Domain 1 Access Control
Asset Control Procedure

Procedure # Insert Procedure Number	EFFECTIVE DATE January 1, 2026	APPROVED BY Insert Approver
VERSION # 2.0	LAST REVISED Insert Last Revised Date	REFERENCE CMMC Domain 1: Access Control Organizationally Controlled Assets (AC.L3-3.1.2e)

Purpose

The purpose of this procedure is to ensure the organization restricts access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.

Scope

The procedure in this document applies to all ORGANIZATION_NAME workforce members including, but not limited to, full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, authorized third parties, and anyone else granted access to sensitive information by ORGANIZATION_NAME.

Procedure

Level 3

ORGANIZATION_NAME will restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.

Identify and Catalog Organization-Controlled Assets

1. Log in to the asset management platform or inventory system with administrator credentials (e.g., Microsoft Intune, ServiceNow, or a similar asset tracking system).
2. Navigate to Asset Inventory
    a. Navigate to the asset or device inventory section within the management system.
3. Verify or Add Assets
    a. Confirm that all organization-controlled assets are listed in the inventory.
    b. If any devices are missing, add them to the inventory, ensuring each asset's details (e.g., owner, type, and provisioning status) are accurate.
4. Apply and Save Changes
    a. Save any updates to the asset inventory, ensuring the list is fully up-to-date.
5. Testing and Confirmation (Optional)
    a. Review the inventory by cross-checking it with physical devices or departmental records to confirm completeness.

Configure Access Controls on Network Devices

1. Log in
    a. Access the network management console (e.g., Cisco, Meraki, or firewall settings) with administrative credentials.
2. Navigate to Access Control Settings
    a. Go to the network security or access control section, often found under "Network Settings" or "Security."

3. Verify or Enable Device Authentication and Access Restrictions
    a. Ensure that only authenticated, organization-issued devices can connect to the network.
    b. Enable certificate-based authentication or MAC address filtering to restrict network access to authorized devices only.
4. Apply and Save Changes
    a. Apply the new security settings and save changes to enforce the restrictions.
5. Testing and Confirmation (Optional)
    a. Attempt to connect with an unauthorized or personal device to verify that access is denied as expected.

Implement Endpoint Management Compliance Policies

1. Log in
    a. Access the endpoint management system, such as Microsoft Endpoint Manager or another MDM solution, with administrative privileges.
2. Navigate to Compliance Policies
    a. Go to “Compliance” or “Policies” in the management system to configure access requirements for organization-owned devices.
3. Verify or Enable Compliance Checks
    a. Set up or verify compliance policies to enforce security baselines on all connected devices (e.g., antivirus, firewall, and encryption requirements).
4. Apply and Save Changes
    a. Apply the compliance policies and save settings to ensure only compliant devices are granted access.
5. Testing and Confirmation (Optional)
    a. Test by using a device that does not meet compliance requirements to confirm that access is restricted.

Configure Group Policies and Access Management

1. Log in to Active Directory or a similar access management tool with administrative credentials.
2. Navigate to Group Policy Management
    a. Go to “Group Policy Management” in the Active Directory console.
3. Verify or Set Access Controls Using Group Policies
    a. Create or edit group policies to restrict system access to approved users and devices only.
    b. Configure rules to deny access from external or personal devices to critical systems.
4. Apply and Save Changes
    a. Apply the group policy updates and save to enforce access restrictions.
5. Testing and Confirmation (Optional)
    a. Test the policy by attempting to log in from a personal device and confirm that access is restricted.

Regular Access Review and Audit

1. Log in
    a. Access the security information and event management (SIEM) tool or audit system (e.g., Splunk, Azure AD) with administrative credentials.
2. Navigate to Access Logs or Audit Reports
    a. Go to the “Access Logs” or “Reports” section within the SIEM or audit platform.
3. Verify Access Logs and Review Permissions
    a. Review recent access logs and audit user permissions to confirm that only authorized devices and users are accessing the network.

4. Apply and Save Changes
    a. Document any findings and adjust access permissions as needed to ensure compliance.
5. Testing and Confirmation (Optional)
    a. Schedule monthly or quarterly reviews to ensure that permissions and access logs remain accurate over time.

Commented [AR1]: This is Sample Text Only – Must Update with your organization specific procedures.

Roles and Responsibilities

The ORGANIZATION_NAME personnel responsible for restricting or prohibiting the use of non-organizationally owned systems, system components, or devices, including system and network administrators, as well as organizational personnel responsible for system security, are responsible for:

- The development, implementation, and maintenance of ORGANIZATION_NAME security procedures.
- Working with employees to develop procedures and plans in support of security procedures.

The Information Security Officer is responsible for conducting at least an annual review of the Asset Control Procedure, making any appropriate changes, and disseminating the updated procedure to workforce members.

Related Form(s) and Evidence

- None

Retention

Every policy and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. Other ORGANIZATION_NAME requirements may stipulate longer retention. Log-in audit information and logs relevant to security incidents must be retained for six years or a longer period depending on the strictest regulatory mandate.

Compliance

Failure to comply with this or any other applicable procedure will result in disciplinary actions. Legal actions may also be taken for violations of applicable regulations and standards. The Human Resources Department is responsible for the management and coordination of action associated with disciplinary actions.

Reference

- Cybersecurity Maturity Model Certification
  https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverviewv2.pdf
- CMMC Level 3 Assessment Guide
  https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL3v2.pdf
- NIST Special Publication 800-172
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf
- NIST Special Publication 800-53 Revision 5
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- NIST Cyber Security Framework
  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

CMMC	
Standard	**Description**
NIST SP 800-172	3.1.2e Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization
NIST SP 800-53 R5	AC-20(3) Non-Organizationally Owned Systems - Restricted Use
NIST Cybersecurity Framework	No mapping

Contact

Insert Contact Person
Insert Full Address

E: Insert Email ID
P: Insert Phone #.

Procedure History

Initial Effective Date: January 1, 2026