	Georgia Technology Authority	
Title:	**Network Security Information Flow**	
PSG Number:	**PS-08-030**	
Effective Date:	3/20/2008	**Review Date:** 09/15/2024
Synopsis:	Establishes a requirement for agencies to control the flow of information traversing their networks	

PURPOSE

IT networks logically and physically extend data, processing and communication across the organization and beyond organizational boundaries. Security services that protect the data, processing and communication infrastructure must also be distributed throughout the network.

When properly selected, configured, monitored and maintained, network security controls help control and protect the flow of information within and between system boundaries and enforce security policy.

This policy requires that agencies protect and control the flow of information traversing their networks.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(8) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(9) - *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(27) - *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(28) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

POLICY

Agencies that manage State of Georgia IT networks shall ensure network configurations enforce assigned authorizations that control the flow of information within the system boundary and between interconnected systems in accordance with applicable security policies, protection requirements and applicable information exchange agreements.

Any connections to the Internet, or other external networks or information systems, shall occur through controlled interfaces.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Network Security Controls (PS-08-027)
Network Security-Boundary Protection (SS-08-047)
Network Access and Session Controls (SS-08-048)
Public Access Systems (PS-08-028)
Web and E-Commerce Security (SS-08-049)

TERMS AND DEFINITIONS

System Boundary – All the components of an information system or an interconnected set of information resources under the same direct management control and security support structure, that share common functionality (normally includes hardware, software, information, data, applications, communications, and people).

Controlled Interfaces - Mechanisms that facilitate the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels).