

Topics:

[security policy](#) [2], [authority](#) [3], [charters](#) [4], [framework](#) [5], [GTA review](#) [6], [security framework](#) [7]

PS-08-005 Enterprise Information Security Charter

Issue Date: 3/20/2008

Revision Effective Date: 3/20/2008

PURPOSE

The state of Georgia is committed to protecting the information assets of the state and its constituents. All state agencies have a responsibility of due diligence and due care to that commitment. This policy reinforces that GTA is the authority to set statewide security governance and establishes the requirement for each agency to develop and maintain an internal information security program that adequately and effectively protects the information assets, personnel and facilities under their control based on an assessment of risks and business objectives.

Information security policies raise awareness of users to the potential risks associated with information technology. Employee awareness through dissemination of the policies helps minimize the cost of security incidents, accelerate the development of new application systems, and assure the consistent implementation of controls for information systems throughout the organization.

State of Georgia data is a valuable asset that must be protected. Prudent steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised. This policy demonstrates the commitment of the State and establishes the requirement to create, maintain, and adhere to a uniform set of information security policies, standards and general guidelines.

SCOPE

All State Agencies, as defined in the Official Code of Georgia Annotated § 50-25-1(b)(1) and all users (employees, contractors, vendors, and other parties) of State of Georgia information technology resources are expected to understand and abide by them.

POLICY

The State of Georgia, through the authority granted to the Georgia Technology Authority (GTA), shall create a framework of policies, standards and practices to facilitate an information security infrastructure based on the risk management framework established by the Federal Information Security Management Act (FISMA) of 2002 and the supporting documentation developed by the National Institute of Standards (NIST), that protects the integrity, confidentiality, and availability of its information assets from unauthorized disclosure, modification, use, or destruction, while still meeting business objectives.

The GTA Office of Information Security (OIS) shall development Enterprise security policies and standards that: identify and address general areas of risk; are clear, concise, measurable, and verifiable; provide a basis for compliance audits; and balance protection with productivity. OIS shall conduct periodic reviews of policies and standards to assess their effectiveness and issue updates as necessary.

All Agencies that create, use or maintain information assets for the State of Georgia shall develop, document,