| | | |
|---|---|---|
| GTA | **Georgia Technology Authority** | |
| **Title:** | **Teleworking and Remote Access (International)** | |
| **PSG Number:** | **SS-22-001** | |
| **Issue Date:** | **05/01/22** | **Effective Date: 06/01/2022** |
| **Synopsis:** | Establishes security requirements for remote access when traveling internationally. | |

## PURPOSE

This standard establishes minimum security requirements for teleworking and remotely accessing state information systems while traveling internationally.

## SCOPE and AUTHORITY

Information Technology Policies, Standards and Guidelines (PM-04-001)

## STANDARD

When teleworking outside of the US and remote access to internal, non-public state information systems, agencies shall develop remote access security plans that explicitly define the architecture, methods, rules, procedures, exemption process, and expectations for all forms of remote access to non-public state information systems. State-issued devices shall not be authorized to be taken outside the US without an exemption request “Approval” from the GTA Office of Information Security.

Request to take state-issued devices to countries outside the US may be denied, protecting state information and assets. GTA recommends all international exemption requests be submitted <14> days prior to travel.

State agency systems and data will not be accessible from outside the US. Any offshore access requires an approved exemption request from the GTA Office of Information Security and must be documented in the system security plans of such system, with a description of any compensating controls, and a business justification. This includes systems and data utilized by State employees operated by cloud providers.

Upon approval, 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 locations, remote access devices and user behavior uphold the physical and technical security requirements and policies for internal systems and mobile data.

Teleworkers and international 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

Teleworking and Remote Access
Remote Access (PS-08-023)
Secure Remote Access (SS-08-038)
Data Storage Location (SS-15-002.01)

## 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

## 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 worksite, 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.