Objectives

[a]

An immediate change to a permanent password is required when a temporary password is used for system logon.

IA.L2-3.5.9

Identification & Authentication

Temporary Passwords

"Allow temporary password use for system logons with an immediate change to a permanent password."

Key Discussion Points

Immediate, Not Optional:
The change must happen at first logon — the system must force it, not suggest it. A user who skips it is noncompliant.

Predictable Formats:
Temp passwords like 'Acme123!' or FirstName+DOB are guessable before first login. Randomized temporary passwords are safer.

Applies to All Resets:
New accounts, password resets, account unlocks, and service desk resets all qualify — any time IT sets a temporary password.

Complexity Still Applies:
The permanent password created must still meet 3.5.7 complexity requirements — the temp-to-perm change is not a bypass.

Assessment Methods

EXAMINE

Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings; password configurations and associated documentation.

INTERVIEW

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

TEST

Mechanisms supporting or implementing password-based authenticator management capability.

IA.L2-3.5.9

IDENTIFICATION & AUTHENTICATION — Temporary Passwords

Plain English

What this control is really saying:

When IT resets a password and hands someone a temporary one, that temporary password is a security risk from the moment it's created — it's known to at least one other person and is often predictable. This control requires that the first thing a user does with a temporary password is replace it with a permanent one they chose themselves.

How it is used:

- All new user accounts are created with 'User must change password at next logon' checked — the system enforces an immediate change at first login.
- Password resets by the service desk use the same 'must change at next logon' flag — temporary passwords cannot be retained beyond the first session.
- Temporary passwords are randomly generated by Active Directory — not derived from employee names, dates, or predictable patterns.
- The process is documented in the SSP and the IT admin onboarding procedure — every new account and reset follows the same enforced workflow.

Real World Example

The Scenario

Acme Defense's IT admin creates new accounts with a standard temporary password of 'Acme2024!' and emails it to the new employee. The 'must change at next logon' flag is not configured — the IT admin expects users to change it themselves.

What the assessor finds

Two of five user accounts are still using 'Acme2024!' — including one account created six months ago. The temporary password was never changed. There is no technical control enforcing an immediate change and no monitoring to detect accounts still using the temp password.

SPRS Score Impact

3.5.9 carries a point value of 3. Temporary passwords that are never changed represent long-lived known credentials — accounts running on default or IT-issued passwords are among the most easily compromised in a DIB environment.

What Good Looks Like

All new accounts and resets configured with 'must change at next logon', temporary passwords randomly generated, first-login change technically enforced, process documented in SSP and IT procedures, accounts monitored for persistent temp password use.

Common Gaps

What assessors actually find in the field:

✗ **No forced change on first login**

Temporary passwords are issued but the 'must change at next logon' flag is not set — users keep using the temp password indefinitely.

✗ **Predictable temp passwords**

IT always issues 'Welcome1!' as the temporary password — it is widely known among staff and easily guessable by attackers.

✗ **Service desk resets exempt**

New accounts enforce first-login change but service desk password resets do not — reset passwords persist as-is.

✗ **IT knows the temp password**

IT admin records temp passwords in a shared spreadsheet — the credential is not truly private to the user from first use.

✗ **Temp passwords not time-limited**

Temporary passwords for contractor accounts are valid indefinitely if not used — an unused reset account is a persistent risk.