PE.L2-3.10.6

Physical Protection

Alternative Work Sites

"Enforce safeguarding measures for CUI at alternate work sites."

Objectives

[a]

Safeguarding measures for CUI are defined for alternate work sites.

[b]

Safeguarding measures for CUI are enforced for alternate work sites.

Key Discussion Points

Define AND Enforce:
Both objectives must be met — a telework policy that nobody follows satisfies [a] but fails [b]. Verification of compliance is required.

Includes Residences:
Private homes are explicitly named as alternate work sites — the same safeguard rigor applies whether the alternate site is a government facility or a home office.

Physical + Electronic:
Safeguards include both physical (locked file drawers, private workspace) and electronic (encryption, VPN, MFA) protections.

Laptop Risk:
A lost or stolen laptop with unencrypted CUI is a reportable breach — full-disk encryption is the primary control for mobile work.

Assessment Methods

EXAMINE

Physical and environmental protection policy; procedures addressing alternate work sites; system security plan; list of safeguards required for alternate work sites; assessments of safeguards at alternate work sites.

INTERVIEW

Personnel approving use of alternate work sites; personnel using alternate work sites; personnel assessing controls at alternate work sites; personnel with information security responsibilities.

TEST

Organizational processes for security at alternate work sites; safeguards employed at alternate work sites; means of communications between alternate site personnel and security.

PE.L2-3.10.6

PHYSICAL PROTECTION — Alternative Work Sites

Plain English

What this control is really saying:

An employee working from home with CUI on their laptop is outside every physical and logical control in your facility. This control requires that you define what safeguards apply when CUI is worked with at home, on the road, or at any non-company location — and then make sure those safeguards are actually in place.

How it is used:

- A telework policy defines the required safeguards for working with CUI at home: full-disk encryption on laptops, VPN with MFA, no CUI on personal devices.
- All remote-worker laptops have full-disk encryption enabled — if a laptop is lost or stolen while traveling, CUI cannot be accessed without the decryption credentials.
- Remote access to CUI systems requires VPN with MFA and split tunneling is disabled — traffic cannot bypass the corporate security stack from remote locations.
- Remote workers may not print or store CUI locally without approval — CUI at alternate sites is handled per the telework policy and reviewed annually.

Real World Example

The Scenario

Acme Defense project managers work from home several days a week and access CUI design files via a shared drive. They use their personal laptops. There is no company telework policy and no specific guidance on how to protect CUI when working remotely.

What the assessor finds

One project manager's personal laptop is unencrypted, has no AV software, and is shared with his teenager. CUI design files are stored in the Downloads folder. There is no policy defining safeguards for alternate work sites and no mechanism to enforce any baseline.

SPRS Score Impact

3.10.6 carries a point value of 1. Remote work dramatically expands the CUI exposure surface — a single unencrypted personal laptop with CUI is an uncontrolled risk that no facility control can address.

What Good Looks Like

Telework policy defines CUI safeguards for alternate sites, full-disk encryption on all remote-worker devices, VPN with MFA for remote access, personal devices prohibited for CUI, safeguard compliance assessed periodically, policy documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ No telework policy

No policy defines the safeguards required when working with CUI at home — remote workers make ad hoc decisions about CUI protection.

✗ CUI on personal devices

Employees use personal laptops for remote work — personal devices have no disk encryption, no MDM, and no security baseline.

✗ No VPN required remotely

Remote workers access CUI systems directly over the internet without VPN — traffic is unencrypted and unmonitored outside the perimeter.

✗ Safeguards not verified

A telework policy exists but compliance is never checked — remote workers may not actually have the required safeguards in place.

✗ CUI printed at home

Employees print CUI documents at home on personal printers — no policy addresses the physical safeguarding of printed CUI at alternate sites.