Change Management Policy

This policy ensures that all changes to the operating environment are planned, approved, tested, and documented so that system integrity, availability, and accuracy are preserved during and after implementation.

Table of Contents

Executive Summary

Casper Studios must ensure that all changes to AWS-hosted infrastructure and applications are systematically managed to preserve system integrity, availability, and accuracy in alignment with SOC 2 Trust Services Criteria. Change Management and Configuration Management controls shall be mandatory, reviewed quarterly and annually, and enforced via automated pipelines and audit logs. Non-compliance triggers defined exception and disciplinary processes, with artifacts retained for SOC 2 audit evidence.

Document Content Page

Applicability and Scope

This Change Management Policy applies to all Casper Studios employees, contractors, and third-party service providers managing or deploying changes in AWS production, staging, and development environments using company-provided laptops and remote access. It covers code, infrastructure, configuration, and system dependencies, with all documentation stored in Google Workspace and Linear. The Information Security Officer shall review this policy annually to ensure ongoing SOC 2 compliance.

Change Management Controls

1. Change requests must be submitted via Linear with clear scope, impact assessment, and rollback plan, and automatically logged in AWS CloudTrail (SOC 2 CC6.1).

2. All change requests must be approved by the Change Advisory Board (CAB), and by the Information Security Officer prior to execution (SOC 2 CC6.1).
3. Emergency changes must follow a documented emergency change process with retroactive approval and post-implementation review completed within five business days (SOC 2 CC6.1).
4. Regression testing must be performed in isolated AWS staging environments and results must be documented in Google Workspace before any production deployment (SOC 2 CC6.3).
5. All deployments shall use automated CI/CD pipelines with IaC (e.g., AWS CloudFormation) and rollback capability to maintain consistency and accuracy (SOC 2 CC6.3).
6. The Information Security Officer shall perform quarterly reviews of change management metrics and compliance dashboards to ensure control effectiveness.

Configuration Management Controls

1. Configuration changes must be defined in standardized IaC templates and tracked via AWS Config (SOC 2 CC7.1).
2. All configuration changes must receive CAB and Information Security Officer authorization, with approvals attached to Linear tickets (SOC 2 CC7.1).
3. Configuration baselines shall be defined and approved by the Security Engineer, with quarterly verification to detect drift (SOC 2 CC7.1).
4. Unauthorized drift must be detected via AWS Config rules and remediated within 48 hours of detection (SOC 2 CC7.1).
5. The Information Security Officer shall perform an annual review of configuration management reports for completeness and accuracy (SOC 2 CC7.1).

Exceptions Process

Exception requests shall be submitted via Linear with business justification, compensating controls, and requested duration. The CAB and Information Security Officer must jointly approve, document, and time-limit each exception, which shall be reviewed at or before expiration. Exception approvals and denials must be recorded in AWS CloudTrail and reviewed quarterly.

Violations and Disciplinary Actions

Automated audits via AWS CloudTrail, AWS Config, and CI/CD logs must detect non-compliance. Suspected violations must be reported immediately to the Information Security Officer and HR. Confirmed violations shall result in disciplinary actions—ranging from formal warnings to termination per HR policy—and may include immediate change rollback and remediation within three business days.

Auditor Evidence Artefacts

- Linear change request tickets with approval timestamps
- AWS CloudTrail and AWS Config logs of change events
- Regression and configuration test results documented in Google Workspace
- CAB meeting minutes and approval records

- Exception request records and time-bound approvals
- Quarterly and annual review reports by the Information Security Officer