PE.L2-3.10.1

Physical Protection

Limit Physical Access [CUI Data]

"Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals."

Objectives

[a]
Authorized individuals allowed physical access are identified.

[b]
Physical access to organizational systems is limited to authorized individuals.

[c]
Physical access to equipment is limited to authorized individuals.

[d]
Physical access to operating environments is limited to authorized individuals.

Key Discussion Points

Access List Required:
Authorized individuals must be identified — a maintained, reviewed list is the evidence base. 'Everyone on the team' is not sufficient.

All Three Targets:
Systems, equipment, AND operating environments — all three must be controlled. Equipment includes printers, scanners, and copiers.

Visitors Need Escorts:
Visitors are not authorized individuals — they require escorting in any area where CUI systems or equipment are located.

Output Device Placement:
Printers in common areas expose CUI — output devices must be in access-controlled locations, not shared hallways or open offices.

Assessment Methods

EXAMINE

Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records.

INTERVIEW

Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities.

TEST

Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations.

PE.L2-3.10.1

PHYSICAL PROTECTION — Limit Physical Access [CUI Data]

Plain English

What this control is really saying:

Anyone who can walk into the room where your CUI systems live can touch them, reboot them, plug in a USB drive, or remove a hard drive. This control requires that physical access to systems, equipment, and the areas that contain them is limited to a defined list of authorized individuals with appropriate credentials.

How it is used:

- The server room requires a badge plus PIN — a maintained access list defines which employees are authorized, and the list is reviewed quarterly.
- Visitors to the CUI workspace are escorted at all times — unescorted visitors are not permitted in areas where CUI systems or equipment are located.
- Printers and scanners in the CUI environment are in a locked room accessible only to authorized staff — they are not in common areas.
- Physical access credentials are revoked within two hours when an employee's role changes or they leave the company.

Real World Example

The Scenario

Acme Defense's engineering office is an open-plan workspace. Anyone with a building badge — including IT, HR, and facilities staff — can walk into the area where CUI workstations are located. The server room is locked but the office itself is not.

What the assessor finds

A facilities technician who came to fix an HVAC unit in the CUI workspace was left unescorted. He photographed engineering drawings displayed on a monitor. No access list governs who enters the workspace and no escort requirement exists.

SPRS Score Impact

3.10.1 carries a point value of 1. Physical access controls are foundational — a threat actor with physical access to a CUI system can bypass virtually all logical security controls.

What Good Looks Like

Authorized access list maintained and reviewed, CUI work areas and equipment rooms physically restricted, badge and PIN or equivalent controls at entry, visitors escorted, printers in access-controlled locations, physical credentials revoked at termination.

Common Gaps

What assessors actually find in the field:

✗ **Unlocked server room**

The server room door is unlocked during business hours — any employee can walk in without authorization.

✗ **No access list maintained**

Multiple staff have badge access to the CUI workspace but no current authorized access list is maintained.

✗ **Visitors unescorted**

Vendors and guests enter the CUI work area without an escort — they have unsupervised proximity to systems and equipment.

✗ **Printers in common areas**

CUI prints to a printer in a shared hallway — any passerby can see or take documents from the output tray.

✗ **Access not revoked on exit**

A former employee's badge still grants access to the CUI facility — physical credentials are not revoked at termination.