Domain 1 Access Control
Limit Information System Access Policy

POLICY #	EFFECTIVE DATE	APPROVED BY
Insert Policy Number	January 1, 2025	Insert Approver
VERSION #	**LAST REVISED**	**REFERENCE**
2.0	Insert Last Revised Date	CMMC Domain 1: Access Control Authorized Access Control [FCI Data] (AC.L1-b.1.i)

Purpose

The purpose of this policy is to ensure information system access is limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

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 1

ORGANIZATION_NAME will limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems.

Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include internal and external systems that are internal to the organization. This requirement focuses on account management for systems and applications.

ORGANIZATION_NAME will enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Additionally, ORGANIZATION_NAME will:

- Define and document the types of system accounts allowed for use within the system in support of organizational missions and business functions.
- Assign account managers for all system accounts.
- Establish conditions for group and role membership.
- Specify authorized users of the system, group, role membership, access authorizations (i.e., privileges), and other attributes (as required) for each account.
- Require approvals by workforce members for requests to create system accounts.
- Create, enable, modify, disable, and remove system accounts in accordance with defined policies, procedures, and conditions.
- Monitor the use of system accounts.
- Notify account managers within 24 hours for each situation when accounts are no longer required, when users are terminated or transferred, and when individual system usage or need-to-know changes for an individual.

- Authorize access to the system based on a valid access authorization, intended system usage, and other attributes, as required by ORGANIZATION_NAME or associated missions and business functions.
- Review accounts for compliance with account management requirements weekly.
- Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
- Align account management processes with personnel termination and transfer processes.

ORGANIZATION_NAME must determine if:

- Authorized users are identified.
- Processes acting on behalf of authorized users are identified.
- Devices (and other systems) authorized to connect to the system are identified.
- System access is limited to authorized users.
- System access is limited to processes acting on behalf of authorized users.
- System access is limited to authorized devices (including other systems).

Sample policy statement:
ORGANIZATION_NAME will enforce the application of Limit Information System Access Procedure for ORGANIZATION_NAME Microsoft 365 and AWS portal environments, including APPLICATION_NAME.

ORGANIZATION_NAME maintains a list of all personnel authorized to use company information systems. This list is used to support identification and authentication activities conducted by IT when authorizing access to systems.

ORGANIZATION_NAME will maintain the Limit Information System Access Procedure to include the most current procedures for:

- MICROSOFT 365 access authorization and management
- AWS client access authorization and management
- AWS employee access authorization and management
- AWS network protection management

Sample policy statement:
ORGANIZATION_NAME does not authorize temporary accounts on ORGANIZATION_NAME production systems.

ORGANIZATION_NAME requires accounts to be disabled after 60 days of inactivity.

Responsibilities

ORGANIZATION_NAME personnel with account management responsibilities, system or network administrators, and personnel with information security responsibilities 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 Limit Information System Access 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/ModelOverview.pdf
- CMMC Level 1 Assessment Guide
  https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL1.pdf
- NIST Special Publication 800-171 Revision 2
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.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 800-171 R2	3.1.1: Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
NIST SP 800-53 R5	AC-2: Account Management AC-3: Access Enforcement AC-17: Remote Access
NIST Cybersecurity Framework	PR.AA-03: Users, services, and hardware are authenticated. PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties. PR.PS-01: Configuration management practices are established and applied. PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.

Contact

Insert Contact Person
Insert Full Address

E: Insert Email ID
P: Insert Phone #.

Policy History

Initial Effective Date: January 1, 2025