MP.L2-3.8.9

Media Protection

Protect Backups

"Protect the confidentiality of backup CUI at storage locations."

Objectives

[a]
The confidentiality of backup CUI is protected at storage locations.

Key Discussion Points

Storage Location:
This control targets the backup storage location — not transport (3.8.6) but where the backup sits at rest: closet, offsite vault, or cloud.

Encrypt or Secure:
Cryptographic mechanisms are the primary method — alternative physical controls (locked vault, access-controlled room) also satisfy this.

Includes System-Level:
OS, application, and license backups count if they contain CUI — system-level and user-level backup data are both in scope.

FIPS Required:
If encryption is used, it must be FIPS 140-2 validated per SC.L2-3.13.11 — proprietary or non-validated encryption fails the assessment.

Assessment Methods

EXAMINE

Procedures addressing system backup; system configuration settings; system security plan; backup storage locations; system backup logs or records.

INTERVIEW

Personnel with system backup responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for conducting system backups; mechanisms supporting or implementing system backups.

MP.L2-3.8.9

MEDIA PROTECTION — Protect Backups

Plain English

What this control is really saying:

Your CUI is encrypted on the server. Your backups of that same CUI go to an unencrypted external drive in a closet. Now your backups are the vulnerability. This control requires that backup CUI is protected at its storage location — encryption, physical security, or both.

How it is used:

- All backup media containing CUI is encrypted before storage — full-system backups use FIPS 140-2 validated AES-256 encryption.
- Offsite backup tapes are stored in a locked, access-controlled vault at the offsite vendor — only authorized personnel can retrieve them.
- Cloud backup destinations for CUI use encryption in transit and at rest — the cloud provider's encryption configuration is documented in the SSP.
- Backup confidentiality controls are reviewed annually and after any change to the backup infrastructure.

Real World Example

The Scenario

Acme Defense encrypts CUI on its file servers. Nightly backups run to an external USB drive that sits in an unlocked storage closet. The backup software does not enable encryption. The backup drive is not password-protected.

What the assessor finds

A cleaning crew member takes the backup drive from the unlocked closet. The drive contains a full unencrypted backup of the CUI file server — all design files, contract documentation, and personnel data are immediately readable. No encryption, no access control on the storage location.

SPRS Score Impact

3.8.9 carries a point value of 3. Organizations frequently protect live CUI systems but neglect backup confidentiality — backups contain the same CUI and are often stored with fewer controls than the primary systems.

What Good Looks Like

Backup CUI encrypted at storage location using FIPS 140-2 validated cryptography, offsite backups in secured access-controlled facility, cloud backups encrypted in transit and at rest, backup confidentiality controls documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ Backups stored unencrypted

Backup drives are stored in an unlocked closet without encryption — anyone who accesses the closet can read the CUI backups.

✗ Offsite vendor unsecured

Backup tapes sent offsite are not encrypted and the vendor's storage facility has no access controls — the tapes are accessible to vendor staff.

✗ Cloud backups not encrypted

Backups are sent to a cloud storage bucket with no encryption configured — bucket misconfigurations have exposed data in similar environments.

✗ Backup media not included

The security program protects live CUI systems but backup media is excluded — backups contain the same CUI but with no protection controls.

✗ Non-FIPS encryption used

Backup software uses proprietary encryption — it is not FIPS 140-2 validated, failing the assessment consideration for this control.