Third-Party Risk Management Policy

This policy ensures that vendors and other third parties do not introduce unacceptable risk to the organization by establishing a structured program for assessing, monitoring, and mitigating supplier risks aligned with security commitments and regulatory requirements.

Table of Contents

Executive Summary

This Third-Party Risk Management Policy ensures that Casper Studios identifies, evaluates, and mitigates vendor risks in strict alignment with SOC 2 security and confidentiality criteria. It mandates annual risk assessments and quarterly monitoring of all third parties that handle organizational or employee data in AWS and home-office environments. Roles and responsibilities are defined for the Information Security Officer, Vendor Owners, and senior management, with all exceptions documented and approved in Linear within five business days.

2. Applicability & Scope

This policy applies to all Casper Studios employees, contractors, and business units in hybrid office and home-office settings who select, onboard, manage, or rely on third parties that store, process, or transmit organizational or employee data within AWS regions. It applies to all vendor engagements via Google Workspace, Slack, Linear, Figma, Zoom, or other enterprise services. The Information Security Officer shall ensure enforcement across corporate-provided laptops and Google Workspace identities.

3. Controls

1. Vendor Classification: All third parties must be classified based on data criticality and SOC 2 risk categories; classification must be reviewed annually.
2. Due Diligence: The Information Security Officer and Vendor Owner shall conduct formal vendor security assessments at onboarding and recurrently on a 12-month cycle.
3. Contractual Requirements: All contracts must include SOC 2-required security, confidentiality, and data handling clauses before engagement; Legal shall verify compliance prior to signature.

4. Continuous Monitoring: Vendor performance metrics and security controls shall be reviewed quarterly, with findings documented via AWS CloudTrail and security dashboards.
5. Issue Remediation: All identified vendor control gaps must be remediated within 30 days and tracked in Linear with SLA targets; status is reported by the Vendor Owner.

4. Exceptions Process

Any deviation from this policy must be submitted via Linear with business justification, compensating controls, and time limit. The Information Security Officer and Vendor Owner must jointly approve or reject requests within five business days; all decisions must be documented and reviewed quarterly.

5. Violations & Disciplinary Action

Non-compliance shall be detected via continuous AWS CloudTrail monitoring and vendor performance reports. Suspected violations must be escalated to the Information Security Officer and HR within three business days. Confirmed violations will result in disciplinary actions up to contract termination, per Casper Studios HR policy.

6. Auditor Evidence Artefacts

- AWS CloudTrail logs demonstrating vendor access and review dates
- Annual vendor risk assessment reports
- Signed vendor contracts with SOC 2 clauses
- Quarterly monitoring reports and remediation tickets from Linear
- Exception approval records in Linear (timestamps and approvers)
- Screenshots of AWS security dashboard configurations