# Access Control Policy

This policy establishes controls that limit access to information systems and data to authorized users, thereby reducing the risk of unauthorized disclosure, alteration, or disruption of critical services.

---

# Table of Contents



# Executive Summary


This Access Control Policy for Casper Studios establishes mandatory controls over logical and physical access to AWS environments, company-provided laptops, and cloud applications (Google Workspace, Slack, Linear, Figma, Zoom) in strict alignment with SOC 2 Trust Services Criteria. It defines roles (Information Security Officer, System Owners, HR), enforces least-privilege and MFA via Google Workspace and AWS IAM, and mandates quarterly and annual reviews. All exceptions, monitoring, and disciplinary processes are documented and auditable.


# 2. Applicability and Scope

This policy applies to all Casper Studios employees, contractors, and third-party vendors using company-provided laptops, home offices, or office workstations to access production consoles, databases, applications, networks, and AWS cloud resources. It covers authentication via Google Workspace, email/password, and integration with Slack, Linear, Figma, and Zoom. All access management activities must align with SOC 2 CC6.1 (Logical and Physical Access Controls) and CC7.1 (Change Management).

# 3. Controls

# 3.1 Access Rights

1. The Information Security Officer shall review and approve the list of IAM users and roles with production access in AWS quarterly.

2. System Owners must approve access requests based on documented job functions and least-privilege principle; all requests are tracked in Linear tickets.
3. User registration and authorization procedures shall be maintained and reviewed annually.
4. Continuous monitoring of AWS CloudTrail logs must alert the security team to unauthorized or anomalous access within 24 hours.
5. Access shall be revoked or disabled within one business day upon role change or termination, as recorded in HR ticketing.
6. Production database (RDS) privileges must be restricted to roles with documented business need and reviewed annually.
7. Administrative privileges are limited to the Information Security Officer and designated System Owners and reviewed quarterly.
8. All privilege escalation events must be approved in Linear and reviewed during quarterly access audits.

## 3.2 Credential Management

1. Passwords must be at least 12 characters with complexity rules enforced via Google Workspace password policy.
2. Multi-factor authentication is mandatory for all Google Workspace and AWS IAM users without exception.
3. Credentials shall be rotated every 180 days and immediately upon suspected compromise.

## 3.3 Remote-Work Security

1. All remote devices must run a managed Endpoint Detection and Response agent, updated monthly.
2. Company laptops shall auto-lock after 5 minutes of inactivity in home-office or public environments.
3. Remote device compliance scans must occur daily via MDM and reported to the security team.

## 3.4 Segregation of Duties

1. Responsibilities for code deployment, change approval, and production access shall be separated between development, operations, and security teams.

# 4. Exceptions Process

All access exceptions must be requested through Linear, include business justification, compensating controls, and duration (max 30 days), and be approved jointly by the Information Security Officer and CTO. Exception tickets shall be reviewed at expiration or quarterly, whichever is sooner.

# 5. Violations and Disciplinary Action

Automated monitoring via CloudTrail and periodic audits shall detect violations; alerts are sent to the Information Security Officer and HR. Confirmed violations result in immediate access revocation and

disciplinary actions per HR policy, up to termination.

# 6. Auditor Evidence Artefacts

- Quarterly AWS IAM access review reports
- AWS CloudTrail logs of access events
- Linear tickets for access provisioning, modification, and exception approvals
- Google Workspace admin console screenshots showing MFA enforcement
- MDM compliance scan reports for remote devices
- Minutes from quarterly access and exception review meetings
- HR termination tickets confirming access removal