PE.L2-3.10.2

Physical Protection

Monitor Facility

"Protect and monitor the physical facility and support infrastructure for organizational systems."

Objectives

[a]
The physical facility where organizational systems reside is protected.

[b]
The support infrastructure for organizational systems is protected.

[c]
The physical facility where organizational systems reside is monitored.

[d]
The support infrastructure for organizational systems is monitored.

Key Discussion Points

Protect + Monitor:
Two requirements: protect the facility (locks, controls) AND monitor it (cameras, guards, logs) — protection without monitoring leaves gaps.

Infrastructure Too:
Wiring closets, power lines, cabling, and network distribution — these are in scope. A locked server room with an unlocked wiring closet is incomplete.

How to Monitor:
Guards, cameras, sensor devices, and access log reviews all qualify — the method must be proportionate to the risk and the facility layout.

Review the Logs:
Access logs are only useful if they are reviewed — generating logs without reviewing them does not satisfy the monitoring objective.

Assessment Methods

EXAMINE

Physical and environmental protection policy; procedures addressing physical access monitoring; system security plan; physical access logs or records; physical access monitoring records; physical access log reviews.

INTERVIEW

Personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for monitoring physical access; mechanisms supporting or implementing physical access monitoring; mechanisms for review of physical access logs.

PE.L2-3.10.2

PHYSICAL PROTECTION — Monitor Facility

Plain English

What this control is really saying:

Locking the door isn't enough if nobody watches who comes and goes. This control requires both protection of the facility and its infrastructure AND monitoring — cameras, guards, sensors, or access logs that create a record of physical access events and enable detection of unauthorized entry.

How it is used:

- Security cameras cover all entrances, exits, and the server room — footage is retained for 90 days and reviewed after any physical security incident.
- The wiring closet is locked at all times — network cabling and power infrastructure are protected against tampering and accidental damage.
- Physical access logs from badge readers are reviewed monthly — anomalies (after-hours access, unusual frequency) are reported to the security officer.
- An alarm system monitors the facility after hours — alerts trigger a notification to the IT admin and a security response if the facility is accessed outside business hours.

Real World Example

The Scenario

Acme Defense has no security cameras in the facility. The server room has a lock but the wiring closet does not. Physical access badge logs are generated by the access control system but the IT admin has never reviewed them.

What the assessor finds

A review of six months of badge logs reveals 14 after-hours entries to the server room by a badge that was supposed to be deactivated. The wiring closet shows signs of cable manipulation. Without cameras or log reviews, both events went undetected for months.

SPRS Score Impact

3.10.2 carries a point value of 1. Physical monitoring creates the audit trail that enables detection of unauthorized access — without it, physical breaches are invisible until their consequences appear in digital logs.

What Good Looks Like

Security cameras at entrances and server room, footage retained per policy, wiring closet and infrastructure locked, physical access logs reviewed regularly, after-hours monitoring and alerting, infrastructure protected against tampering.

Common Gaps

What assessors actually find in the field:

✗ **No security cameras**

There are no cameras at facility entrances or in the server room — physical access events are not recorded.

✗ **Wiring closet unlocked**

The network wiring closet is accessible to any staff member — cabling can be tampered with or tapped without detection.

✗ **Access logs not reviewed**

Badge access logs are generated but never reviewed — unauthorized entries could go undetected indefinitely.

✗ **No after-hours monitoring**

The facility has no alarm system or monitoring after business hours — nighttime physical access is completely undetected.

✗ **Infrastructure unprotected**

Power and network cabling runs through unsecured areas — accidental damage and physical tampering are undetected risks.