x

	Georgia Technology Authority	
Title:	**Third-Party Security Requirements**	
PSG Number:	**SS-08-013**	
Effective Date:	03/31/2008	**Review Date: 12/01/2024**
Synopsis:	Establishes security requirements for conducting business with contractors, outsourcing vendors and/or other third parties	

PURPOSE

In almost every aspect of state government, there is a need to outsource services to individuals or companies that are external to state government. The use of these outsourced services also known as third-party service providers, engagement contractors and/or consultants introduce certain risks to the enterprise because they have not been vetted through the state human resources and recruiting process. As such, their trustworthiness has not been established. However, for these individuals to be able to provide the services requested of them, there must be a level of trust granted to them that allows access to state facilities and state information assets. This standard establishes the minimum requirements for mitigating those risks.

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

Third Party – contractor, service provider, consultant or any other individual and/or organization external to state government providing services or behalf of, for, or as an agent of state government.
Sponsoring Agency – the state agency that has acquired the services of a third party or is otherwise responsible for granting physical and/or logical access to facilities, information, and/or information systems to entities external to state government, including but not limited to those defined in Third Party
Sourcing Agency – an external entity responsible for staffing state contracts on behalf of the sponsoring agencies.

STANDARD

Any agency sponsoring a contract with a third party shall assess and manage the risks associated with granting any access or outsourcing any services to the third-parties.

A signed contract is required prior to granting third parties physical or logical access to state facilities and/or information resources. The contract shall contain sections that delineate State information security issues relevant to that business access and requires the contractor to employ adequate security measures to protect state information, applications, and/or services outsourced to them and adhere to all state and agency security policies and standards.

The sponsoring agency shall provide documented notification of and ensure compliance with the Official Code of Georgia Annotated Computer Security Act as well as other applicable state or federal regulations, enterprise policies and standards, terms of confidentiality, non-disclosure, disciplinary procedures and other conditions of employment.

Third-party users that are not already covered by an existing confidentiality and non-disclosure agreement, per their agents, shall be required to sign such agreements prior to being given access to the information. Confidentiality and non-disclosure agreements shall be reviewed regularly, not to exceed every three years or when individuals leave the organization or when contracts expire.

Sponsoring agencies shall ensure that sourcing agencies for contractors, consultants, and third-party vendors conduct an identity validation and employment screening process similar to that required by the Personnel Identity and Verification Screening standard, to include: identity validation, employment eligibility, job-specific screening and notification of re-screening if there is cause for doubt or concern.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Third-Party Access (PS-08-011)
Personnel Security (PS-08-014)
Personnel Identity and Verification Screening (SS-08-017)
Outsourced IT Services and Third-Party Interconnections (SS-08-044)