# Business Continuity Policy

This policy ensures the organization can quickly restore critical operations after a disruption by maintaining reliable backups, robust disaster-recovery plans, and validated continuity procedures, thereby reducing the risk of prolonged outages, data loss, and safety hazards.

---

# Table of Contents



# Executive Summary

Casper Studios shall maintain business continuity to ensure rapid recovery of critical operations by aligning disaster recovery and backup processes with SOC 2 Trust Services Criteria. The policy addresses cloud-based and remote working environments using AWS infrastructure and company-provided laptops to mitigate risks of data loss, prolonged outages, and service disruption. All controls shall be reviewed quarterly and validated through testing to ensure effectiveness.

# Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third parties who design, operate, or support information systems, infrastructure, and facilities in AWS or home offices. It covers backup, disaster recovery, and continuity procedures for AI product development and employee data. Roles include the Information Security Officer, Business Continuity Manager, and IT Operations team.

# Business Continuity Controls

# Backup Management (SOC 2 CC7.1)

1. Casper Studios must maintain automated backups of all critical system and user data in AWS with an RPO of four hours and an RTO of eight hours.
2. Backups shall be encrypted in transit and at rest using AES-256 and stored in a separate AWS account.

3. Backup integrity shall be verified by IT Operations monthly, and verification reports shall be submitted to the Information Security Officer.

# Disaster Recovery Planning (SOC 2 CC7.2)

1. The Business Continuity Manager shall maintain a documented disaster recovery plan defining roles, responsibilities, and procedures for restoring AWS-hosted services.
2. The disaster recovery plan shall be tested quarterly via simulated failover exercises involving IT Operations and key stakeholders.
3. Test results and remediation actions shall be documented and reviewed by senior leadership within two weeks of each exercise.

# Infrastructure Resilience (SOC 2 CC7.3)

1. Critical services must run in multi-AZ AWS deployments to ensure high availability and fault tolerance.
2. Network configurations and security groups shall be reviewed quarterly by IT Operations to validate resilience and secure remote access.
3. Configuration changes impacting continuity must be approved by the Information Security Officer and tracked in Linear.

# Exceptions Process

All exceptions to this policy must be submitted via Slack ticket with business justification, compensating controls, and duration. The Information Security Officer and Business Continuity Manager shall review exceptions within five business days; approved exceptions shall be documented, time-bound, and re-evaluated before expiry.

# Violations and Disciplinary Action

Non-compliance shall be detected through audits, monitoring tools, and incident reviews. Suspected violations must be reported to the Information Security Officer and HR. Confirmed violations shall result in disciplinary action up to termination, immediate access revocation, and possible legal proceedings.

# Audit Evidence

- AWS backup logs and snapshot records
- Quarterly disaster recovery test plans, reports, and meeting minutes
- Configuration change approval tickets in Linear
- Exception request and approval records from Slack tickets
- Quarterly policy review and sign-off by Information Security Officer