	Georgia Technology Authority	
Title:	**Information Security Controls**	
PSG Number:	**PS-17-01**	
Effective Date:	05/01/2017	**Review Date:** 09/15/2024
Synopsis:	Security controls policy in a shared services environment	

PURPOSE

Security operation remains a top priority and is necessary to continue to advance security practices and processes. The definition of "ownership" within a shared services environment has different dimensions. Pertaining to security in a shared service environment, controls are established by agency business owners, but are executed by multiple parties. Often the delineation of these duties between parties are not clearly understood which may cause inconsistencies regarding the execution responsibilities of security controls. The Information Security Control Policy addresses this business challenge by establishing clear lines of delineation of security controls, ownership and overall execution responsibilities. The increased complexity of operating environments, service provider's management platforms and agency application service integration require established governance rules and processes.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(10) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(21) - *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 Service Providers- any person or entity that maintains, processes, or otherwise is permitted access to state-owned information through its provision of services. This includes all cloud-based technologies (i.e.):

- Software as a Service (SaaS) providers - companies that provide hosted application services.
- Infrastructure as a Service (IaaS) providers - companies that provide hosted data storage or processing services.

System Boundary – all the components of an information system or an interconnected set of information resources under the same direct management control and security support structure, that share common functionality (normally includes hardware, software, information, data, applications, communications, and

people).

Controlled Interfaces - mechanisms that facilitate the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels).

POLICY

Agencies, Service Providers and Service Integrators will comply with all applicable Security Controls required within NIST (or other Industry standard) required for state and federal compliance. These controls listed in standard SS-17-001 will be outlined in more detail within the NIST Control Families, Technical, Operational and Managerial Controls. Security controls will be determined and aligned to application/system classifications of Low, Moderate and High. After which each entity will work within this control framework to identify the appropriate security controls to support the application and system portfolio being managed. Control ownership will be identified, once identified that entity will be responsible for implementation and management of said control(s). Controls identified as "shared" will be co-owned between two or more entities who will assume responsibility together for execution of the control(s). The expectations are agencies, service providers and service integrators will work together within the enterprise environment to promote, foster and ensure a viable enterprise security program. Agencies using third-party service providers are still responsible for ensuring that their applications are operating within the security control compliance outlined in this policy.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Information Security Control Standard (SS-17-001)