MA.L2-3.7.3

Maintenance

Equipment Sanitization

"Ensure equipment removed for off-site maintenance is sanitized of any CUI."

Objectives

[a]

Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.

Key Discussion Points

Before Departure:
CUI must be removed from equipment before it leaves the facility — not after it returns from the vendor, but before departure.

Three Methods:
Clear (overwrite), purge (degauss/secure erase), or destroy (shred/incinerate) — NIST SP 800-88 Rev. 1 is the authoritative reference.

Document It:
Sanitization must be documented — device, method, who, and when. Sanitization records are a named EXAMINE artifact for this control.

All Relationships:
Warranty, contract, in-house, and software maintenance agreements are all covered — the maintenance relationship type does not matter.

Assessment Methods

EXAMINE

System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan.

INTERVIEW

Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators.

TEST

Organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components.

MA.L2-3.7.3

MAINTENANCE — Equipment Sanitization

Plain English

What this control is really saying:

When a hard drive goes to a vendor for repair, any CUI on it goes with it. This control requires that before any equipment leaves your facility for maintenance, it is sanitized — data overwritten, degaussed, or otherwise rendered unrecoverable. Shipping a drive with CUI still on it is a spillage event.

How it is used:

- Before any drive or storage device is shipped for repair, the IT admin runs a DoD-compliant wipe using approved software — the wipe is documented in the equipment record.
- Defective SSDs are processed with a secure erase tool; defective HDDs with known data are degaussed before leaving the facility.
- Equipment sanitization records include the asset tag, sanitization method, technician name, date, and confirmation that the action completed successfully.
- For equipment that cannot be sanitized before removal (e.g., failed drive unreadable), the SSP documents the escalation procedure — including possible destruction.

Real World Example

The Scenario

Acme Defense's storage array experienced disk failures on two drives that housed CUI project files. The IT admin shipped the failed drives to the manufacturer under warranty. No sanitization was performed — the drives were not readable so staff assumed they were safe to ship.

What the assessor finds

Failed drives are not necessarily unreadable — vendor forensic tools routinely recover data from 'unreadable' drives. No sanitization records exist. No procedure for sanitizing or destroying failed drives before shipment is documented anywhere.

SPRS Score Impact

3.7.3 carries a point value of 3. Shipping unsanitized drives to a vendor is a CUI spillage event — and because vendor repair facilities are outside the organization's control, there is no way to recover or remediate the exposure once it occurs.

What Good Looks Like

Sanitization performed on all equipment before off-site removal, method appropriate to media type per NIST SP 800-88, sanitization records maintained, procedure for unsanitizable equipment documented, records retained as evidence.

Common Gaps

What assessors actually find in the field:

✗ **No sanitization before shipment**

Defective drives are shipped directly to the vendor with no sanitization — whatever CUI was on them goes with the drive.

✗ **No sanitization records**

Informal wiping is sometimes performed but never documented — no evidence exists that sanitization occurred before removal.

✗ **Wrong sanitization method**

A quick format is used instead of a DoD-compliant wipe — the data is still recoverable and the control is not met.

✗ **Not all media types covered**

Servers and workstations are wiped but printer hard drives and USB-connected storage are shipped for repair without sanitization.

✗ **No procedure for failed drives**

If a drive cannot be read, staff do not know what to do — there is no documented escalation path for equipment that cannot be sanitized.