**NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.10.3, 3.10.4, 3.10.5**

Video: <https://attendee.gotowebinar.com/recording/8253128218370944259>

**3.10.3** Escort visitors and monitor visitor activity.

**3.10.3 Self-Assessment Workbook Questions**

1. Are all visitors to sensitive areas always escorted by an authorized employee?
2. Are visitors escorted and monitored as required in security policies and procedures?

**3.10.4** Maintain audit logs of physical access.

**3.10.4 Self-Assessment Workbook Questions**

1. Are logs of physical access to sensitive areas maintained per retention policies? (This includes authorized access as well as visitor access.)
2. Are visitor access records retained for as long as required by approved policy?

**3.10.5** Control and manage physical access devices.

**3.10.5 Self-Assessment Workbook Questions**

1. Are physical access devices (such as card readers, proximity readers, and locks) maintained and operated per the manufacturer recommendations?
2. Are these devices updated with any changed access control information necessary to prevent unauthorized access?
3. Does the facility/building manager review the location and type of each physical access device and evaluate its suitability for the company’s needs?
4. Are keys, combinations, and other physical access devices secured?

<Organization Name> <Date of Current Revision>

**NIST 800-53 Safeguard PE-3**

**PE-3 PHYSICAL ACCESS CONTROL**

a. Enforce physical access authorizations at [*Assignment: organization-defined entry and exit points to the facility where the system resides*] (typically “entry and exit points”) by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using [*Selection (one or more):* [*Assignment: organization-defined physical access control systems or devices*]; *guards*] (typically “locks”);

b. Maintain physical access audit logs for [*Assignment: organization-defined entry or exit points*] (typically “all entry and exit points”);

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [*Assignment: organization-defined physical access controls*] (typically “receptionist and locked doors”);

d. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity*] (typically “at all times”);

e. Secure keys, combinations, and other physical access devices;

f. Inventory [*Assignment: organization-defined physical access devices*] (typically “keys”) every [*Assignment: organization-defined frequency*] (typically “year”); and

g. Change combinations and keys [*Assignment: organization-defined frequency*] (typically “every 5 years”) and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

**Suggested Policy Clauses:**

* 1. <Organization Name> controls all entry and exit points to buildings or rooms that have computer systems.
1. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] (typically “all entry and exit points”) by;
2. Verifying individual access authorizations before granting access to the facility; and
3. Controlling ingress/egress to the facility using <receptionist and locks>.
4. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*] (typically “6 years”);
5. Provides [*Assignment: organization-defined security safeguards*] (typically “escorts”) to control access to areas within the facility officially designated as publicly accessible;
6. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*] (typically “at all times”);
7. Secures keys, combinations, and other physical access devices;
8. Inventories [*Assignment: organization-defined physical access devices*] (typically “keys”) every <year> and;
9. Changes combinations and keys <every five years> and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

**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**

**3.10.3 ASSESSMENT OBJECTIVE** Determine if:

3.10.3[a] visitors are escorted.

3.10.3[b] visitor activity is monitored.

**3.10.3** **Potential Assessment Method and Objects** SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records.

**CMMC Level 3 Assessment Guide**

* Are personnel required to accompany visitors to areas in a facility with physical access to organizational systems?
* Are visitors clearly distinguishable from regular personnel?
* Is visitor activity monitored (e.g., use of cameras or guards, reviews of secure areas upon visitor departure, review of visitor audit logs)?

**3.10.4 ASSESSMENT OBJECTIVE** Determine if audit logs of physical access are maintained.

**3.10.4 Potential Assessment Method and Objects** SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records.

**CMMC Level 3 Assessment Guide**

* Are logs of physical access to sensitive areas (both authorized access and visitor access) maintained per retention requirements?
* Are visitor access records retained for as long as required?

**3.10.5 ASSESSMENT OBJECTIVE Determine if,**

3.10.5[a] physical access devices are identified.

3.10.5[b] physical access devices are controlled.

3.10.5[c] physical access devices are managed.

**3.10.5 Potential Assessment Method and Objects** SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records.

**CMMC Level 3 Assessment Guide**

* Are lists or inventories of physical access devices maintained (e.g., keys, facility badges, key cards)?
* Is access to physical access devices limited (e.g., granted to, and accessible only by, authorized individuals)?
* Are physical access devices managed (e.g., revoking key card access when necessary, changing locks as needed, maintaining access control devices and systems)?

**Suggested ACRMS data inputs**

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



**Question** **PE-3: PHYSICAL ACCESS CONTROL**

**Answer PE-3:** [ ]  Yes [ ]  Yes/Alt [ ]  No [ ]  NA [x]  Partial

**Policy File PE-3:** CUI 3.10.3 3.10.4 3.10.5 PE3 MoYr

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

****

The <Compliance Officer> inventories <keys and badges> every <year>. File signed and dated report in Document Management Center (DMC).

Report Example: Inventory List - Keys and Badges

Bobby Lee inventories keys and badges ever year.

Filename: PE-3 Inventory List – Keys and Badges 01152023

Report Date: 01/15/2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Report Author: Bobby 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: \_\_\_\_ Bobby Lee \_\_\_\_\_



Estimated hours: 1

The organization’s <Compliance Officer> changes combinations and keys <every 5 years> and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. File signed and dated report in Document Management Center (DMC).

Report Example: Key Change

Bobby Lee changes combinations and keys every 5 years and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. Next change is due on 09/02/2023

Filename: PE-3 Key Change 09022023

Report Date: 09/02/2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Report Author: Bobby 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: \_\_\_\_ Bobby Lee \_\_\_\_\_



Estimated hours: 10

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.



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

Implementation Date: \_\_\_09/02/2023\_\_\_\_\_(new date)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

[x]  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