	Georgia Technology Authority	
Title:	**Teleworking and Remote Access**	
PSG Number:	**SS-08-037**	
Effective Date:	03/31/2008	**Review Date:** 12/01/2024
Synopsis:	Establishes minimum security requirements for teleworking and remotely accessing state information systems	

PURPOSE

Teleworking and remote access allows employees and contractors to conduct official state business from locations other than state facilities and has increased productivity for State of Georgia employees. Various devices and technologies support teleworking and remote access such as desktop and laptop computers, cell phones, PDAs, broadband, VPN and wireless networking. However, the use of these devices and technologies has introduced new risks to the enterprise. As employees connect remotely to the enterprise networks using consumer devices not issued or controlled by the agency, these storage media entry points and data transmission modes become increasingly vulnerable. Agencies must approach security with the same risk management approach they use for their internal 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)(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

Remote Access -the ability of an organization's users to access its non-public computing resources from locations outside the organization's security boundaries. (Examples are teleworking, mobile computing, wireless, remote work-site, VPN, broadband, internet cafés, etc)

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 - generic term describing one's ability to use technology "untethered", that is not physically connected, or in remote or mobile (non-static) environments.

STANDARD

When teleworking and remotely access to internal, non-public state information systems is permitted, agencies shall develop remote access security plans that explicitly define the architecture, methods, rules, procedures, and expectations for all forms of remote access to non-public state information systems.

System owners shall provide remote users with secure login, connection procedures and instructions to securely access internal systems.

Agencies shall provide teleworkers and remote users with the requirements, guidance and recommendations for ensuring that remote/telework sites, remote access devices and user behavior uphold the physical and technical security requirements and policies for internal systems and mobile data.

Teleworkers and remote access users shall be required to acknowledge (in writing) understanding of their responsibilities and accountability for protecting state information assets when working remotely.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Remote Access (PS-08-023) [7]
Secure Remote Access (SS-08-038) [8]

REFERENCES

NIST SP 800-46, Security for Telecommuting and Broadband Communications
NIST SP 800-114 User's Guide to Securing External Devices for Telework and Remote Access
NIST SP 800-48, Wireless Network Security
NIST SP 800- 28 Guidelines on Active Content and Mobile Code
NIST SP 800-19 Mobile Agent Security