Information Protection Policy

This policy preserves the confidentiality, integrity, and availability of organizational information by establishing clear requirements for data retention and secure disposal, network protections, and strong cryptographic safeguards for data at rest and in transit.

Table of Contents

Executive Summary

Casper Studios' Information Protection Policy establishes mandatory requirements to preserve the confidentiality, integrity, and availability of employee and business data across AWS-hosted systems and company-provided laptops in compliance with SOC 2 Security and Confidentiality criteria. The policy mandates defined retention and disposal schedules, network segmentation with deny-by-default firewall rules, and AWS KMS-backed encryption in transit and at rest, all subject to quarterly reviews. All personnel, contractors, and third-party administrators shall comply with these controls, with any deviations managed through a documented exception process.

Document Contents

Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third-party service providers who access, create, store, transmit, or manage organizational information in AWS (e.g., us-east-1, us-west-2), Google Workspace, Slack, Linear, Figma, or Zoom on company-provided laptops or authorized home-office devices. It covers all environments—production and non-production—as well as network infrastructure, databases, and endpoints. Roles subject to this policy include but are not limited to system administrators, developers, HR personnel, and third-party auditors.

Controls

Data Retention and Disposal

1. Retention periods must be defined per data classification (e.g., employee records retained for seven years) and documented in Linear, subject to quarterly review by the Information Security Officer. AWS S3 lifecycle policies or equivalent automated mechanisms shall enforce secure deletion in accordance with NIST 800-88 guidelines. Disposal process efficacy must be validated quarterly and logged in Google Workspace audit logs.
2. Media decommissioning (e.g., AWS EBS volumes, local disk images) must employ cryptographic wipe or overwriting procedures; evidence of sanitization shall be retained for audit and reviewed annually.

Network Security

1. All AWS workloads must reside in VPC subnets with Security Groups and Network ACLs configured with deny-by-default rules; changes shall be approved via Slack #security-alerts and reviewed quarterly. Home-office connections must use company VPN and local firewall policies matching deny-by-default principles.
2. Every host (production and non-production) running on AWS or company laptops must enforce a host-based firewall (e.g., ufw, Windows Defender Firewall) with deny-by-default and allow-list rules; configurations are to be audited quarterly.
3. Communications protection controls shall require TLS 1.2 or higher for all internal and external traffic, using AWS Certificate Manager for certificate management, reviewed quarterly for expiration and cipher strength.

Data Transmission Security

1. All data in transit across public or untrusted networks must use industry-standard encryption (HTTPS/TLS 1.2+); configuration must be captured in Figma network diagrams and reviewed quarterly.
2. Production and non-production databases handling employee data must encrypt data at rest using AWS KMS-managed keys; key rotation shall occur annually and be logged in AWS CloudTrail.

Exceptions Process

Personnel must submit exception requests in Linear, providing business justification, compensating controls, and proposed duration. The Information Security Officer and relevant data owner shall jointly review and approve exceptions, documenting decisions and timing in Slack #security-exceptions. All exceptions must be reviewed at or before expiration, no less frequently than quarterly.

Violations and Disciplinary Action

Continuous monitoring via AWS CloudWatch, Google Workspace audit logs, and Slack integrations shall detect non-compliance. Suspected violations must be reported immediately to the Information Security Officer and HR for investigation. Confirmed violations shall invoke disciplinary procedures—verbal warning, written warning, suspension, or termination—aligned with severity and may include immediate access revocation.

Auditor Evidence Artefacts

- Retention and deletion logs (AWS S3 lifecycle, NIST 800-88 reports)
- Security Group and firewall configuration screenshots
- AWS CloudTrail and CloudWatch logs
- TLS certificate inventories and renewal tickets
- Exception request tickets and approval records