Vulnerability Management Policy

This policy ensures timely identification, evaluation, and remediation of vulnerabilities to prevent exploitation, reduce business impact, and maintain the confidentiality, integrity, and availability of organizational systems and data.

Executive Summary

This Vulnerability Management Policy defines how Casper Studios shall identify, assess, and remediate vulnerabilities within its AWS-hosted infrastructure and company-provided laptops. It aligns with SOC 2 Security and Monitoring controls by mandating monthly automated scans, quarterly reviews, and annual penetration tests. All remediation activities must be tracked in Linear and reviewed by the Security Lead quarterly.

Table of Contents

Scope and Applicability

This policy applies to all Casper Studios employees, contractors, and third-party service providers who design, administer, or use cloud-hosted infrastructure on AWS and company-provided laptops in home offices. All systems authenticating via Google Workspace or email/password must be included. Data in scope includes employee data and system metadata.

Controls

Vulnerability Identification and Assessment

1. Casper Studios shall perform automated vulnerability scans of AWS environments and company-provided laptops at least monthly
2. The Security Lead shall review scan results and prioritize findings by CVSS score within five business days of scan completion.

3. Annual penetration testing of public-facing systems shall be conducted by a qualified third party, with a report delivered to the InfoSec Officer.

Remediation Tracking and Reporting

1. All identified vulnerabilities must be entered into Linear within one business day and assigned an SLA: critical within one week, high within two weeks, medium within one month, low within one quarter.
2. Remediation progress shall be reviewed by the Vulnerability Management Lead quarterly and reported to executive management.

Configuration and Patch Management

1. Company-provided laptops shall receive OS and application patches within one month of vendor release during monthly maintenance windows.
2. AWS AMIs and container images shall be rebuilt and redeployed with security updates at least quarterly.

Exceptions Process

Exceptions to this policy must be requested via the Linear ticketing system with business justification, compensating controls, and duration. The InfoSec Officer and Vulnerability Management Lead shall jointly approve and time-limit exceptions. All exceptions shall be reviewed quarterly.

Violations and Disciplinary Action

Non-compliance is detected via automated scan reports, patch status dashboards, and security audits. Violations shall be reported to the InfoSec Officer and HR. Confirmed violations may result in verbal or written warnings, suspension, termination, and immediate access revocation.

Auditor Evidence Artefacts

- Monthly vulnerability scan logs
- Annual penetration test reports
- Linear remediation tickets with SLA timestamps
- Exception approval records
- Patch compliance and deployment screenshots