

PAPER TIGER TECHNOLOGIES

Physical and Environmental Security Policy

1. Purpose

The purpose of this Physical and Environmental Security Policy is to describe the physical safeguards that would protect the fictional PaperTiger operating environment. Physical controls sit underneath the logical controls and protect the assets that host the service.

Logical security assumes the physical layer is intact: an attacker with physical access to a server can often bypass everything above it. This policy therefore covers facility access, visitor control, equipment protection, and environmental safeguards as the foundation the rest of the program stands on.

This policy is fictional and illustrative. It describes no real facility, room, or piece of equipment.

Digital controls mean little if the hardware can be walked away with, so the policy secures the physical layer as the foundation beneath everything else.

Physical security exists so the equipment and media that hold the demonstration are not reached through a door that was left open, and the policy makes the measures a reviewed set rather than an assumption.

2. Definitions

Term	Definition (illustrative)
Facility	The fictional building or room that houses the illustrated environment.
Secure area	A zone with restricted access, such as a server room.
Badge	The credential that grants and records physical access.
Visitor log	The record of visitors and their escort.
Equipment	The servers, network devices, and media that host the service.
Environmental control	The power and climate safeguards that protect equipment.
Removable media	Portable storage that holds data.
Camera	The video monitoring of sensitive areas.
Access control list	The roster of who may enter secure areas.
Physical incident	A breach or disruption at the physical layer.
Physical credential inventory	The tracked badges and keys.

Clean desk policy	The rule that sensitive material is secured when unattended.
Tailgating	Following an authorized person through a secured door.
Perimeter	The boundary of a facility, such as walls, doors, and entry points.
Restricted zone	An area where access is limited to people with a specific need and an active badge.
Visitor escort	The practice of a sponsor staying with a visitor for the full duration of access.
Media destruction	The irreversible destruction of storage media so data cannot be recovered.
Badge reader	The device that records physical access at an entry point.
Environmental monitoring	The sensing of temperature, power, and moisture around equipment.
Media register	The log of removable storage items and their status.
Mantrap	A two-door chamber that prevents tailgating.
Biometric access	Access granted by a biological factor such as a fingerprint.
Security perimeter	The physical boundary of the controlled area.
Surveillance	The monitoring of an area by camera or other means.
Intrusion detection	The detection of unauthorized physical entry.
Zone access review	The periodic re-confirmation of who may enter a zone.
Walkthrough	The physical inspection of zones and controls.
Clean desk	The practice of clearing sensitive material when not in use.
Access badge	The credential that grants physical entry.
Access log	The record of physical entry events.
Facility zone	A defined area with its own access rules.
Physical access control	The means that limit who can enter a zone.

3. Scope and Boundaries

This policy applies to fictional facilities, rooms, and equipment that would house the illustrated platform, and to the workforce and visitors who access them. It covers access, monitoring, and environmental safeguards.

It applies to every physical asset that hosts or stores demo data, so no asset is left physically unguarded.

Out of scope are real facilities and real equipment. This policy creates no real obligation.

Escalation for a physical security concern follows a fixed chain: an observation goes to the facility owner, then to the Information Security Lead when a controlled area is involved, and finally to the governance forum when the concern could affect availability.

The physical controls protect the provider's equipment and any media that holds customer data; a control that fails is corrected before it can be exploited.

The physical controls are reviewed at least annually, and a finding from the review is remediated before the next cycle.

The physical controls are documented and reviewed, and a missing or unlogged device is treated as an incident until it is accounted for.

The physical control inventory is reviewed with the other control inventories, so the security picture is complete.

The physical controls are fictional and reviewed at least annually.

A control that fails is corrected before it can be exploited, and a missing or unlogged device is treated as an incident until accounted for.

4. Roles and Responsibilities

Role	Illustrative responsibility
Physical Security Lead	Owns the policy and the access-control list.
Facility Manager	Maintains the physical environment and its controls.
Workforce Member	Follows access and badge rules.
Security Operations	Monitors cameras and responds to physical incidents.
Trust Center Coordinator	Maintains the fictional label on shared copies.

The following RACI is illustrative.

Illustrative RACI for physical security:

Activity	Physical Security Lead	Facility Manager	Security Ops
Grant access	A	R	I
Escort visitors	I	R	I
Monitor	I	C	R
Secure media	C	R	I
Review access	R	C	I

5. Policy Requirements and Controls

PTT-POL-024-C01. Control facility access

Access to secure areas is limited to authorized personnel, so the physical perimeter matches the logical boundary. An unguarded door undermines every access control above it. Entry is logged and the log is reviewed.

PTT-POL-024-C02. Use badges and visitor logs

Entry is recorded and visitors are escorted, so every person in a secure area is both authorized and accounted for. An unescorted visitor is a gap. A visitor is logged in and out.

PTT-POL-024-C03. Protect equipment

Server and network equipment is secured against unauthorized access, so the hardware that hosts the service cannot be physically tampered with. Equipment access is restricted and logged.

PTT-POL-024-C04. Monitor with cameras

Sensitive areas are under video monitoring in the demo, so a physical breach is detectable and reconstructable after the fact. The camera coverage is checked for gaps.

PTT-POL-024-C05. Manage environmental risks

Power and climate are maintained to protect equipment, so a heat or power event does not take the service down. Temperature, power, and moisture are managed.

PTT-POL-024-C06. Protect removable media

Media is stored and transported under controls, so a portable drive does not become an easy data exfiltration channel. Removable media is tracked and limited.

PTT-POL-024-C07. Review physical access

The access list is revalidated on a defined cadence, so former personnel do not retain physical access. The review is dated and a stale access is removed.

PTT-POL-024-C08. Escalate physical incidents

A physical breach is escalated through the incident process, so a door forced open is treated like any other security event. A physical incident is escalated.

PTT-POL-024-C09. Maintain a media inventory

Removable media is inventoried, so a missing drive is noticed rather than silently gone. The inventory is reconciled on a schedule.

PTT-POL-024-C10. Segregate secure areas

Server areas are physically separated from general office space, so casual access does not reach critical equipment. Secure areas are segregated from general space.

PTT-POL-024-C11. Maintain a key and badge inventory

Physical credentials are inventoried so a lost badge or key is noticed and revoked rather than lost in the noise. Keys and badges are inventoried.

PTT-POL-024-C12. Enforce clean desk and screen

A clean desk and locked screen policy reduces the chance that sensitive material is left visible to an unauthorized passerby. A clean desk and screen are enforced.

PTT-POL-024-C13. Protect against tailgating

Tailgating through a secured door is addressed by the access control design, so a single badge does not admit multiple people. Tailgating is prevented.

PTT-POL-024-C14. Document facility zones

The physical zones and their controls are documented, so the layout of protection is explicit. The zones are documented.

PTT-POL-024-C15. Review physical access logs

Physical access logs are reviewed for anomalies, so an unusual entry is noticed.

PTT-POL-024-C16. Coordinate with logical access

Physical and logical access are coordinated, so a person's physical and logical access are revoked together on departure.

PTT-POL-024-C17. Escort visitors

Visitors are logged and escorted, so an unfamiliar person is not left unsupervised in a sensitive area. A visitor is escorted for the full visit.

PTT-POL-024-C18. Protect against environmental hazards

Power, cooling, and fire detection are in place and tested, because a server room is one power failure away from an availability incident. A hazard is mitigated.

PTT-POL-024-C19. Secure media and hardware

Removable media and hardware awaiting disposal are secured against theft, because physical loss is a data loss. Media and hardware are secured.

PTT-POL-024-C20. Control the perimeter

Entry points are limited and locked, so physical access follows a defined route rather than an open door. The perimeter is limited and locked.

PTT-POL-024-C21. Destroy media securely

Storage media is destroyed or degaussed before disposal, so a discarded drive does not become a data leak. The destruction is recorded in the register.

PTT-POL-024-C22. Monitor the environment

Temperature, power, and moisture are monitored, so equipment-damaging conditions are caught before they cause an outage. The environment is monitored.

PTT-POL-024-C23. Keep an access audit trail

Badge reads and entry events are logged, so a physical access question can be answered from records rather than memory. Access events are logged.

PTT-POL-024-C24. Test environmental alarms

The temperature, power, and moisture alarms are tested on a schedule, so they are known to work before an actual failure. The alarms are tested.

PTT-POL-024-C25. Secure the equipment room

Server and network equipment lives in a restricted zone with its own access, so the systems are not left in an open shared space. The equipment room is restricted.

PTT-POL-024-C26. Keep a media register

Every removable storage item is logged with its owner and status, so a device can be accounted for at any point. The register is checked for completeness.

6. Operating Procedures

Grant physical access.

Access is assigned by role and recorded on the access-control list.

Escort visitors.

Visitors are logged and accompanied throughout their time in secure areas.

Monitor the environment.

Cameras and environmental sensors are reviewed on a cadence.

Secure media.

Removable media is locked and inventoried.

Review access.

The access list is revalidated on schedule.

Respond to physical incidents.

Breaches are escalated per the incident process.

Inventory physical credentials.

Badges and keys are inventoried and reconciled on a cadence, and lost items are revoked.

Review clean desk compliance.

A periodic walkthrough checks clean desk and locked screen compliance.

Document zones.

The facility zones and controls are documented.

Review access logs.

Physical access logs are reviewed on a cadence.

Issue facility access.

Access is granted based on role, recorded, and the entry credential is issued and logged.

Review physical access.

The access list is reviewed, stale entries are removed, and the change is recorded.

Escort a visitor.

The sponsor signs the visitor in, stays with them for the visit, and signs them out before they leave the controlled area.

Destroy a media item.

The custodian logs the item, destroys it by an approved method, and records the destruction in the media register.

Revoke a badge.

On separation or role change, the badge is disabled and the access record is updated the same day.

Test the environmental alarms.

The facility owner triggers each alarm on the schedule and records the result, then repairs any that fail.

Review zone access.

The facility owner compares the current access list to the actual staff, removes anyone who left, and records the review.

Test an environmental alarm.

The facility owner triggers each alarm on the schedule, records the result, and repairs any that fail.

Conduct a walkthrough.

The facility owner walks the zones, checks the controls, and records any gap.

Review surveillance.

The owner checks camera coverage for gaps and repairs any that fail.

Test a mantrap.

The owner confirms the two-door chamber prevents tailgating and records the result.

Segregate a secure area.

The facility owner limits the area to those with a need and an active badge.

Enforce clean desk.

The owner checks that sensitive material is cleared at the end of the day.

Protect against tailgating.

The facility owner confirms the entry controls prevent a person from following another through.

Review physical access logs.

The facility owner samples the access logs and flags any entry without a match.

7. Frequency and SLAs

Illustrative physical cadence:

Activity	Frequency (illustrative)
Access list review	Quarterly
Visitor log review	Monthly
Camera review	As needed

Media inventory	Quarterly
-----------------	-----------

8. Exceptions and Lifecycle

An exception permits a short-term visitor access or a temporary media transfer when the Physical Security Lead documents the reason and adds supervision.

Exceptions are reviewed quarterly, and a visitor or media exception that recurs is reviewed for a change to the process.

A visitor or media exception that recurs is reviewed for a change to the process, because a recurring exception indicates the standing control is not matching operational reality.

9. Records and Evidence

Record type	What it demonstrates (illustrative)
Access control list	The roster of authorized personnel.
Visitor logs	The recorded and escorted visitors.
Camera records	The monitoring output.
Media inventory	The tracked removable media.
Physical access reviews	The revalidated access.
Credential inventory	The tracked and reconciled badges and keys.
Clean desk walkthrough	The periodic compliance review.
Access lists	The authorized personnel and their access levels.
Entry logs	The recorded entry events.
Visitor log	The sign-in and sign-out record for each visit.
Media destruction register	The dated record of each destroyed item.
Badge inventory	The issued and revoked badges.
Camera coverage map	The documented camera placement.
Surveillance footage	The retained camera recordings.
Alarm test records	The dated tests of intrusion and environmental alarms.

10. Oversight and Metrics

- Access accuracy: 100 percent of access matches the list (illustrative).
- Visitor compliance: zero unescorted visitors.
- Media accountability: 100 percent of media inventoried.
- Incident response: physical incidents escalated within the window.
- Credential accountability: 100 percent of physical credentials inventoried.
- Access list accuracy: the share of listed personnel with current need trending to 100 percent.
- Visitor log completeness: the share of visits with a logged escort.

- Number of unescorted visitor events each month
- Time from separation to badge revocation
- Unescorted visitor events per month.
- Tailgating events observed per period.
- Badge inventory discrepancies.
- Alarm tests passed.
- Unauthorized entry events.

11. Appendix

Illustrative physical zones:

Zone	Control (illustrative)
Perimeter	Badge entry and visitor log
Server area	Restricted access and monitoring
Media storage	Locked and inventoried

12. Related Policy Dependencies

- Asset Management Policy (inventories the equipment to be protected)
- Incident Response Policy (escalates physical breaches)
- Business Continuity and Disaster Recovery Policy (assumes a physically protected primary)
- Security Access Policy (the logical access above the physical layer)
- Asset Management Policy (inventories the equipment this policy protects)

13. Review Cadence

The Physical Security Lead reviews this policy at least annually, after a change to the illustrated facility, and after a significant simulated physical incident.

Revision History

Version	Date	Change summary	Author
1.0	September 28, 2026	Original enterprise-depth fictional demo policy for controlled trust-center testing.	Paper Tiger Technologies

Document Control

Field	Value
Document ID	PTT-POL-024
Document Owner	Physical Security Lead
Status	Fictional demo artifact
Effective Date (illustrative)	September 28, 2026
Review Cadence	At least annually and after material fictional changes
Classification	Internal Demo
Approval	Illustrative governance approval only; no real adoption represented