[Insert Company Name or Logo]	
Title: Mapping IT Communication and Data Flows	**P&P #:**
Approval Date:	**Review: Annual**
Effective Date:	**Information Technology**

Purpose
This document outlines the guidance and processes for controlling the flow of information within the organization (physical and virtual) and between connected systems based on organization-defined information flow control policies.

Scope
This applies to all information technology systems owned and operated by [insert company name.]

Definitions: N/A

Policy
This information flow control policy regulates where information can travel within a system and between systems based on the characteristics of the information and/or the information path.

Communications (data) can be monitored, controlled, and protected at boundary components by restricting or prohibiting interfaces in organizational systems. Boundary protection components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Organizations must also consider the trustworthiness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content.

Procedure
The Security Officer has established, implemented and maintains a network configuration standard by implementing the following support controls:

1. Use of active asset inventory discovery tool to identify sensitive information for data flow diagrams
2. Establishment, implementation, and maintenance of a sensitive information inventory
3. Inclusion of information flows to third parties in the data flow diagram
4. Deployment of gateways to monitor the volume/content of date being transferred

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

5. Identification, inventorying, and management of the types of data that flow through the company's information assets from internal and external users and outside entities.
6. Enforcement of organization-defined information flow control policies as a basis for flow control decisions.

The Security Officer shall further:

- Establish, document, and manage a diagram that shows all communication and data flow across systems and networks with baseline mapping of network resources, expected connections and data flows.

- Create data flow documentation to identify what/where data is processed, stored or transmitted, and if it is temporarily or permanently retained. Review data flow documentation at defined intervals, at least annually, and after any change.

- Design and configure Network environments and virtual instances to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.

- Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Violations: Our workforce members are responsible for complying with our data flow management policies and procedures. Employees who violate these policies and procedures are subject to discipline up to and including termination.

Attachments: Organization-created Data Flow Schematic

Related Policies: IT Asset Management

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.