	Georgia Technology Authority	
Title:	**Remote Access**	
PSG Number:	**PS-08-023**	
Effective Date:	03/20/2008	**Review Date:** 12/01/2023
Synopsis:	Establishes the requirement for agencies to protect internal state information resources from the risks associated with remote access.	

PURPOSE

Remote access, through technologies such as broadband, VPN, internet cafés, wireless and other mobile computing technologies has increased productivity for State of Georgia employees and contractors. However, the use of these technologies has introduced new security risks to the enterprise. Allowing remote access to non-public information resources is a logical extension of the enterprise yet outside the security boundary of the agency's control. As employees connect remotely to the corporate networks, these entry points and data transmission modes become increasingly vulnerable to agency internal networks and must be properly secured. Agencies need to approach the security of remote devices in the same manner as the wired internal components of the network.

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 Charter*

TERMS AND DEFINITIONS

Remote Access - the ability of an organization's users to access its non-public computing resources from locations other than the organization's facilities.
Telework or Telecommute - the ability of an organization's employees and contractors to conduct work from locations other than the organization's facilities.
Mobile Computing - a generic term describing one's ability to use technology 'untethered', that is not physically connected, or in remote or mobile (non static) environments.

POLICY

Agencies shall assess the risks and establish policies that explicitly define the architecture, methods, rules, procedures, and expectations for all forms of remote access to non-public state information systems, to include, but not limited to,

wireless, mobile computing and teleworking systems.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Secure Remote Access (SS-08-038)
Teleworking and Remote Access (SS-08-037)
Wireless and Mobile Computing (SS-08-039)

REFERENCES

NIST SP 800-46 Rev2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

NIST SP 800-114 Rev2 User's Guide to Telework and Bring Your Own Device (BYOD) Security

NIST SP 800- 28 Guidelines on Active Content and Mobile Code