PS.L2-3.9.2

Personnel Security

Personnel Actions

"Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers."

Objectives

[a]
A policy and/or process for terminating system access and any credentials coincident with personnel actions is established.

[b]
System access and credentials are terminated consistent with personnel actions such as termination or transfer.

[c]
The system is protected during and after personnel transfer actions.

Key Discussion Points

Covers Both Actions:
Terminations AND transfers both trigger this control — access from a prior role must be revoked even when the person stays at the company.

Timing Is Critical:
For terminations for cause, access should be disabled before or at the moment of notification — not hours or days later.

Exit Interviews:
Exit interviews remind departing employees of their ongoing CUI obligations and nondisclosure agreements — documentation of the interview is evidence.

Equipment Return:
Hardware tokens, badges, laptops, and storage devices must be returned — a device with CUI in the hands of a former employee is an exposure.

Assessment Methods

EXAMINE

Personnel security policy; procedures addressing personnel transfer and termination; records of personnel transfer and termination actions; list of system accounts; records of terminated or revoked credentials; records of exit interviews.

INTERVIEW

Personnel with personnel security responsibilities; personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities.

TEST

Organizational processes for personnel transfer and termination; mechanisms for disabling system access and revoking authenticators.

PS.L2-3.9.2

PERSONNEL SECURITY — Personnel Actions

Plain English

What this control is really saying:

A terminated employee whose access isn't revoked is an insider threat with a grudge and a key. This control requires a defined process for terminations AND transfers: revoke access, recover equipment, change credentials, and conduct an exit interview reminding them of their CUI obligations.

How it is used:

- HR notifies IT on the same day a termination is confirmed — IT disables all system accounts, revokes MFA tokens, and removes physical access within two hours.
- Exit interviews are conducted with all departing employees covering CUI obligations, nondisclosure agreements, and equipment return.
- When an employee transfers to a new role, access from the prior role is revoked on the effective date and new access matching the new role is provisioned.
- A termination checklist is completed for every departure: accounts disabled, equipment returned, badges revoked, access records updated.

Real World Example

The Scenario

An Acme Defense engineer is terminated for cause on a Friday afternoon. HR sends an email to IT about the termination. IT does not check email until Monday morning. The former employee's accounts remain active all weekend.

What the assessor finds

The former engineer logged into the CUI file server Saturday night and downloaded 2,400 design files to a personal cloud storage account. Active Directory shows the access occurred 14 hours after termination. There is no same-day revocation procedure.

SPRS Score Impact

3.9.2 carries a point value of 1. Terminated employees with active accounts represent one of the highest-probability insider threat scenarios — access revocation timing is a frequent audit finding and a direct breach vector.

What Good Looks Like

Termination procedure documented and enforced, same-day account revocation for all terminations, terminations for cause handled immediately, transfer access reviewed on effective date, exit interviews conducted, equipment recovered, records retained.

Common Gaps

What assessors actually find in the field:

✗ **Accounts not disabled on exit**

Former employees' accounts remain active for days or weeks after termination — they retain CUI access after leaving.

✗ **No termination procedure**

There is no defined offboarding checklist — access revocation depends on whoever the departing employee worked with.

✗ **Transfer access not adjusted**

Employees who transfer keep all prior-role access — over time individuals accumulate CUI access far beyond their current role.

✗ **No exit interview**

Departing employees are not reminded of CUI obligations — they leave unaware that their nondisclosure obligations persist.

✗ **Equipment not recovered**

A terminated employee kept their company laptop — it contains CUI and there is no procedure for equipment recovery.