# Endpoint Protection Policy

This policy safeguards the organization’s information assets by ensuring endpoints are protected against malware, encrypted against unauthorized access, and accurately inventoried, thereby minimizing the risk of compromise, data loss, or service disruption.

---

# Executive Summary

This Endpoint Protection Policy defines mandatory controls for Casper Studios’ cloud and home-office endpoints to meet SOC 2 requirements. It assigns roles, specifies measurable review cycles, and leverages AWS us-east-1 and Google Workspace integrations to protect employee data. All unresolved configuration details are marked for review.

# Table of Contents



# 2. Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third parties configuring, using, or managing company-provided laptops, home-office desktops, and AWS EC2 instances in us-east-1 that access, store, or process employee data.

# 3. Controls

# 3.1 Malware Protection

1. All endpoints accessing AWS-hosted applications or storing employee data must have approved anti-malware software (e.g., Sophos Endpoint Protection agent version) installed, configured, and updated daily; the Security Administrator shall verify signature updates quarterly.

# 3.2 Inventory and Encryption

1. The IT Manager must maintain an automated endpoint inventory via AWS Config and a CMDB, reviewing asset records quarterly for accuracy and completeness.

2. All company-provided laptops and EBS volumes shall be encrypted with AES-256 using AWS KMS keys managed in us-east-1; compliance scans shall run monthly.

## 3.3 Endpoint Security Administration

1. The Security Administrator shall document and maintain endpoint configuration procedures in the internal Security Wiki, reviewing them annually.
2. Encryption keys and anti-malware policies must be centrally managed via AWS IAM and Google Workspace APIs, with access reviewed quarterly by Executive Management.

# 4. Exceptions Process

Employees must request endpoint exceptions through Linear tickets, including business justification, compensating controls, and duration capped at 30 days. The Information Security Officer and IT Manager shall jointly approve, document, and time-limit each exception; all exceptions shall be re-evaluated at expiration.

# 5. Violations and Disciplinary Action

Automated monitoring via AWS CloudWatch and intrusion detection systems shall detect non-compliance. Suspected violations must be reported to the Information Security Officer and HR within 24 hours. Confirmed violations will trigger HR disciplinary tiers (verbal warning through termination) and may include immediate access revocation or device quarantine.

# 6. Auditor Evidence Artefacts

- AWS Config export reports and KMS key configuration screenshots
- Daily anti-malware update logs and quarterly verification records
- CMDB asset inventory exports with quarterly review annotations
- Linear exception request and approval tickets
- Incident reports and HR disciplinary action logs
- Minutes from quarterly security review meetings