Privacy Policy

This policy embeds privacy-by-design principles across all business processes to protect personal data, meet global regulatory requirements, and maintain stakeholder trust.

Table of Contents

Executive Summary

Casper Studios shall embed privacy-by-design aligned with SOC 2 Privacy and Confidentiality Criteria across all processes to safeguard employee data and customer PII. The policy defines mandatory governance, data inventory, access controls, retention, vendor management, incident response, and monitoring controls for AWS-hosted applications and remote work. This policy shall be reviewed quarterly by the Privacy Officer and Information Security Manager.

Document Content Page

1. Applicability & Scope

This policy applies to all Casper Studios employees, contractors, and third parties collecting, processing, or storing employee or customer data on AWS, Google Workspace, Slack, Linear, Figma, or Zoom, in office and home-office environments.

2. Privacy Controls (SOC 2 Aligned)

2.1 Governance & Accountability

Casper Studios shall appoint a Privacy Officer and an Information Security Manager to oversee SOC 2 control implementation and compliance; responsibilities and delegations shall be documented and reviewed quarterly.

2.2 Data Inventory & Classification

Maintain an up-to-date inventory of employee and customer data categories in AWS Config and Google Workspace; classification and usage purposes shall be validated quarterly.

2.3 Data Lifecycle & Retention

Define retention periods for each data category; data shall be archived or securely disposed in AWS S3 per schedule and reviewed annually.

3.4 Access & Authorization

All access to privacy-related systems (AWS, Google Workspace, Slack) must require MFA and be provisioned via formal ticketing with manager approval; access rights shall be reviewed quarterly.

3.5 Vendor & Third-Party Management

Maintain a list of third-party processors with privacy clauses in contracts; conduct privacy-risk assessments annually and require notifications of unauthorized disclosures within 24 hours.

3.6 Incident Response & Monitoring

Monitor AWS CloudTrail, Google Workspace logs, and Slack audit logs daily; the incident response team shall investigate and notify affected parties within 24 hours of breach detection and conduct post-incident reviews quarterly.

4. Exceptions Process

Exceptions shall be requested via the ticketing system with business justification and compensating controls; the Privacy Officer and Information Security Manager shall jointly approve and time-limit each exception and review before expiration.

5. Violations & Disciplinary Action

Suspected policy violations must be reported to the Privacy Officer and HR; confirmed violations shall follow HR disciplinary procedures (verbal warning, written warning, suspension, termination) and may involve regulatory notification.

6. Auditor Evidence Artefacts

- Access review reports from ticketing system.
- AWS CloudTrail and Google Workspace activity logs.
- Privacy-risk assessment records.
- Incident and breach response tickets and post-incident reports.
- Vendor privacy compliance assessment documentation.