Process

Personnel must submit exception requests via Linear tickets with business justification, compensating controls, and duration. The Information Security Officer and HR Manager shall jointly approve and document each exception; all exceptions are reviewed at or before expiration quarterly.

D. Violations & Disciplinary Action

Compliance is monitored through quarterly log reviews in AWS CloudTrail and Slack audit logs. Violations must be reported to the Information Security Officer and HR; confirmed breaches shall result in disciplinary action up to termination, based on severity, and may require retraining.

E. Auditor Evidence Artefacts

- Annual training completion logs from Google Workspace and Linear.
- AWS CloudTrail audit logs and VPN connection records.
- Signed policy acknowledgments and exception approval tickets.
- Records of disciplinary actions and retraining schedules.