AC.L2-3.1.21

Access Control

Portable Storage Use

"Limit use of portable storage devices on external systems."

Objectives

[a]
The use of portable storage devices containing CUI on external systems is identified and documented.

[b]
Limits on the use of portable storage devices containing CUI on external systems are defined.

[c]
The use of portable storage devices containing CUI on external systems is limited as defined.

Key Discussion Points

External System Focus:
This control addresses company portable storage used on external systems — USB drives taken to client sites, personal computers, or any system outside the CUI environment.

Bidirectional Risk:
A USB drive used on an uncontrolled external system can introduce malware back into the CUI environment on return — this is as much a malware introduction control as an exfiltration control.

Two Implementation Paths:
v2.13 describes two approaches: written policy defining authorized devices and uses, or device authentication that technically limits the drive to approved systems only.

AutoRun Must Be Disabled:
AutoRun on CUI systems means any media inserted after external exposure executes automatically — disabling AutoRun via GPO is a baseline requirement across the CUI environment.

Assessment Methods

EXAMINE

Access control policy; procedures addressing the use of external systems; system security plan; system configuration settings; system connection or processing agreements; account management documents.

INTERVIEW

Personnel with responsibilities for restricting or prohibiting use of organization-controlled storage devices on external systems; system or network administrators; personnel with information security responsibilities.

TEST

Mechanisms implementing restrictions on use of portable storage devices.

AC.L2-3.1.21

ACCESS CONTROL — Portable Storage Use

Plain English

What this control is really saying:

This control is specifically about what happens when company-owned portable storage — USB drives, external hard drives, CDs — leaves the controlled CUI environment and gets plugged into external systems. A USB drive used on an unmanaged client laptop and returned to the CUI environment is a malware vector. This control requires documenting the circumstances, defining the limits, and enforcing them.

How it is used:

- Company policy prohibits use of company-issued portable storage devices on any external or personal systems — the acceptable use policy defines 'external system' to include client sites, personal computers, and non-CUI networks.
- Group Policy blocks USB storage devices on CUI workstations unless they are company-issued encrypted drives registered in the device management system.
- Engineers who require portable storage for a specific business function check out a company-issued encrypted USB drive from IT — the checkout is logged with the purpose, destination, and return date.
- AutoRun is disabled on all CUI workstations via GPO — media inserted into any CUI system does not execute automatically.

Real World Example

The Scenario

Acme Defense engineers regularly use USB drives to transfer design files between the CNC machine (not on the network), the engineering workstations, and the prime contractor's facility. Personal USB drives are freely used alongside company drives.

What the assessor finds

Personal USB drives are inserted into CUI workstations daily with no restriction. Company USB drives are carried to the prime contractor and plugged into their systems without controls. AutoRun is enabled on all workstations. Three engineers cannot account for company-issued USB drives. No GPO restricts USB use.

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

Portable storage policy defines authorized devices and approved external use cases, GPO restricts USB to company-issued encrypted devices, personal drives prohibited on CUI systems, AutoRun disabled, drive inventory maintained, checkout log for external use, drives encrypted.

Common Gaps

What assessors actually find in the field:

✗ Free-for-all USB use

Employees use personal USB drives on CUI workstations and company drives on personal computers daily — no restrictions, no policy, no controls.

✗ No portable storage policy

No policy defines what portable storage is authorized for external use — [a] and [b] are not met and [c] cannot be enforced without a defined baseline.

✗ GPO not restricting USB

Group Policy is supposed to block unauthorized USB use but it is not configured or not functioning — any device inserts freely.

✗ Unencrypted media on external systems

USB drives carrying CUI to the prime contractor's facility have no encryption — CUI data on unencrypted media used on external systems is immediately exposed if the drive is lost.

✗ AutoRun enabled

USB AutoRun is enabled on CUI workstations — malware on a drive inserted after an external visit executes automatically without user action.