Capacity & Performance Management

This policy ensures critical assets are continuously monitored for capacity, performance, and anomalous behavior so the organization can anticipate demand, prevent service degradation, and defend against denial-of-service or other capacity-related threats.

Table of Contents

Document Content Page

Executive Summary

This Capacity & Performance Management policy mandates continuous monitoring and alerting of critical cloud assets to anticipate demand, prevent service degradation, and defend against denial-of-service threats. It aligns with SOC 2 CC7 controls by enforcing measurable review cycles, documented approvals, and incident response triggers. Roles and responsibilities are assigned across the Infrastructure Team, DevOps Lead, and Information Security Officer to ensure accountability and compliance.

A. Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third parties who design, operate, or support production infrastructure, applications, networks, and AWS resources that handle business-critical workloads in AWS. It covers capacity, performance, and anomaly monitoring activities using company-provided laptops and Google Workspace authentication. Compliance is mandatory for Slack, Linear, Figma, Zoom integrations, and AWS-hosted systems.

B. Controls

Resource Capacity Management

1. CloudWatch and custom metrics shall monitor EC2, RDS, Lambda, and ELB every 5 minutes. Alerts for CPU, memory, network, and I/O thresholds must be configured and tested quarterly to detect capacity and performance issues and potential denial-of-service activity.
2. The Information Security Officer shall review capacity and performance dashboards monthly and lead quarterly capacity planning sessions to forecast demand, document headroom requirements, and update the capacity planning repository.
3. System Administrators shall analyze alerts and logs for anomalous behavior within 15 minutes of trigger, initiate incident response per the Incident Response Policy, and escalate unresolved issues to the DevOps Lead and InfoSec Officer.
4. All capacity and performance configurations, alert rules, and monitoring scripts shall undergo annual validation by an independent auditor or via automated compliance checks integrated in the CI/CD pipeline.

C. Exceptions Process

Employees must submit capacity-management exceptions through our ticketing system, providing business justification, compensating controls, and requested duration. The DevOps Lead and Information Security Officer shall approve or deny exceptions within 3 business days. All approved exceptions expire after 30 days and are reviewed by the Security Steering Committee quarterly.

D. Violations and Disciplinary Action

Automated monitoring, monthly performance audits, and management reviews shall detect non-compliance. Suspected violations must be reported to the Information Security Officer and HR within 24 hours. Confirmed violations trigger HR disciplinary tiers (verbal warning, written warning, suspension, termination) and immediate access revocation for critical non-compliance.

Auditor Evidence Artefacts

- Screenshots of AWS CloudWatch monitoring configurations and alert rules.
- Monthly and quarterly capacity and performance reports.
- Alert and incident tickets from the ticketing system.
- Approval records from the DevOps Lead and Information Security Officer.
- Audit logs demonstrating alert triggers, incident responses, and follow-up actions.