PE.L2-3.10.4

Physical Protection

Physical Access Logs [CUI Data]

"Maintain audit logs of physical access."

Objectives

[a]
Audit logs of physical access are maintained.

Key Discussion Points

Flexible Format:
Paper sign-in sheets, badge reader logs, or a combination — the guide explicitly allows procedural, automated, or mixed approaches.

Retain the Records:
Logs must be retained for an organization-defined period — generating logs but overwriting them defeats the purpose of the control.

Both Access Types:
Employee access AND visitor access both need to be logged — visitor-only logs with no employee records are incomplete.

Covers Entry Points:
Facility access points, server room doors, CUI workspace entrances — any physical access point to systems or components is in scope.

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.L2-3.10.4

PHYSICAL PROTECTION — Physical Access Logs [CUI Data]

Plain English

What this control is really saying:

If someone broke into your facility, would you know who was there and when? This control requires that a record be kept of who enters and exits areas where CUI systems are located — paper sign-in sheets, badge reader logs, or any other form of documented access trail that is retained per policy.

How it is used:

- Badge reader logs from the server room and CUI workspace are retained for one year — entry and exit timestamps are captured electronically for every access event.
- Visitor sign-in sheets are maintained at reception — name, host, entry time, and exit time are recorded and retained in a locked filing cabinet per the retention policy.
- Physical access logs are reviewed monthly by the security officer — after-hours entries, multiple entries in a short window, and deactivated badge activity are flagged.
- The SSP defines the log retention period and the review frequency — log retention is treated as evidence documentation for assessment purposes.

Real World Example

The Scenario

Acme Defense has badge readers at the server room and CUI workspace. The badge reader system generates log files automatically. The IT admin has never configured log retention — logs older than 30 days are automatically overwritten by the system.

What the assessor finds

A physical security review requires six months of access logs. Only 28 days of logs are available. A suspected unauthorized entry event from 45 days ago cannot be investigated — the relevant logs no longer exist. No retention policy was ever defined.

SPRS Score Impact

3.10.4 carries a point value of 1. Physical access logs are the audit trail for the facility — without them, unauthorized entry events cannot be investigated, attributed, or defended against.

What Good Looks Like

Physical access logs maintained for employees and visitors, retention period defined in SSP, logs reviewed on defined schedule, badge reader or sign-in sheet at all CUI area entry points, logs available as evidence for assessors.

Common Gaps

What assessors actually find in the field:

✗ No physical access log

There is no sign-in sheet or badge reader — no record exists of who has entered facility areas containing CUI systems.

✗ Logs not retained

Sign-in sheets are discarded after the week — no retention policy exists and historical access records are unavailable.

✗ Logs not reviewed

Badge reader logs exist but are never reviewed — unauthorized access events go undetected until a separate incident surfaces.

✗ Visitors not logged

Employee access is logged via badge readers but visitor sign-ins are informal — visitor access history is not retained.

✗ No retention period defined

Logs are kept 'for a while' but no specific retention period is documented — the organization cannot demonstrate consistent compliance.