Incident Response Policy

This policy ensures the organization can rapidly detect, report, and respond to information-security incidents to minimize business impact, fulfill legal obligations, and protect stakeholder interests.

Incident Response Policy

Executive Summary

Casper Studios must rapidly detect, report, and respond to security incidents affecting its AWS-hosted applications and home-office environments to minimize business impact and maintain SOC 2 compliance. The policy applies to all employees, contractors, and third-party vendors using Google Workspace and company-provided laptops to access corporate systems. The Information Security Officer shall review the policy quarterly and perform an annual audit to ensure continued alignment with SOC 2 CC7 and CC8 controls.

Table of Contents

Document Content Page

- Policy Title: Incident Response Policy
- Owner: Information Security Officer
- Review Cycle: Quarterly technical review; Annual SOC 2 audit

Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third-party vendors accessing systems in AWS or remote environments via Google Workspace, Figma, Slack, and Zoom on company-provided laptops. It covers the full incident lifecycle—from detection through closure—for events impacting the confidentiality, integrity, or availability of employee data. The Incident Response Lead must review scope applicability quarterly.

Controls

Incident Detection and Reporting

1. Casper Studios must deploy and maintain AWS CloudWatch, GuardDuty, and Slack-integrated alerts to detect anomalies and security events in real time (SOC 2 CC7.2).
2. Employees and contractors must report suspected incidents via the internal incident-ticketing system and to ir@casperstudios.xyz within 1 hour of detection (SOC 2 CC7.2).
3. The Incident Response Lead shall review all alerts daily and escalate high-severity events to the Information Security Officer within 2 hours.

Incident Response and Recovery

1. Casper Studios shall maintain a documented AWS-centric incident-response runbook defining roles (Incident Response Lead, Engineering Team, Information Security Officer) and response steps (SOC 2 CC7.3).
2. The Incident Response team must contain and eradicate incidents within 24 hours, performing root-cause analysis and recovery actions on cloud and home-office endpoints.
3. The Information Security Officer shall notify stakeholders and customers per breach notification guidelines within 72 hours of incident confirmation (SOC 2 CC7.4).
4. Post-incident reviews must be conducted within 10 business days and documented for continuous improvement; lessons learned shall be presented quarterly to executive management.

Exceptions Process

Employees must submit exception requests to the incident-ticketing system with justification, compensating controls, and duration. The Information Security Officer and Incident Response Lead shall approve or reject exceptions within 5 business days. Exceptions must be reviewed at expiration and no later than 30 days.

Violations and Disciplinary Action

Compliance monitoring tools shall detect policy deviations. Suspected violations must be reported to the Information Security Officer and HR within 24 hours. Confirmed violations shall result in disciplinary actions per company policy, up to termination and legal action; access privileges will be revoked immediately.

Auditor Evidence Artefacts

- AWS GuardDuty and CloudWatch logs
- Incident ticket records and timelines
- Approval records from the ticketing system
- Post-incident review reports and meeting minutes
- Stakeholder notification logs and screenshots