Physical Security Policy

Appoint Compliance Program Manager delegated with responsibility for planning and implementing internal control environment

---

Executive Summary

Casper Studios maintains strict physical security controls for its on-site office and remote assets in alignment with SOC 2 Trust Services Criteria. This policy defines objectives, scope, and detailed controls with quarterly and annual review cycles. It assigns clear roles and responsibilities and enforces mandatory processes to mitigate risks of unauthorized access.

Objective

Establish and enforce physical security measures for Casper Studios' on-site office and remote home offices, as well as company-provided laptops and AWS infrastructure, to prevent unauthorized access, damage, or interference.

Scope and Applicability

This policy applies to all Casper Studios employees, contractors, and third-party personnel accessing company-provided laptops, AWS consoles, on-site office premises, or working from home. It covers physical access to offices, secure handling of keys/badges, device storage, and monitoring systems.

Controls

Access Rights Management

1. (P-001) Casper Studios Compliance Program Manager must maintain an up-to-date list of individuals authorized for physical access to secure office areas, reviewed quarterly.
2. (P-002) Approval for office badge provisioning must be documented in Google Workspace admin tickets and endorsed by the Information Security Officer.

3. (P-003) Visitor registration procedures must be performed through the front-desk ticketing system <> with pre-approval from the Facilities Manager.
4. (P-004) Continuous CCTV monitoring in office common areas must record 24/7 with 90-day retention and prompt alerts to security personnel.
5. (P-005) Access rights to secure areas must be reviewed and confirmed by the Facilities Manager and InfoSec quarterly.
6. (P-006) Physical access must be revoked within one business day of role change or termination, via deactivation of badges and remote console access.

Key and Badge Management

1. (P-007) All badges and master keys must be issued and tracked in the asset inventory system, reviewed annually by the Compliance Program Manager.
2. (P-008) Spare keys must be stored in a locked cabinet with access logs maintained by Facilities.
3. (P-009) Issued badges and keys must be returned or deactivated when no longer required, verified annually.

Monitoring and Surveillance

1. (P-010) CCTV and badge-entry logs must be correlated daily by the Security Analyst to detect anomalies.
2. (P-011) Physical security controls (doors, locks, barriers) must be inspected by Facilities quarterly and defects remediated within five business days.

Remote Workspace Security

1. (P-012) Remote employees must secure company-provided laptops in locked storage when unattended and enable screen lock after five minutes of inactivity.
2. (P-013) Lost or stolen devices must be reported within 24 hours to IT via ticketing system, and devices must be remotely wiped.

Segregation of Duties

1. (P-014) Duties among the Compliance Program Manager, Facilities Manager, and IT Security team must be segregated to prevent conflicts of interest and reviewed annually.

Exceptions Process

All physical security exception requests must be submitted via the ticketing system with business justification, compensating controls, and duration. The Information Security Officer and Facilities Manager shall review and approve exceptions, which are time-bound and reassessed prior to expiration quarterly.

Violations and Disciplinary Actions

Physical security violations must be reported immediately to the Information Security Officer. Confirmed violations will result in disciplinary action up to termination, and may include immediate access revocation and legal referral.

Auditor Evidence Artifacts

- Access review logs (quarterly reports)
- Badge/key issuance and return tickets
- CCTV footage retention records
- Inspection and remediation logs
- Exception approvals and review meeting minutes