Acceptable Use Policy

Define acceptable behaviour and technology usage so employees safeguard organisational assets, uphold confidentiality, integrity and availability, and foster a respectful work environment.

Executive Summary

Casper Studios' Acceptable Use Policy defines mandatory behaviours and controls to protect the confidentiality, integrity, and availability of AWS-hosted and corporate assets in strict alignment with SOC 2 Trust Services Criteria.

This policy applies to all employees, contractors, interns, and third parties accessing Casper Studios systems (Google Workspace, Slack, Linear, Figma, Zoom) via company-provided laptops or enrolled BYOD in home-office or hybrid work settings.

Controls are monitored quarterly, and the Information Security Officer shall review this policy annually.

Table of Contents

1. Scope and Applicability

This policy shall apply to all Casper Studios employees, contractors, interns, and third parties who access or use company systems, networks, devices or data in any location (office, home-office, or hybrid) from onboarding through off-boarding.

2. Controls

2.1 Acceptable Use Standards

• Users shall access company resources only with unique, organization-issued credentials protected by MFA (CC6.1); credentials must never be shared or left unattended.

- Endpoints shall install security patches within 7 days of release, run approved endpoint protection (enable full-disk encryption, and auto-lock after no more than 5 minutes idle (CC7.2).
- Sensitive data shall be stored only in AWS approved services (e.g., S3, RDS) and transmitted via encrypted channels (TLS 1.2+ or corporate VPN) in accordance with CC3.4.
- On untrusted networks users must connect via corporate VPN; creating unauthorized personal hotspots or using network-scanning tools is prohibited (CC6.4).
- Prohibited activities include using pirated software, accessing illegal content, harassment, crypto-mining, personal commercial ventures, or any actions that degrade service or security (CC6.3).
- All activity on corporate assets may be logged and monitored continuously (CC7.3); users shall have no expectation of personal privacy.
- Personal devices accessing company data must enroll in MDM and are subject to remote wipe upon termination or suspected compromise (CC6.1).

3. Policy Acknowledgement

- All new personnel shall acknowledge this policy during onboarding via Google Workspace forms (CC2.3).
- All personnel shall re-acknowledge annually or upon significant policy changes to reinforce accountability.

4. Exceptions Process

Employees shall request acceptable-use exceptions through Linear ticketing with business justification, compensating controls and duration; the Information Security Officer and HR Manager shall jointly approve, document, time-limit, and review each exception at or before expiration (CC5.2).

5. Violations and Disciplinary Action

Automated monitoring and quarterly audits shall detect non-compliance; suspected violations are reported to the Information Security Officer and HR Manager for investigation. Confirmed violations shall follow HR disciplinary tiers—verbal warning, written warning, suspension, or termination—and may include immediate access revocation or legal action (CC7.4).

6. Auditor Evidence Artefacts

- Access logs and MFA reports
- Patch and encryption deployment tickets
- Data storage configuration screenshots
- Annual policy acknowledgement records
- Exception approval tickets