AC.L2-3.1.10

Access Control

Session Lock

"Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity."

Objectives

[a]
The period of inactivity after which the system initiates a session lock is defined.

[b]
Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.

[c]
Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.

Key Discussion Points

Define the Period:
[a] requires specifying the inactivity period — 'a few minutes' is not sufficient. A specific number of minutes must be documented in policy and configured in the system.

Lock vs. Logout:
Session lock is for temporary absence. v2.13 notes it is not an acceptable substitute for logout when policy requires users to log off at end of day.

Pattern-Hiding Required:
[c] adds specificity beyond just locking — the lock display must conceal what was previously visible. A transparent screensaver or one that shows the desktop background fails [c].

Re-Auth to Unlock:
A lock screen that dismisses without credentials does not prevent access — [b] requires that the lock actually prevent system access and data viewing until credentials are re-entered.

Assessment Methods

EXAMINE

Access control policy; procedures addressing session lock; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; system security plan.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developers.

TEST

Mechanisms implementing access control policy for session lock.

AC.L2-3.1.10

ACCESS CONTROL — Session Lock

Plain English

What this control is really saying:

An unattended workstation with CUI visible on screen is a physical security failure. Session lock automatically blanks the screen after a defined inactivity period and requires re-authentication before access is restored. The lock screen must use a pattern-hiding display — not a transparent or decorative screensaver — so that previously visible information cannot be read by someone walking past.

How it is used:

- Group Policy configures session lock at 15 minutes of inactivity across all CUI workstations and laptops — the inactivity threshold is documented in the SSP.
- The lock screen uses the Windows default lock pattern that fully conceals the desktop — no transparent or partially visible screensaver is used.
- Re-authentication is required to unlock — pressing a key or moving the mouse dismisses the lock screen only after valid credentials are entered.
- Laptops also lock automatically on lid close — the lock-on-lid-close policy is enforced by GPO.

Real World Example

The Scenario

Acme Defense engineers regularly display CUI engineering drawings on their workstations. The office has an open floor plan with occasional visitors. Engineers leave workstations unattended during lunch breaks and meetings — sometimes for 30 to 60 minutes.

What the assessor finds

No session lock policy is configured on any workstation. Engineers leave CUI drawings visible on screen while away at lunch. Three workstations have decorative screensavers that activate after 60 minutes — but the screensavers display the company logo over a semi-transparent desktop, leaving content partially visible.

SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

Inactivity period defined and documented in SSP, GPO-enforced session lock at 15 minutes or less on all CUI devices, pattern-hiding display conceals all previous content, re-authentication required to unlock, laptops lock on lid close.

Common Gaps

What assessors actually find in the field:

✗ **No session lock configured**

Workstations never lock regardless of inactivity — CUI remains visible on unattended screens indefinitely.

✗ **Decorative screensaver only**

A decorative screensaver activates but it is semi-transparent or shows the desktop — previously visible information can still be read.

✗ **Inactivity timeout too long**

Session lock is configured but set to 60 minutes — CUI is visible on unattended workstations for a full hour before locking.

✗ **Inconsistent application**

Desktops lock at 15 minutes but laptops and remote desktop sessions have no inactivity timeout configured.

✗ **No re-authentication on unlock**

A lock screen activates but pressing any key bypasses it without requiring credentials — access to the session is not actually prevented.