IA.L2-3.5.6

Identification & Authentication

Identifier Handling

"Disable identifiers after a defined period of inactivity."

Objectives

[a]

A period of inactivity after which an identifier is disabled is defined.

[b]

Identifiers are disabled after the defined period of inactivity.

Key Discussion Points

Define the Threshold:
The inactivity period must be formally defined — 30, 45, or 90 days are common — and documented in policy or the SSP.

Ghost Accounts:
Former employees, contractors, or vendors with accounts that were never disabled are the most common finding for this control.

Disable, Not Delete:
Disabling preserves the account for investigation — deleting it destroys the audit trail. Disable first, archive or delete later.

Automated Preferred:
A script or AD policy that auto-disables after N days of inactivity is more reliable than manual periodic reviews.

Assessment Methods

EXAMINE

Identification and authentication policy; procedures addressing identifier management and account management; system security plan; system design documentation; system configuration settings; list of system accounts; list of identifiers generated from physical access control devices.

INTERVIEW

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

TEST

Mechanisms supporting or implementing identifier management.

IA.L2-3.5.6

IDENTIFICATION & AUTHENTICATION — Identifier Handling

Plain English

What this control is really saying:

An account that nobody has logged into in 90 days is a ghost — and ghosts are dangerous. A former employee, a vendor from a completed project, or a service account that was never cleaned up can all become entry points for attackers. This control requires that you define when 'inactive' becomes 'disabled' and then actually do it.

How it is used:

- Policy defines a 45-day inactivity threshold — accounts with no logon activity in 45 days are automatically disabled via Active Directory.
- A PowerShell script runs nightly and generates a report of accounts approaching the 45-day threshold — supervisors are notified before automatic disablement.
- Disabled accounts are retained for 90 days before removal — preserved for potential forensic investigation.
- Physical access control identifiers (key fob IDs) are reviewed quarterly — inactive fob assignments are deactivated on the same 45-day schedule.

Real World Example

The Scenario

Acme Defense has 12 active user accounts in Active Directory. The IT admin has not reviewed the account list in 8 months. Two employees left the company 5 and 7 months ago respectively. A subcontractor account was created 11 months ago for a 3-month project.

What the assessor finds

All three accounts are still enabled with no activity in months. No inactivity policy is defined. The subcontractor account has domain user rights and was last used 8 months ago. None of these accounts were flagged or disabled.

SPRS Score Impact

3.5.6 carries a point value of 3. Stale accounts belonging to departed employees and forgotten vendors are among the most commonly exploited entry points — attackers can use them for months before anyone notices.

What Good Looks Like

Inactivity period defined in policy, automated AD check disables accounts after threshold, former employee accounts disabled at termination, vendor accounts tied to project end dates, physical access credentials on same review cycle, disabled accounts retained for investigation.

Common Gaps

What assessors actually find in the field:

✗ No inactivity period defined

The organization has never defined what 'inactive' means — no threshold triggers account review or disablement.

✗ Former employee accounts active

Three departed employees still have enabled Active Directory accounts — none have been disabled since termination.

✗ Vendor accounts still active

An MSP account created for a completed project 14 months ago is still active and enabled in the directory.

✗ Manual review only

Account review happens 'when we remember' — no scheduled review, no automated check, no consistent enforcement.

✗ Physical access not included

Door fob assignments are never reviewed — several former employees still have active physical access credentials.