Domain 1 Access Control
Control the Flow of CUI Policy

POLICY # Insert Policy 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 Control CUI Flow (AC.L2-3.1.3)

Purpose
The purpose of this policy is to ensure the flow of CUI is controlled according to approved authorizations.

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 2
ORGANIZATION_NAME will control the flow of CUI in accordance with approved authorizations.

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following:

- Keeping export-controlled information from being transmitted in the clear to the Internet.
- Blocking outside traffic that claims to be from within the organization.
- Restricting requests to the Internet that are not from the internal web proxy server.
- Limiting information transfers between organizations based on data structures and content.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on the characteristics of the information or the information path.

Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing keyword searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

Transferring information between systems representing different security domains with different security policies introduces a risk that such transfers violate one or more domain security policies.

In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes:

- Prohibiting information transfers between interconnected systems (i.e., allowing access only).
- Employing hardware mechanisms to enforce one-way information flows.
- Implementing trustworthy mechanisms to reassign security attributes and security labels.

ORGANIZATION_NAME must determine if:

- Information flow control policies are defined.
- Methods and enforcement mechanisms for controlling the flow of CUI are defined.
- Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.
- Authorizations for controlling the flow of CUI are defined.
- Approved authorizations for controlling the flow of CUI are enforced.

Sample policy statement:
Control of CUI Flow:
ORGANIZATION_NAME enforces controls on the flow of CUI to ensure it is not sent, accessed, or transferred to unauthorized individuals or external systems. CUI may only be transmitted or accessed on approved systems and secure channels, ensuring that only authorized users and devices handle sensitive data.

All transfers of CUI, whether within ORGANIZATION_NAME or externally, must occur through secure, encrypted methods that comply with the organization's security protocols. Unauthorized methods of transfer, such as unencrypted email or unauthorized cloud storage, are strictly prohibited.

Monitoring and Logging of CUI Transfers:
All transmissions and movements of CUI within ORGANIZATION_NAME are monitored and logged. These logs capture essential details of each transfer, including the sender, recipient, date, and method of transfer. Monitoring ensures compliance with security controls and that any unauthorized attempt to transfer CUI is promptly identified and addressed.

Third-Party Transfers:
Before CUI is shared with any third party, ORGANIZATION_NAME requires formal authorization and a review to confirm that the third party adheres to CUI protection standards. Agreements specifying security requirements for CUI handling must be in place, and ORGANIZATION_NAME will periodically assess third-party compliance with these requirements.

Roles and Responsibilities

ORGANIZATION_NAME system or network administrators, personnel with information security responsibilities, and system developers 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 Control the Flow of CUI 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 a 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 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	3.1.3: Control the flow of CUI in accordance with approved authorizations.
NIST SP 800-53 R5	AC-4: Information Flow Enforcement
NIST Cybersecurity Framework	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained. 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