AC.L2-3.1.5

Access Control

Least Privilege

"Employ the principle of least privilege, including for specific security functions and privileged accounts."

Objectives

[a]
Privileged accounts are identified.

[b]
Access to privileged accounts is authorized in accordance with the principle of least privilege.

[c]
Security functions are identified.

[d]
Access to security functions is authorized in accordance with the principle of least privilege.

Key Discussion Points

Users and Processes:
Least privilege applies to both — standard users get minimum necessary access, and service accounts and automated processes must be scoped equally tightly.

Security Functions:
[c] and [d] require identifying specific security functions (account management, audit config, access control settings) and restricting who can perform them.

Privileged Inventory:
[a] requires identifying privileged accounts — without a documented list of who holds elevated access and why, the principle cannot be evaluated or enforced.

Separate Daily Account:
Admins should use standard accounts for routine work and privileged accounts only for admin tasks — using admin credentials for email and browsing is a critical exposure.

Assessment Methods

EXAMINE

Access control policy; procedures addressing least privilege; system security plan; system configuration settings; list of active system accounts with associated individuals; list of security functions and security-relevant information for which access is explicitly authorized; list of system-generated privileged accounts; list of system administration personnel; access authorization records; account management compliance reviews.

INTERVIEW

Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities; personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.

TEST

Organizational processes for managing system accounts; mechanisms for implementing account management; mechanisms implementing least privilege functions; mechanisms prohibiting privileged access to the system.

AC.L2-3.1.5

ACCESS CONTROL — Least Privilege

Plain English

What this control is really saying:

Give every user exactly what they need to do their job — and nothing more. Least privilege applies to everyone: standard users get standard access, IT admins get admin access only for admin tasks, and security functions like configuring access controls or setting audit parameters are restricted to those with a specific, documented need.

How it is used:

- Privileged accounts are documented in the SSP — each one is listed with the individual assigned to it and the business justification for the elevated access.
- IT administrators have two accounts: a standard account for daily work and a separate privileged account used only when performing administrative tasks.
- Service accounts for applications are configured with only the minimum permissions needed for that application — not domain admin rights.
- Privileged account assignments are reviewed quarterly — access is revoked when the business justification no longer applies.

Real World Example

The Scenario

Acme Defense has three IT staff. All three were given domain administrator accounts when hired. They use these accounts for all daily tasks including email, web browsing, and routine file access. One contractor from a project two years ago still retains domain admin credentials.

What the assessor finds

All three staff browse personal websites and check personal email with full domain administrator accounts. A compromised browser session would immediately yield full domain admin access. The contractor's credentials have never been reviewed. No privileged account inventory exists in the SSP.

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

Privileged accounts inventoried in SSP with business justification, separate standard and admin accounts for all IT staff, admin accounts used only for admin tasks, service accounts scoped to minimum necessary, privileged access reviewed quarterly, contractor access time-limited.

Common Gaps

What assessors actually find in the field:

✗ **Everyone is admin**

All IT staff have full domain administrator rights regardless of actual job function — no one has been assessed against the principle of least privilege.

✗ **No separate admin accounts**

Administrators use their privileged accounts as their primary daily-use account for email and browsing — a compromised session immediately yields admin access.

✗ **Service account over-privilege**

Application service accounts run with domain admin rights 'just in case' — no review has ever scoped them to minimum necessary permissions.

✗ **Privileged accounts not inventoried**

No list of privileged accounts exists — [a] is not met and the extent of over-privilege cannot be assessed.

✗ **Never reviewed**

Privileged account assignments have never been reviewed since initial creation — former employees and former contractors may still hold elevated access.