Secure Development Policy

This policy embeds secure-coding and data-validation practices into the software development life cycle (SDLC) to preserve processing integrity and prevent unauthorized or malformed data from compromising organizational systems.

Secure Development Policy

Executive Summary

Casper Studios shall enforce SOC 2–aligned secure development controls across its AWS-hosted environments and home-office configurations to ensure processing integrity and confidentiality. All secure SDLC processes must be reviewed quarterly by the Application Security Lead and approved by the Information Security Officer. Automated validation, code review, and continuous monitoring shall prevent unauthorized or malformed data from impacting systems.

Table of Contents

1. Scope and Applicability

This policy applies to all Casper Studios employees, contractors, and third-party service providers who design, develop, test, or maintain software that stores, processes, or transmits employee data in AWS (us-east-1) or home-office networks. Company-provided laptops must enforce disk encryption, endpoint protection, and VPN for cloud resource access. Roles include Software Developers, Application Security Lead, and Information Security Officer.

2. Secure SDLC Controls

2.1 Requirements and Design Review (SOC 2 CC3.1, CC6.1)

• Requirements shall be documented in Linear with security criteria and approved by the Application Security Lead before development. \n• Architecture diagrams for AWS deployments shall include IAM roles, VPC segmentation, and encryption at rest and in transit (TLS 1.2+).

2.2 Implementation and Validation (SOC 2 CC7.1)

• All code must pass automated static analysis (SAST) in CI/CD pipelines (GitHub Actions) and dynamic analysis (DAST) monthly. \n• Input validation routines must enforce type, length, format, and range checks for all user and API inputs. \n• Mandatory fields and schema validation shall be enforced at the application and database layers (RDS PostgreSQL).

2.3 Code Review and Approval

• Peer code reviews in GitHub are mandatory; pull requests must have approval from at least one senior developer and the Application Security Lead. \n• Secrets scanning (GitGuardian) and dependency vulnerability checks (Dependabot) shall block merges until remediated.

2.4 Deployment and Monitoring

• Production deployments via Terraform in AWS require approval tickets in Linear. \n• CloudWatch and GuardDuty alerts shall be configured for anomalous activity; the InfoSec Officer reviews alerts daily. \n• Quarterly penetration tests shall be conducted by a qualified external vendor.

3. Exception Handling

Developers must submit exception requests in Linear, including business justification, compensating controls, and expiration date. The Application Security Lead and Information Security Officer shall jointly evaluate and approve exceptions, which are reviewed at or before expiration.

4. Violations and Remediation

Non-compliance detected via automated scans, code reviews, or audit findings must be reported to the Information Security Officer within 24 hours. Violations shall invoke remediation plans with defined timelines, and HR disciplinary action follows confirmed incidents per severity tiers (warning to termination). All security incidents requiring legal notification shall follow the Incident Response Policy.

5. Audit Evidence

- CI/CD pipeline logs showing SAST/DAST results
- Linear tickets for design reviews and exception approvals
- GitHub pull-request approvals and secrets-scan screenshots
- AWS CloudWatch and GuardDuty alert logs
- Quarterly penetration test reports