Domain 1 Access Control

Limit System Access Procedure

Procedure # Insert Procedure Number	EFFECTIVE DATE January 1, 2025	APPROVED BY Insert Approver
VERSION # 2.0	LAST REVISED Insert Last Revised Date	REFERENCE CMMC Domain 1: Access Control Authorized Access Control [CUI Data] (AC.L2-3.1.1)

Purpose

The purpose of this procedure is to ensure the organization limits system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

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 2

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

Defining Access Control Policies

1. Log in to Microsoft 365 and Azure Admin Centers:
   a. The IT Administrator logs in to the Microsoft 365 Admin Center and Azure Portal via https://admin.microsoft.com/ and https://portal.azure.com/ to configure access controls and manage user accounts.
2. Establish Role-Based Access Control (RBAC):
   a. Use Role-Based Access Control (RBAC) to define roles and permissions for all users, ensuring access is granted based on job functions:
      i. Navigate to Azure AD > Roles and Administrators and configure roles, limiting access to critical systems like SharePoint, Teams, and internal applications based on job requirements.
      ii. Review and update roles quarterly to reflect any changes in job responsibilities or organizational structure.
3. Enable Multi-Factor Authentication (MFA):
   a. Enforce Multi-Factor Authentication (MFA) for all users accessing critical systems.
   b. Navigate to Azure AD > Security > MFA and configure MFA for all high-privilege users (e.g., administrators) and users accessing sensitive data in Microsoft 365.
   c. Ensure MFA is enabled for remote access and sensitive systems.

Managing User Accounts and Access Requests

1. Submit Access Requests:
   a. Employees must submit a formal Access Request to their Department Head specifying the systems and resources required for their role.

2. Review and Approve Access Requests
    a. The Department Head reviews access requests and verifies that the requested access aligns with the employee's job responsibilities. Approved requests are forwarded to the IT Administrator for provisioning.

3. Provision Access in Microsoft 365 and Azure:
    a. The IT Administrator provisions access.
    b. Navigating to Azure AD > Users to create or update the user's account, assigning the appropriate RBAC roles.
    c. Configuring access to SharePoint, Teams, and OneDrive based on the user's job role.
4. Grant Access to Shared Resources:
    a. Access to shared resources (e.g., shared drives, network devices) is granted based on RBAC roles:
        i. In SharePoint Admin Center, configure permissions for document libraries to ensure only authorized users can view or modify sensitive data.
        ii. For network resources, use Windows Server or Azure File Shares to control access to shared folders based on role.

Monitoring and Auditing Access

1. Monitor Access via Microsoft Defender:
    a. The Security Officer uses Microsoft Defender for Identity to continuously monitor user access, tracking login attempts, and identifying any unauthorized access attempts:
        i. Set up alerts for failed login attempts or unusual access patterns, such as logins from unfamiliar devices or locations.
        ii. Review Azure AD Sign-In Logs to detect anomalies in user access behavior.
2. Review User Access Logs Weekly:
    a. The IT Administrator reviews access logs from Azure AD and Microsoft 365 weekly to verify that users are accessing only authorized systems:
        i. Logs should include successful and failed login attempts, changes to access permissions, and file access activity. Store these logs securely in SharePoint for compliance tracking.
3. Conduct Quarterly Audits:
    a. The Compliance Officer performs quarterly audits of access permissions to ensure that users only have access to the resources required for their job roles. Any unnecessary or excessive permissions must be revoked.
        i. The audit includes reviewing RBAC configurations, checking MFA enforcement, and validating access to critical systems.

Revoking and Adjusting Access

1. Revoke Access for Departing Employees:
    a. Upon receiving a termination notice, the IT Administrator immediately revokes the employee's access by:
        i. Deactivating the user account in Azure AD and removing access to Microsoft 365, SharePoint, and other company resources.
        ii. Disabling any VPN or remote access credentials the employee may have.
2. Review Access for Role Changes:
    a. For employees changing roles, the Department Head must submit an Access Review Request to adjust permissions:

        i. The IT Administrator reviews and updates the employee’s RBAC permissions in Azure AD to reflect the new role, removing access to previous systems and granting access to new ones as needed.

3. Handle Temporary Access Needs:
    a. If an employee requires temporary access to additional systems for a specific project, the Department Head submits a Temporary Access Request:
        i. The IT Administrator configures temporary access in Azure AD, setting an expiration date for access, after which it is automatically revoked.

Reporting and Documentation

1. Generate Monthly Access Control Reports:
    a. The IT Administrator generates monthly reports from Azure AD and Microsoft 365 documenting new accounts, changes in permissions, and any security incidents related to unauthorized access attempts:
        i. These reports are reviewed by the Security Officer and stored in SharePoint for compliance tracking.
2. Document Access Control Policies in the SSP:
    a. The Security Officer ensures that all access control policies, including provisioning, monitoring, and revocation procedures, are documented in the System Security Plan (SSP). This documentation is stored in SharePoint for audit purposes.

ORGANIZATION_NAME must determine who, what, when and how:

- 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).

Roles and Responsibilities

The 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 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 Limit System Access 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/ModelOverview.pdf
- CMMC Level 2 Assessment Guide
  https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL2.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 #.

Procedure History

Initial Effective Date: January 1, 2025