Risk Management Policy

This policy establishes a structured risk management process to identify, analyze, and treat threats that could jeopardize the organization’s ability to meet its security commitments and business objectives.

Risk Management Policy

Executive Summary

Casper Studios shall identify, assess, and mitigate information security risks to ensure confidentiality, integrity, and availability in alignment with SOC 2 risk management criteria. The Information Security Officer and Risk Owner shall perform risk assessments at least annually and update risk treatment plans quarterly, covering AWS deployments and home office environments. Exceptions require documented approval and regular reviews to maintain control effectiveness.

1. Document Content Page

2. A. Applicability and Scope

This policy shall apply to all Casper Studios employees, contractors, and third-party service providers accessing AWS-hosted applications and employee data from company-provided laptops or home offices. Covered tools include Google Workspace, Slack, Linear, Figma, and Zoom in all regions. The Information Security Officer and Risk Owner shall enforce and review applicability quarterly.

3. B. SOC 2 Control Mapping

Risk Assessment and Treatment

1. (TSC.CC3.1) Casper Studios shall identify and document information security risks to its AWS-hosted services, home-office environments, and Google Workspace assets at least annually.
2. (TSC.CC3.4) The Information Security Officer shall assess each risk’s likelihood and impact on confidentiality, integrity, and availability, assigning risk scores and prioritizing remediation within 30

days.

3. (TSC.CC3.6) The Risk Owner shall define and implement risk responses, including acceptance, mitigation, transfer, or avoidance, aligning with Casper Studios' risk appetite documented in Comp AI.
4. (TSC.CC3.7) Quarterly reviews of risk mitigation plans shall be conducted and results reported to senior management to ensure effectiveness.
5. (TSC.CC5.2) Potential fraud risks shall be included in the risk matrix and reviewed in collaboration with HR and Legal.

4. C. Exceptions Process

Employees and contractors shall submit exception requests through Linear, including business justification, compensating controls, and duration. The Information Security Officer and Risk Owner shall jointly approve, document, and time-limit exceptions, which shall be reviewed at least quarterly or upon significant risk changes.

5. D. Violations and Disciplinary Action

Continuous monitoring using AWS CloudWatch and security logs shall detect non-compliance. Suspected violations must be reported to the Information Security Officer and HR. Confirmed violations shall result in disciplinary actions consistent with HR policies, up to termination, and may include immediate mitigation or legal referral.

6. Auditor Evidence Artefacts

- AWS CloudTrail and CloudWatch logs
- Risk assessment reports and scoring matrices
- Linear tickets for exception requests and approvals
- Approval records from Slack notifications and email archives
- Screenshots of quarterly review meeting agendas and minutes