Domain 1 Access Control
Asset Control Policy

POLICY # Insert Policy 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 policy is to ensure that access to systems and system components is restricted solely to information resources that are owned, provisioned, or issued by the organization.

Scope
The policies in this document apply 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.

Policy
Level 3

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

ORGANIZATION_NAME recognizes that information resources not owned, provisioned, or issued by the organization, including systems or components owned by other organizations and personally owned device, present significant risks. These non-organizational information resources complicate the ability to implement a 'comply-to-connect' policy or to utilize component or device attestation techniques to ensure the integrity of the organizational systems.

ORGANIZATION_NAME must determine if:

- Information resources that are owned, provisioned, or issued by the organization are identified.
- Access to systems and system components is restricted to only those information resources that are owned, provisioned, or issued by the organization.

Sample policy statement:

Centralized Inventory and Tracking

All assets, including systems, devices, software, and information resources, are documented in a centralized inventory. This inventory is regularly updated and audited to ensure that all organizational assets are accurately tracked.

Access Restrictions

Access to systems and system components is restricted based on job roles and responsibilities. Only authorized personnel with a legitimate need are granted access. Access permissions are reviewed regularly to maintain compliance with organizational policies.

Asset Management System
Each organizational asset is labeled and tracked through an asset management system, which records asset type, assigned owner, location, and access restrictions. This system ensures that assets are managed effectively and securely.

Use of Organizational Resources
Access to ORGANIZATION_NAME systems, networks, and data is limited to organizationally owned, provisioned, or issued resources. Unauthorized use of personal or external devices for accessing organizational systems is strictly prohibited.

Monitoring and Logging of Asset Access
All access attempts to systems and system components are monitored and logged. These logs capture details such as user identity, date and time of access, and the resources accessed. Continuous monitoring helps identify and address any unauthorized access attempts promptly.

Third-Party Access
Before granting access to any third party, ORGANIZATION_NAME requires a formal authorization process to ensure that the third party adheres to the organization's asset protection standards. Agreements specifying security requirements for asset handling must be in place, and third-party compliance with these requirements is periodically assessed.

Roles and Responsibilities

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 personnel responsible for system security, are responsible for:

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

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

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 these or any other applicable policy 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.

Related Form(s) and Evidence

- None

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 #.

Policy History

Initial Effective Date: January 1, 2026