	Georgia Technology Authority	
Title:	**Network Security Controls**	
PSG Number:	**PS-08-027**	
Effective Date:	03/20/2008	**Review Date:** 09/15/2024
Synopsis:	Requirements for network security controls	

PURPOSE

IT networks logically and physically extend data, processing and communication across the organization and beyond organizational boundaries. Security of IT networks is a critical element in an organization's information security infrastructure and in obtaining and maintaining established security objectives.

To reduce the risk of having a successful and possibly very costly compromise to a network adequate network security requires the proper combination of security policies, procedures, and personnel, as well as technical and operational controls applied in a defense-in-depth approach.

This policy requires each agency to establish multiple layers of network security controls along with network security best practices for State information systems to minimize the risks of attack or compromise while providing acceptable functionality and performance.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(10) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(21) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

TERMS AND DEFINITIONS

Defense-in Depth – Information Assurance (IA) "best practices" strategy for protecting networked environments where multiple layers of security defenses (policy, personnel, technology and operations) are placed throughout a network infrastructure to protect internal data, systems, networks, and users such that if one mechanism fails, another will already be in place to continue to protect the assets.

POLICY

Agencies shall implement a defense-in-depth strategy and network security best practices for securing the information technology networks that they operate.

These strategies shall protect the network communications and infrastructure, network boundary, control the flow of information and access to the computing environment (hosts/servers/applications/data, etc) while still providing acceptable functionality and performance.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Network Security-Information Flow (PS-08-030)
Network Access and Session Controls (SS-08-048)
Network Security-Boundary Protection (SS-08-047)
Web and E-Commerce Security (SS-08-049)