Information Security Program

This policy defines and governs the organization’s information security program to protect the confidentiality, integrity, and availability of information assets and to reduce risks arising from inadequate governance, oversight, or staff awareness.

Information Security Program

Executive Summary

Casper Studios shall implement a SOC 2-aligned Information Security Program that enforces confidentiality, integrity, and availability of employee data, cloud-hosted applications on AWS, and collaboration platforms such as Google Workspace and Slack. Governance roles and control activities shall be defined with annual or quarterly review cycles to ensure oversight and continuous improvement. This policy applies to all personnel, contractors, and systems within Casper Studios’ hybrid cloud and home-office environments.

Table of Contents

1. Document Content Page

This document comprises the sections listed in the Table of Contents and defines controls, roles, and processes in strict alignment with SOC 2 Trust Services Criteria.

2. Applicability and Scope

This policy shall apply to all Casper Studios employees, contractors, and third parties with access to information systems, data, networks, AWS environments, Google Workspace, and home-office devices. It shall govern use of company-provided laptops and collaboration tools (Slack, Figma, Linear, Zoom). All cloud and on-premise assets storing or processing employee data shall be included in

scope.

3. Security Governance Roles

1. Information Security Officer (ISO) shall centrally manage the SOC 2 program, approve controls, and report quarterly to senior management.
2. Compliance Program Manager shall maintain risk assessments and vendor reviews, ensuring annual updates and remediation tracking.
3. People Operations Officer shall enforce pre-employment screening and coordinate security training for all new hires, including AWS and Google Workspace access.

4. Policy Compliance Controls

1. Staff shall acknowledge the Information Security Program upon onboarding and annually thereafter (T-003, T-002).
2. All policies and procedures shall be published in the company intranet and Google Drive for immediate access (T-022).
3. Control activities for AWS access, email authentication (Google Workspace), and Slack integrations shall be documented and enforced through automated configuration management tools.

5. Management Security Accountability

1. Senior management shall review and approve the Information Security Program, Risk Assessment, and Vendor Risk Assessment annually (T-010 to T-014, T-038).
2. Quarterly reports on control effectiveness and remediation status shall be presented to the Board or designate.
3. Insights from annual reviews shall drive control enhancements and updated SOPs (T-048 to T-052).

6. Personnel Security

1. Conduct identity verification and background checks before granting AWS or system access (T-016).
2. Deliver role-based security and privacy training during onboarding and quarterly refreshers; track completion in HRIS.
3. Retain training records, screening results, and access logs for a minimum of seven years in compliance with SOC 2 Data Retention requirements.

7. Exceptions Process

Personnel shall submit exception requests in Linear with business justification, compensating controls, duration, and risk assessments. The ISO and Compliance Program Manager shall approve and time-box exceptions, with expiration checks at least quarterly.

8. Violations and Disciplinary Action

Automated monitoring shall detect policy violations; incidents shall be reported to the ISO and People Operations. Confirmed violations shall result in corrective action per HR policy—verbal warning, written warning, suspension, or termination—aligned with severity.

9. Auditor Evidence Artefacts

- Access logs from AWS, Google Workspace, Slack
- Policy acknowledgment tickets in Linear
- Annual review meeting minutes and approval emails
- Training completion certificates and HRIS records
- Exception approval tickets and expiration logs
- Security incident reports and remediation evidence (screenshots, patch logs)