	Georgia Technology Authority	
Title:	**Data Location and Access**	
PSG Number:	**SS-15-002**	
Issue Date:	**12/15/2014**	**Review Date: 12/01/2024**
Synopsis:	Establishes storage requirements for State data	

PURPOSE

When a data storage facility is not located in the United States (US), there is an increased risk that the data stored offshore will be subject to the sovereign control of the country where the data is located. Offshore data storage can occur in several ways as follows:

- A cloud service provider, such as one who provides Software as a Service (SaaS) applications, stores State data on servers in another country.
- A third-party service provider, a contractor that hosts an application utilized by State employees via network links, uses a data center in another country or uses a US data center but uses storage in another country.
- A Cloud or third-party service provider uses facilities in another country for disaster recovery, capacity management or other purposes.

There are significant risks to offshore data storage as follows:

- The physical location of data is often critical in determining which sovereign nation controls that data. There is no international standard that governs the question of data sovereignty. Rather, disputes about the control of data are resolved on a case-by-case basis, often depending upon geography and/or economic factors.
- Government authorities, courts, administrative bodies where a server is located may have more access or different access to State data than one expects in the United States.
- The potential for the exploitation of an insider threat increases whenever non-American staff has access to American data. Local cybersecurity capabilities of the hosting country and its internet service providers may be weaker than they are here in the United States.

In general, principles of good governance and caution require the State of Georgia to control its own destiny. Third-party hosted applications and cloud based services might utilize servers located anywhere in the world unless restricted by the State's contract with the service provider.

This standard requires all State data to be stored only on servers within the United States in order to reduce the jurisdictional and security concerns that attend offshore data storage.

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

Storage -technology consisting of computer components and recording media used to retain digital data.

Data Center - data center outside of the enterprise operational environment is a facility used for State approved processing and/or storage of State data, regardless of the data center's ownership.

STANDARD

When using contracted cloud services, a State agency must include appropriate contract language to retain data ownership and ensure appropriate measures of confidentiality, integrity and availability. This becomes more critical as the data's security categorization increases.

1. All State data must be processed, stored, transmitted and disposed of onshore (within the jurisdiction of the United States).

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

3. Agency services which are active upon the effective date of this standard which process, store, transmit or dispose of data offshore shall be brought into compliance with this standard at the earliest date of 1) the next renewal of the service's agreement or 2) two years from the effective date of this standard

State policy PS-08-024 and State standard SS-08-040 require the use of cryptographic controls when dictated by security objectives, risks of compromise or exposure, due to policy, statutory or regulatory requirements, or when other compensating controls are insufficient to meet required security levels. Agencies are directed to SS-08-040 for full requirements. SS-08-040 applies to cloud hosted processing, State entity locally operated applications and applications in operation in the enterprise operational environment.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Outsourced Facilities Management PS-08-019
Use of Cryptography, PS-08-024
Data Categorization – Impact Level SS-08-014
Computer Operations Center Security SS-08-016
Secure Remote Access SS-08-038
Cryptographic Controls, SS-08-040
Outsourced IT Services and Third-party Interconnections SS-08-044
Teleworking and Remote Access, International SS-08-037