PE.L2-3.10.5

Physical Protection

Manage Physical Access [CUI Data]

"Control and manage physical access devices."

Objectives

[a]
Physical access devices are identified.

[b]
Physical access devices are controlled.

[c]
Physical access devices are managed.

Key Discussion Points

Device Types:
Keys, locks, combinations, and card readers — all physical access devices must be identified, controlled, and managed.

Inventory First:
You cannot control what you haven't identified — maintaining a list of all devices with assigned owners is the foundation of this control.

Manage Changes:
When personnel leave or change roles, devices must be recovered or deactivated — an unrevoked badge is as risky as an active account.

Combinations Too:
Keypad combinations are often forgotten — they must be changed when personnel who know them leave or when the combination may be compromised.

Assessment Methods

EXAMINE

Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs; inventory records of physical access control devices; system entry and exit points; physical access control devices.

INTERVIEW

Personnel with physical access control responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices.

PE.L2-3.10.5

PHYSICAL PROTECTION — Manage Physical Access [CUI Data]

Plain English

What this control is really saying:

A key that isn't tracked is a risk you don't know about. This control requires that every physical access device — keys, badges, key cards, lock combinations — is inventoried, controlled (limited to authorized people), and managed (revoked, changed, or updated when personnel or circumstances change).

How it is used:

- An inventory is maintained for all keys and badges — each item has a serial number, assigned individual, issuance date, and access areas documented.
- Badge access profiles are updated within two hours when an employee changes roles or leaves — old access is revoked and new access matched to the new role is provisioned.
- Lock combinations are changed annually and whenever personnel with that combination leave the organization — changes are documented in the physical access records.
- All physical access devices are stored securely when not assigned — spare keys are in a locked safe accessible only to the facility manager.

Real World Example

The Scenario

Acme Defense issues physical keys to the server room. There is no inventory of who has been issued keys. When employees leave, HR retrieves their building badge but does not specifically ask about server room keys.

What the assessor finds

A former engineer who left the company eight months ago still has a server room key. The key was never returned because nobody tracked who had been issued one. The badge access was revoked but the physical key remains unaccounted for.

SPRS Score Impact

3.10.5 carries a point value of 1. Untracked physical access devices are invisible risks — an unreturned key or unrevoked badge combination allows persistent facility access that logical security controls cannot detect.

What Good Looks Like

Inventory of all physical access devices maintained, devices limited to authorized individuals, devices revoked at termination or role change, combinations changed on schedule and at personnel departure, spare devices secured, records retained as evidence.

Common Gaps

What assessors actually find in the field:

✗ **No device inventory**

No list of keys, badges, or access devices exists — the organization cannot account for who has what or how many devices are in circulation.

✗ **Keys not returned at exit**

Employees return laptops at termination but physical keys are not tracked — former employees may retain facility access.

✗ **Combinations not changed**

A keypad combination in use since 2019 has never been changed — multiple former employees know it.

✗ **Devices accessible to all**

Spare key cards are kept in an unlocked desk drawer — any employee can issue themselves additional access without authorization.

✗ **Badge profiles not updated**

A transferred employee's old access profile was never updated — they retain physical access to a project area they no longer support.