**NIST 800-171 Cybersecurity Policy and Procedure Form CUI 3.13.16**

**3.13.16** Protect the confidentiality of CUI at rest.

CMMC SC.3.191Protect the confidentiality of CUI at rest.

**3.13.16 Self-Assessment Workbook Questions**

1. Are there controls used to protect CUI while stored in company information systems?
2. Does the system protect the confidentiality of information at rest?

<Organization Name> <Date of Current Revision>

**NIST Safeguard SC-28**

**SC-28 PROTECTION OF INFORMATION AT REST**

CMMC SC.3.191Protect the confidentiality of CUI at rest.

Control: The information system protects the confidentiality of [*Assignment: organization-defined information at rest*].

**Suggested Policy Clauses:**

1. The IT Manager shall appropriately encrypt any protected information residing in the information system.
2. The data protection plan shall be approved by the Compliance Officer.

**Implementation Date:** \_\_\_\_<Date of Current Revision>\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Authorizing Official:** \_\_\_\_<Name of Authorizing Official>\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  **Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.**

**Typed Signature:** \_\_\_\_<Typed Name of Authorizing Official or Designee>\_\_\_\_\_\_

**NIST 800-171A Assessment of Policy Effectiveness**

**3.13.16 ASSESSMENT OBJECTIVE**

Determine if the confidentiality of CUI at rest is protected

**Suggested ACRMS data inputs**

**Screen shot of front of ACRMS data input page**



**Question** **SC-28: PROTECTION OF INFORMATION AT REST**

**Answer SC-28:** [ ]  Yes [ ]  Yes Alt [ ]  No [ ]  NA [ ]  Partial

**Update SC-28:** 1 [ ]  Week [ ]  Month [ ]  Year

**Comments SC-28:** Specify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Policy File SC-28:** CUI 3.13.16 SC28 0820

**Screen shot of back of ACRMS data input page**



**Responsible Party SC-28:** [ ]  Compliance Officer [ ]  IT Manager [ ]  IT Consultant

[ ]  Other: Specify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Status SC-28:** [ ]  Pending [ ]  In Process [ ]  Complete [ ]  Other: Specify \_\_\_\_\_\_\_\_\_\_\_\_

**Target Date (for task) SC-28:** [ ]  Default (+1 year) [ ]  Other: Specify \_\_\_\_\_\_\_\_\_\_\_\_

**Task Edit SC-28:** [ ]  None [ ]  Other: The IT Manager shall appropriately encrypt any protected information residing in the information system.

The data protection plan shall be approved by the Compliance Officer.

**Screen shot of ACRMS task edit page**



Video Link: <https://attendee.gotowebinar.com/recording/5883155077189961729>