	Georgia Technology Authority	
Title:	**Network Access and Session Controls**	
PSG Number:	**SS-08-048**	
Effective Date:	**03/31/2008**	**Review Date: 12/01/2024**
Synopsis:	Establishes requirements for agencies to control and monitor network sessions	

PURPOSE

An unattended workstation or a hijacked network connection left idle can expose an organization to the risks of unauthorized access. Establishing controls that govern the rules and conditions for establishing, maintaining and terminating a network session is paramount to mitigating these risks.

This standard requires each agency to establish network access and session controls commensurate with the authorizations assigned to the users, the criticality of the network and sensitivity of the data.

SCOPE and AUTHORITY

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*

PM-04-001 – *Information Technology Policies, Standards and Guidelines*

PS-08-005 – *Enterprise Information Security Policy*

TERMS and DEFINITIONS

Network Session – lasting connection in a network protocol or between a user and a peer, typically a server, usually involving the exchange of many packets between the user's computer and the server.

STANDARD

Unless specifically designated as a public information system, access to any State of Georgia network and its resources shall require the use of state-issued identification and authentication credentials.

Access and use of state networks shall be in accordance with the appropriate use and access control-related enterprise policies and standards.

Only the minimum required network service access points shall be enabled and exposed.

All agencies shall establish and enforce network session controls that define rules and conditions for network connections.

- SESSION LOCK - All systems, network and/or applications, used to process, store, or transfer data with a security categorization of MODERATE or higher shall automatically initiate a session/screen lock after a limited period of inactivity, not to exceed 15 (fifteen) minutes, that remains in effect until the user re-establishes access using appropriate identification and authentication.
- SESSION TERMINATION - All remote access networked sessions and public facing applications requiring a logon must automatically TERMINATE the connection after an inactivity timeout not to exceed 15 (fifteen) minutes. The user must provide appropriate identification and authentication to re-establish the connection.

Access to and interconnections with State networks from external networks and systems shall occur through controlled interfaces.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Appropriate Use of IT Resources (PS-08-003)
Appropriate Use and Monitoring (SS-08-001)
Access Control (PS-08-009)
Authorization and Access Control Management (SS-08-010)
Network Security Controls (PS-08-027)
Network Security-Information Flow (PS-08-030)
Third Party Access (PS-08-011)
Secure Remote Access (SS-08-038)
Public Access Systems (PS-08-028)

REFERENCES

NIST SP 800-47 Interconnecting Information Technology Systems