

 Georgia Technology Authority	Georgia Technology Authority	
Title:	Secure Remote Access	
PSG Number:	SS-08-038.01	Topical Area: Security
Document Type:	Standard	Pages: 2
Issue Date:	3/31/08	Effective Date: 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes requirement to protect internal state information systems from risks associated with remote access.	

PURPOSE

Remote access technologies have 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 physical security boundary of the agency's control. As employees connect remotely to the corporate networks these entry points and data transmission modes increase the vulnerability to agency internal networks and must be properly secured.

This standard establishes the requirement for agencies to protect internal state information resources from the risks associated with remote access.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

When allowing remote access to non-public state information systems, agencies shall conduct a risk analysis to determine the access/connection methods that best supports the required security levels.

To mitigate the security risks associated with remote access to non-public State information systems, system owners shall protect the internal systems by implementing the strongest, most appropriate security controls for encryption, user authentication and end-point protection mechanisms.

- Remote Administrative Access: all network traffic supporting remote administrative access to servers must be encrypted from end to end. No clear text will be allowed.

Title:	Secure Remote Access
--------	----------------------

Anti-virus protection and perimeter controls shall be properly configured and port openings shall be secured, restricted and monitored.

All remote access shall support an automatic session termination after no more than 15 minutes of inactivity.

Granting remote access to state information resources shall be in accordance with the Enterprise Access Control policies and standards

Agencies shall ensure that remote users are aware of their roles and responsibilities for maintaining the security requirements of state information assets and adhering to security policies when they are away from state controlled facilities. Users shall acknowledge (in writing) their understanding of these policies and be held accountable.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Remote Access (Policy)
- Teleworking and Mobile Computing (Standard)
- Wireless LAN (Standard)
- Use of Cryptography (Policy)
- Implementing Cryptographic Controls (Standard)

REFERENCES

- NIST SP 800-46, Security for Telecommuting and Broadband Communications
- 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

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

Note: PSG number administratively changed from S-08-038.01 on September 1, 2008.

Effective Date:	March 31, 2008	2 of 2
-----------------	----------------	--------