**NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.1.10**

Video <https://attendee.gotowebinar.com/recording/8036273738871298054>

**3.1.10** Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

**3.1.10 Self-Assessment Workbook Questions**

1. Is the system configured to lock sessions after a predetermined period of inactivity?
2. Is a pattern hiding display used when sessions are locked?
3. Can users lock sessions for temporary absence?
4. Does the system session lock mechanism place a publicly viewable pattern onto the screen? Hiding what was previously visible on the screen?

<Organization Name> <Date of Current Revision>

**NIST 800-53 Safeguard AC-11, AC-11(1)**

**AC-11: DEVICE LOCK**

a. Prevent further access to the system by [*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*] (typically “initiating a device lock after 15 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended”); and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

**AC-11(1) DEVICE LOCK: PATTERN-HIDING DISPLAYS**

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Supplemental guidance: When a system is unused for a long period (set by group policy), the computer system prevents further access to the system by beginning a session lock. The session lock continues until the user is able to gain access to restricted areas using the correct identification and password. Note: Users can directly start session locks. A session lock is not a substitute for logging out of the computer. A workstation that is unused for 15 minutes will go into session lock. A valid user id and password will be required to restart the workstation. If users intend to leave the area, the workstation is turned off.

**Suggested Policy Clauses:**

1. Each workstation shall go into session lock after <15 minutes> of inactivity as enforced by the <IT Manager>.
2. Workstations will be turned off when users leave the area.
3. Session lock screens will include a publicly viewable image.

**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>\_\_\_\_\_\_

(Editor’s note: The auditor assessment and the CMMC questions are below. Confirm that your policy meets these.)

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

**3.1.10 ASSESSMENT OBJECTIVE**: Determine if, for an organizational system that processes, stores, or transmits CUI:

3.1.10[a] the period of inactivity after which the system initiates a session lock is defined;

3.1.10[b] access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity; and

3.1.10[c] previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.

**3.1.10** **Potential Assessment Method and Objects** SELECT FROM: Access control policy; procedures addressing session lock; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; security plan; other relevant documents or records.

**CMMC Level 3 Assessment Guide**

* Does the session lock hide previously visible information (e.g., replacing what was visible with a lock screen or screensaver that does not include sensitive information)?
* If session locks are not managed centrally, how are all computer users made aware of the requirements and how to configure them?

**Suggested ACRMS data inputs**

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

Graphical user interface, application, Teams

Description automatically generated

**Question** **AC-11: SESSION LOCK**

**Answer AC-11:**  Yes  Yes/Alt  No  NA  Partial

**Policy File AC-11:** CUI 3.1.10 AC11 11(1) MoYr

**Screen shot of the ACRMS task edit page**

**Graphical user interface, text, email

Description automatically generated**

Each workstation shall go into session lock after <15 minutes> of inactivity as enforced by the <IT Manager>. File signed and dated report in Document Management Center (DMC).

Report Example: Session Lock

Tommy Lee enforces that each workstation shall go into session lock after 15 minutes of inactivity.

Filename: AC-11 Session Lock 09062023

Report Date: 09/06/2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Report Author: Tommy Lee \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

☒   Inserting my typed signature on the line below I hereby attest that I am an authorized report author or designated representative of an authorized report author and I approve the above Report on behalf of my organization.

Typed Signature: \_\_\_\_ Tommy Lee \_\_\_\_\_



Estimated hours: 5

The <Compliance Officer> reviews this policy and updates annually or as needed. File signed and dated policy in Document Management Center (DMC).

Example of updated Policy when no changes are made:

Download existing policy by opening the Document Management Center and right clicking on the file name and selecting download – see screen below.

Graphical user interface, application

Description automatically generated

Open Downloaded file in Microsoft Word. Update as shown below and save as PDF

Implementation Date: \_\_\_09/06/2023\_\_\_\_\_(new date)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Authorizing Official: \_Bobby Lee\_\_\_(no change)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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: \_\_\_Bobby Lee\_\_\_\_\_\_\_(no change)\_\_



Estimated hours: 0.10

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

Graphical user interface, application, Teams

Description automatically generated

**Question** **AC-11(1) SESSION LOCK: PATTERN-HIDING DISPLAYS**

**Answer AC-11(1):**  Yes  Yes Alt  No  NA  Partial

**Policy File AC-11(1):** CUI 3.1.10 AC11 11(1) MoYr