AC.L2-3.1.1

Access Control

Authorized Access Control [CUI Data]

"Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)."

Objectives

[a]
Authorized users of the system are identified.

[b]
Processes acting on behalf of authorized users are identified.

[c]
Devices (and other systems) authorized to connect to the system are identified.

[d]
System access is limited to authorized users.

[e]
System access is limited to processes acting on behalf of authorized users.

[f]
System access is limited to authorized devices (including other systems).

Key Discussion Points

Users:
Every person must have a unique named account — shared logins fail [a] and [d] and make individual accountability impossible.

Processes:
Service accounts and automated scripts are 'processes acting on behalf of authorized users' — each must be documented and authorized.

Devices:
Printers, laptops, and other systems must be on an authorized device list — unmanaged devices are blocked even with valid credentials.

Deny by Default:
Authorization is explicit, not assumed — if a user, process, or device is not on the list, access is denied.

Assessment Methods

EXAMINE

Access control policy; procedures addressing account management; system security plan; system configuration settings; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts; access authorization records; account management compliance reviews; list of devices and systems authorized to connect to organizational systems.

INTERVIEW

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

TEST

Organizational processes for managing system accounts; mechanisms for implementing account management.

AC.L2-3.1.1

ACCESS CONTROL — Authorized Access Control [CUI Data]

Plain English

What this control is really saying:

Only the right people, on the right devices, running the right processes should be able to get into your system. This control covers all three categories: named users with accounts, processes and service accounts acting on behalf of those users, and specific devices and systems that are authorized to connect. Everything else is denied by default.

How it is used:

- IT maintains a list of all authorized users in Active Directory — every person with access has a named individual account tied to their identity.
- Service accounts for automated backups and software agents are documented in the SSP with the name of the person who authorized each one.
- Only domain-joined and MDM-enrolled devices appear on the authorized device list — personal or unmanaged devices are blocked at the network boundary.
- When an employee transfers or terminates, their account is disabled the same day and the authorized user list is updated immediately.

Real World Example

The Scenario

Acme Defense is a 45-person machine shop manufacturing precision components for a DoD prime. They handle CUI engineering drawings and have a Windows Server with Active Directory, a handful of engineering workstations, and CNC machines on the shop floor.

What the assessor finds

Three machinists share a 'shop_user' login to access CNC software. A former engineer terminated eight months ago still has an active AD account with access to the CUI file share. Two laptops on the shop floor are personal devices with no domain join or authorization record.

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

Named accounts for every user, no shared logins, terminated employee accounts disabled same day, service accounts documented in SSP, personal devices blocked, authorized device list maintained and reviewed.

Common Gaps

What assessors actually find in the field:

✗ **Shared accounts**

A single 'shop_user' login shared by multiple machinists — no individual accountability and no way to know who accessed CUI.

✗ **Stale accounts**

Former employees still have active accounts in Active Directory — sometimes months or years after termination.

✗ **No device control**

Personal laptops connect to the CUI network with no MDM enrollment, no domain join, and no authorization record.

✗ **Undocumented service accounts**

Scripts and automated processes run under credentials that nobody has reviewed — sometimes with administrator rights.

✗ **Policy without technical controls**

An access control policy exists on paper but no system configuration enforces it — anyone who knows a password can connect.