MP.L2-3.8.2

Media Protection

Media Access

"Limit access to CUI on system media to authorized users."

Objectives

[a]

Access to CUI on system media is limited to authorized users.

Key Discussion Points

Authorized Users Only:
Access to CUI on media must be limited to individuals specifically authorized — proximity or employment alone does not qualify.

Access List Required:
The guide example designates a data owner who maintains a named list of authorized users — access without being on the list is a finding.

Audit Log:
Access to physical CUI media should be logged — the guide explicitly calls for an audit trail of who accessed media and when.

Extends 3.8.1:
3.8.1 requires secure storage; 3.8.2 limits who can access what is stored — both must be met, and they reinforce each other.

Assessment Methods

EXAMINE

System media protection policy; procedures addressing media storage; physical and environmental protection policy; access control policy and procedures; system security plan; system media; designated controlled areas.

INTERVIEW

Personnel with system media protection and storage responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection.

MP.L2-3.8.2

MEDIA PROTECTION — Media Access

Plain English

What this control is really saying:

Not everyone in the company should be able to pick up a USB drive with CUI on it. This control requires that access to CUI media is restricted to a defined list of authorized users, that a checkout procedure controls who has it, and that an audit log tracks every access.

How it is used:

- The project manager maintains a named list of individuals authorized to access CUI on USB drives — access is only granted to personnel on the list.
- A checkout log is required before any authorized user can remove a CUI media item — name, date, item ID, and return date are recorded.
- Physical access to the locked media cabinet is limited to the project manager and designated alternates — the key is not shared with general staff.
- Unauthorized access attempts are logged and reported to the security officer — access to CUI media outside the approved list is treated as an incident.

Real World Example

The Scenario

Acme Defense's CUI USB drives are stored in a cabinet in the engineering bay. All six engineers have a key. No authorized user list exists — any engineer can access any drive at any time. No checkout log is maintained.

What the assessor finds

An engineer who left the company two weeks ago had a cabinet key and is still listed as having the last-known drive in his possession. No audit log exists. There is no data owner, no access list, and no way to determine who has accessed CUI media.

SPRS Score Impact

3.8.2 carries a point value of 1. Unauthorized access to CUI media is a direct spill risk — without an access list and audit log, there is no way to detect or prove a breach involving physical media.

What Good Looks Like

Named authorized user list maintained by designated data owner, checkout log required for all media access, audit trail of access retained, access reviewed when personnel change, unauthorized access treated as incident.

Common Gaps

What assessors actually find in the field:

✗ **No authorized user list**

Any employee can pick up and use CUI media — no named list of authorized users exists.

✗ **No checkout log**

CUI media is stored but access is unlogged — there is no record of who accessed media or when.

✗ **Access list outdated**

An authorized user list was created but never updated — former employees and reassigned staff are still listed.

✗ **All staff have cabinet access**

The media cabinet key is on a shared hook in the office — anyone can access CUI media without authorization.

✗ **No data owner designated**

CUI media has no designated owner — nobody is responsible for approving or tracking access.