	Georgia Technology Authority	
Title:	**Third Party Service Provider Verification & Screening**	
PSG Number:	**SS-24-001**	
Effective Date:	12/01/2024	**Review Date:**
Synopsis:	Establishes the process and requirements for screening and verification of third-party service providers	

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)(9) - *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

Agency – every state department, agency, board, bureau, commission, and authority but shall not include any agency within the judicial or legislative branch of state government, the Georgia Department of Defense, departments headed by elected constitutional officers of the state, or the University System of Georgia and shall also not include any authority statutorily required to effectuate the provisions of Part 4 of Article 9 of Title 11.

Third-Party Provider – contractor, sub-contractor, service provider, consultant or any other individual or organization external to state government providing services on behalf of, for, or as an agent of state government or otherwise requiring access to non-public state facilities and/or information resources.

Information Technology Services- refers to the application of business and technical expertise to enable agencies in the creation, management and optimization of or access to information and business processes.

STANDARD

Prior to authorizing access to agency information and information systems, agencies shall conduct personnel screening checks in accordance with applicable federal, or state laws, regulations, policies, standards and guidance for all contractors providing information technology services, outsourced applications, system development, testing or assessment services and network and security management. The level of background verification checks shall be commensurate with the role, responsibilities, level of access to be granted, risk designation and security concerns associated with the position responsibilities.

Agencies shall ensure that third-party provider screenings are consistent with background checks required by state or federal law based on role and/or access to sensitive state information and information systems.

Agency Process for Verifying Third-Party Providers

Each agency shall have a process that meets the following minimum requirements for verifying the identity of all third-party providers, their employment eligibility, and position qualifications prior to hiring and issuing credentials to access state facilities or information resources not otherwise designated as public access resources. The process shall also include defined standards that preclude third-party provider employment with the agency.

1. Validation through a federal work authorization program
2. Employment history verification
3. Education history verification
4. Validation of degrees and professional licenses
5. Residence verification
6. Criminal history - Information types for which access requires the successful completion of a criminal background check includes, but is not limited to,

Federal Tax Information (FTI), Criminal Justice Information (CJI), and Centers for Medicaid and Medicare System (CMMS) information.

7. References
8. In cases where a position calls for a more extensive background checks, other National Agency Checks (NACs) and credit bureau checks shall be conducted.

Agencies shall ensure that the third-party provider performs additional verification screenings prior to the provider transitioning to a role or is assigned responsibilities that involve access to state data and information systems.

Third-Party Provider Contracts and Agreements

Agencies shall include third-party personnel screening requirements in all contracts with consultants, contractors, and vendors that are to be provided with access to agency information assets. Contracts shall specify conditions of use and security requirements and the access, roles, and responsibilities of the third-party provider before access is granted.

Agency operational and/or sensitive information shall not be released to third-party providers without properly executed contracts and confidentiality agreements. Third-party providers that are not already covered by an existing confidentiality and non-disclosure agreement, shall be required to sign such agreements prior to being given access to the information.

Third-Party Provider Notification and Acknowledgement

Agency human resource officials shall provide third-party provider candidates documented notification and acknowledgment of the Official Code of Georgia Annotated Computer Security Act as well as other applicable federal, state and agency regulations or policies, terms of confidentiality, non-disclosure, sanctions and disciplinary procedures, and other conditions of employment, including mandatory participation in annual security awareness training.

Verification Renewals

Each state agency shall conduct third-party provider verification renewals in accordance with established agency policy and/or procedures not to exceed every five years. Agencies shall determine frequency of renewals based upon the third-party service provider's access to data and information systems, categorization of

data being accessed and all applicable federal, state, and local laws, regulations and requirements. Confidentiality and non-disclosure agreements shall be reviewed regularly, not to exceed every three years, or when contracts expire.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Third-Party Access (PS-08-011)
Third-Party Security Requirements (SS-08-013)
Outsourced IT Services and Third-Party Interconnections (SS-08-044)
Authorization and Access Management (SS-08-010)