AC.L2-3.1.6

Access Control

Non-Privileged Account Use

"Use non-privileged accounts or roles when accessing nonsecurity functions."

Objectives

[a]

Nonsecurity functions are identified.

[b]

Users are required to use non-privileged accounts or roles when accessing nonsecurity functions.

Key Discussion Points

The Behavioral Piece:
3.1.5 requires having separate accounts. 3.1.6 requires actually using the right one — an admin who browses the web with a domain admin account fails 3.1.6 regardless of 3.1.5.

Define Nonsecurity First:
[a] requires identifying nonsecurity functions — email, file access, web browsing, document editing — before [b] can be evaluated or enforced.

Written Policy Required:
The requirement must be stated explicitly — a verbal expectation that admins should use standard accounts does not satisfy [b].

Risk Is Asymmetric:
A phishing link clicked in a standard user session is recoverable. The same click in a domain admin session may result in full enterprise compromise.

Assessment Methods

EXAMINE

Access control policy; procedures addressing least privilege; system security plan; list of system-generated security functions assigned to system accounts or roles; system configuration settings; system audit logs and records.

INTERVIEW

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

TEST

Mechanisms implementing least privilege functions.

AC.L2-3.1.6

ACCESS CONTROL — Non-Privileged Account Use

Plain English

What this control is really saying:

3.1.6 is the behavioral complement to 3.1.5 — not just having separate accounts, but actually using the right one for the right task. An admin who checks email and browses the web with their privileged account is operating outside this control every minute of every day. Nonsecurity functions must be done with non-privileged accounts, full stop.

How it is used:

- Administrators have two accounts — standard for email, browsing, and file access; privileged for system configuration, account management, and security functions only.
- A written policy defines which tasks constitute nonsecurity functions and requires non-privileged account use for those tasks — the policy is communicated to all IT staff.
- Audit logs record which account type was used for each administrative action — privileged account use outside defined admin tasks triggers a review.
- Group policy prevents privileged accounts from being used for web browsing and email client access on designated admin workstations.

Real World Example

The Scenario

Acme Defense has one IT administrator. He was given a domain administrator account on day one and has used it exclusively for all tasks — reading company announcements, browsing vendor websites, checking personal email, and performing system administration.

What the assessor finds

The IT admin has never used a standard user account. His privileged account is used for every task without exception. If his session were compromised while browsing, the attacker would immediately have full domain admin access. No policy exists requiring account switching. No standard account has ever been created for him.

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

Nonsecurity functions documented, written policy requires non-privileged account use for all non-admin tasks, all IT staff have separate standard accounts used for routine work, privileged accounts used only for admin tasks, audit logs capture account type used for each action.

Common Gaps

What assessors actually find in the field:

✗ Admin account for everything

The IT administrator uses their domain admin account as their only account — email, web browsing, and routine tasks all performed with privileged credentials.

✗ No nonsecurity functions defined

The organization has never documented what constitutes nonsecurity functions — [a] is not met and [b] cannot be enforced without that baseline.

✗ No policy requiring use switch

No written policy requires administrators to switch to non-privileged accounts for routine tasks — the expectation exists verbally but is not enforced.

✗ No technical enforcement

Nothing technically prevents a privileged account from being used for email or web browsing — the restriction exists on paper only.

✗ No audit distinction

Audit logs do not distinguish between admin-account and standard-account activity — privileged use for nonsecurity tasks is invisible.