AC.L2-3.1.22

Access Control

Control Public Information [CUI Data]

"Control CUI posted or processed on publicly accessible systems."

Objectives

[a]
Individuals authorized to post or process information on publicly accessible systems are identified.

[b]
Procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.

[c]
A review process is in place prior to posting of any content to publicly accessible systems.

[d]
Content on publicly accessible systems is reviewed to ensure that it does not include CUI.

[e]
Mechanisms are in place to remove and address improper posting of CUI.

Key Discussion Points

Designated Posters Only:
[a] requires identifying who is authorized to post — not everyone with website access. The designation must be documented and those individuals must be trained on CUI identification.

Periodic Audit Required:
New content is not the only risk — old capabilities briefs, case studies, and archived pages from past contracts may contain CUI that has been publicly accessible for years.

Pre-Publication Review:
[c] and [d] both require a review process — [c] establishes the process exists, [d] requires it is actually applied. A checklist with CUI screening and documented sign-off satisfies both.

Removal and Notification:
[e] requires mechanisms to remove CUI and address the incident — removal alone is not sufficient. The notification chain (prime contractor, contracting officer, DFARS 252.204-7012) must be documented.

Assessment Methods

EXAMINE

Access control policy; procedures addressing publicly accessible content; system security plan; list of users authorized to post publicly accessible content; training materials and records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records.

INTERVIEW

Personnel with responsibilities for managing publicly accessible information posted on organizational systems; personnel with information security responsibilities.

TEST

Mechanisms implementing management of publicly accessible content.

AC.L2-3.1.22

ACCESS CONTROL — Control Public Information [CUI Data]

Plain English

What this control is really saying:

CUI must never end up on the company website, LinkedIn, or any other publicly accessible system. This control requires designating who is authorized to post public content, establishing a pre-publication review process to screen for CUI, actively reviewing what is already public, and having a clear removal procedure for when CUI is discovered. Accidental public disclosure of CUI is a reportable incident.

How it is used:

- Only the marketing coordinator and the program manager are designated as authorized to post content to the company website — the authorized list is documented in the SSP.
- A pre-publication checklist is completed for every piece of content before it goes live — the checklist includes a CUI screening step with sign-off by a designated reviewer.
- The company website is audited quarterly for CUI — every page, document, and image is reviewed against the current list of CUI categories handled under active contracts.
- A documented procedure covers CUI removal: who is notified, how quickly the content is taken down, how the prime contractor and contracting officer are alerted, and what is preserved for incident documentation.

Real World Example

The Scenario

Acme Defense has a company website managed by the owner's spouse who handles marketing. The company recently posted a detailed capabilities brochure that includes photos of work on a DoD program and excerpts from the technical specifications.

What the assessor finds

The posted capabilities brochure contains program names, technical specifications, and design details that are CUI. The document was posted without any review. Nobody designated to post content has received CUI identification training. No review of existing web content for CUI has ever been conducted. No removal procedure exists.

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

Authorized poster list defined and trained on CUI identification, pre-publication review checklist for all web content, quarterly CUI audit of public-facing systems, immediate removal procedure documented with notification chain, staff trained on CUI marking and identification.

Common Gaps

What assessors actually find in the field:

✗ **No authorized poster list**

Any employee with the CMS password can post to the company website — no designated authorized individuals and no accountability for what gets published.

✗ **No pre-publication review**

Content goes live without any screening for CUI — press releases, case studies, capability briefs, and photos are published without a CUI review step.

✗ **CUI already on public website**

A capabilities document posted to the company website contains technical specifications, program names, or design details that are CUI.

✗ **No removal procedure**

No procedure exists for what to do when CUI is found on the public website — nobody knows who to call, what to preserve, or who must be notified.

✗ **No periodic review**

The company website has never been audited for CUI content — material from old contracts may have been publicly accessible for years.