AC.L2-3.1.18

Access Control

Mobile Device Connection

"Control connection of mobile devices."

Objectives

[a]
Mobile devices that process, store, or transmit CUI are identified.

[b]
Mobile device connections are authorized.

[c]
Mobile device connections are monitored and logged.

Key Discussion Points

Identify First:
[a] requires identifying every mobile device that touches CUI — phones, tablets, laptops, and e-readers — before authorization or monitoring can be applied.

BYOD Risk:
Personal devices connecting to CUI systems represent the hardest gap to remediate — BYOD either requires strong MDM containerization controls or outright prohibition.

MDM Is the Mechanism:
Mobile Device Management is the standard technical control for [b] and [c] — it enforces authorization policy, applies security baselines, and generates connection logs.

Offboarding Gap:
Former employees' personal devices often retain CUI access indefinitely — mobile device disconnection must be a required step in the offboarding procedure.

Assessment Methods

EXAMINE

Access control policy; authorizations for mobile device connections to organizational systems; procedures addressing access control for mobile device usage including restrictions; system design documentation; configuration management plan; system security plan; system audit logs and records; system configuration settings.

INTERVIEW

Personnel using mobile devices to access organizational systems; system or network administrators; personnel with information security responsibilities.

TEST

Access control capability authorizing mobile device connections to organizational systems.

AC.L2-3.1.18

ACCESS CONTROL — Mobile Device Connection

Plain English

What this control is really saying:

Phones and tablets are walking data stores. An employee who reads CUI email on a personal iPhone, or browses the CUI file server from a personal iPad, is a mobile device control problem. Every mobile device that touches CUI must be identified, explicitly authorized, and monitored. Personal devices without MDM enrollment mean uncontrolled CUI on unmanaged hardware.

How it is used:

- All mobile devices connecting to corporate email or CUI systems are enrolled in Microsoft Intune MDM before any CUI access is permitted — unenrolled devices are blocked by Conditional Access.
- MDM enforces minimum security baselines on all enrolled devices: PIN or biometric lock, full-disk encryption, and current OS version — non-compliant devices are automatically quarantined.
- BYOD is prohibited for CUI access — only company-issued devices enrolled in Intune are authorized, and this is documented in the access control policy and SSP.
- MDM generates connection logs for all enrolled devices — logs are reviewed monthly and non-compliant or unauthorized devices are immediately disconnected.

Real World Example

The Scenario

Acme Defense uses Microsoft 365 for email and file storage. Three engineers have corporate email on their personal iPhones. The operations manager uses a personal iPad to review CUI drawings during customer visits. No MDM exists.

What the assessor finds

Four personal devices access corporate email and CUI documents with no MDM enrollment, no encryption verification, no remote wipe capability, and no authorization record. One engineer recently departed — his personal phone still has active access to the M365 tenant with CUI.

SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

Mobile devices accessing CUI identified and inventoried, MDM enrollment required before CUI access, authorization documented per device, BYOD prohibited or strictly controlled, MDM compliance reports reviewed monthly, offboarding includes immediate mobile device disconnection.

Common Gaps

What assessors actually find in the field:

✗ **No MDM**

Employees access corporate email containing CUI on personal smartphones with no MDM, no encryption requirement, and no remote wipe capability.

✗ **BYOD without controls**

Personal devices connect to CUI systems with no authorization process, no MDM enrollment, and no baseline security requirements enforced.

✗ **No mobile device inventory**

The organization has no list of mobile devices accessing CUI — [a] is not met and [b] and [c] cannot be verified without identifying the devices first.

✗ **Terminated employee still connected**

A former employee's personal phone still has access to corporate email with CUI — no offboarding process disconnects mobile devices.

✗ **No monitoring or logging**

Mobile devices connect to CUI systems but no logs capture which devices connected, when, or what data was accessed — [c] is not met.