	Georgia Technology Authority	
Title:	**Network Security - Information Flow**	
PSG Number:	PS-08-030.01	**Topical Area:** Security
Document Type:	Policy	**Pages:** 2
Issue Date:	3/20/08	**Effective Date:** 3/20/08
POC for Changes:	GTA Office of Information Security	
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, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See Enterprise Information Security Charter (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, GUIDELINES

- Network Security Controls (Policy)
- Network Security-Boundary Protection (Standard)
- Network Access Control (Standard)
- Public Access Systems (Policy)
- Web and E-Commerce Security (Standard)

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).

Note: The PSG number was changed from P-08-030.01 on September 1, 2008