

	Georgia Technology Authority	
Title:	Wireless and Mobile Computing	
PSG Number:	SS-08-039	
Effective Date:	03/31/2008	Review Date: 12/01/2024
Synopsis:	Establishes the minimum requirements for implementing wireless network access	

PURPOSE

Wireless and mobile computing technologies offer network users benefit such as portability, flexibility and increased productivity. As employees connect remotely to the state networks, these entry points and data transmission modes increase the risks and vulnerabilities to agency internal networks and must be properly secured.

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 - ability of an organization’s users to access its non-public computing resources from locations outside the organization’s security boundaries.

Telework or telecommute - 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

Prior to implementing wireless and mobile technologies, agencies shall be aware of the technical and security implications associated with these technologies and assess the risks to ensure appropriate steps are taken to mitigate these risks.

To mitigate the security risks associated with wireless and mobile computing, system owners shall protect the internal systems by implementing the strongest, most appropriate security controls for encryption, user authentication and end-point protection mechanisms. Anti-virus protection and perimeter controls shall be properly configured and port openings shall be secured, restricted and monitored.

Agencies shall create a Wireless LAN (WLAN) Implementation Plan (as described in the WLAN Implementation Guideline) that adequately addresses the following areas of concern:

- Remote access, wireless access, and mobile computing policies and procedures
- WLAN architecture and implementation
- Configuration and security of access points
- Encryption and encryption keys
- Integration of wireless network to wired network (VPN)
- Security of data transmissions between wired and wireless networks
- Logical and physical protection of wireless/mobile/end-point devices
- Logical and physical protection of stored data in transit.
- Change management and configuration control
- Audit/monitoring
- Penetration tests and vulnerability assessments
- Malicious code protection and Incident handling
- Security Awareness and Training

Agencies shall conduct periodic reviews to ensure that the wireless network and remote access technologies are utilized in a secure manner and in compliance with all applicable security requirements and standards.

The deployment and operation of open, unsecured wireless network access technology is prohibited.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Remote Access (PS-08-023)
Secure Remote Access (SS-08-038)
Use of Cryptography (PS-08-024)
Cryptographic Controls (SS-08-040)

REFERENCES

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
NIST SP 800-97 Establishing Wireless Robust Security Networks