MA.L2-3.7.6

Maintenance

Maintenance Personnel

"Supervise the maintenance activities of maintenance personnel without required access authorization."

Objectives

[a]

Maintenance personnel without required access authorization are supervised during maintenance activities.

Key Discussion Points

Who Needs Supervision:
Anyone without formal access authorization — vendors, consultants, OEM technicians, system integrators — must be supervised.

Time-Limited:
Use time-limited accounts scoped to minimum necessary access — the guide explicitly recommends temporary credentials with expiration dates.

What Supervision Means:
Physical presence or active session monitoring for the full duration — not dropping by once and leaving them alone the rest of the time.

Revoke When Done:
Temporary access must be revoked immediately when the maintenance work is complete — not at end of day, not next week.

Assessment Methods

EXAMINE

System maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan.

INTERVIEW

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

TEST

Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting or implementing authorization of maintenance personnel.

MA.L2-3.7.6

MAINTENANCE — Maintenance Personnel

Plain English

What this control is really saying:

When a vendor technician or consultant shows up to work on your CUI systems, they probably don't have the same background check and access authorization as your staff. This control says: that's fine, but someone must watch them the entire time. Supervision means physical presence, session monitoring, or both — not just leaving them alone with a temporary password.

How it is used:

- Vendor technicians receive time-limited accounts (12-hour expiration) scoped to only the systems they need to access — accounts are revoked immediately when work is complete.
- The IT admin or a designated backup is physically present or remotely monitoring the session for the entire duration of any unauthorized-personnel maintenance activity.
- A maintenance log entry is created for each vendor visit: name, company, date, systems accessed, work performed, and supervising employee.
- Third-party software providers who need remote access are given a temporary account that expires after the maintenance window — standard user accounts are never issued.

Real World Example

The Scenario

A software vendor arrives to update CAD software on two engineering workstations. The IT admin gives the technician the admin password, shows him to the server room, and goes back to his desk for the rest of the day. The vendor is alone for four hours.

What the assessor finds

The vendor had unsupervised physical and logical access to systems containing CUI for four hours. No supervision log exists. The admin password given to the vendor was the shared IT admin account — it was not temporary and has not been changed since the visit.

SPRS Score Impact

3.7.6 carries a point value of 3. Unsupervised vendor access to CUI systems is a well-documented insider threat and supply chain risk vector — an unescorted technician with admin access is an uncontrolled risk.

What Good Looks Like

Supervision required for all unauthorized maintenance personnel, time-limited accounts scoped to minimum access, supervisor present or monitoring throughout, maintenance log documents visit details, accounts revoked when work is complete.

Common Gaps

What assessors actually find in the field:

✗ **Vendor left unsupervised**

A vendor technician was given the server room keypad code and left alone to work — no escort, no monitoring, no supervision.

✗ **Permanent account issued**

A consultant was given a standard domain account for a two-week project — the account is still active six months later.

✗ **No supervision procedure**

The policy says vendors must be supervised but no procedure defines who supervises, what that entails, or how it is documented.

✗ **Temporary account not revoked**

Temporary maintenance accounts are created but never reviewed — IT has no process to ensure they are disabled after the work is done.

✗ **Broad access granted**

Vendor accounts are given domain admin rights for convenience — the access is far beyond what the maintenance work requires.