	Georgia Technology Authority	
Title:	**Enterprise Information Security Charter**	
PSG Number:	PS-08-005.03	
Issue Date:	3/20/08	**Revision Date:** 7/01/2018
Synopsis:	Commits the State of Georgia to protecting information systems and data from unauthorized disclosure, modification, use, or destruction.	

PURPOSE

Georgia agencies are heavily dependent upon information and information systems to successfully conduct their missions. With ever increasing reliability on and growing complexity of information systems as well as a constantly changing risk environment, information security has become a mission-essential function. This function must be conducted in a manner that reduces the risks to the information entrusted to the agency, its overall mission, and its ability to do business and to serve the citizens of Georgia.

The State of Georgia is committed to protecting the information assets of the state and its constituents from unauthorized disclosure, destruction, or modification and to ensure its availability when needed. All state agencies and employees have a fiduciary responsibility of due diligence and due care to that commitment. This policy reinforces that GTA is the authority to establish statewide information security governance, and to facilitate each agency's ability to effectively meet both security and business objectives.

Information security policies and standards raise user awareness of the potential risks associated with information and information technology. Employee awareness through dissemination of the policies and standards helps reduce the likelihood and thus minimize the cost of security incidents, accelerate the development/deployment of new IT systems, and assure the consistent implementation of controls for information systems throughout the organization.

State of Georgia information is a valuable asset and prudent steps must be taken to ensure it is reliable, available and protected. This policy confirms the commitment of the State to manage information security risks and establishes the requirement that all agencies adhere to a uniform set of information security policies, standards, and general guidelines.

SCOPE

All State Agencies[1], 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.

POLICY

All agencies and representatives for the State of Georgia shall perform its legal and fiduciary duty of due diligence and due care to protect the information assets of the state and its constituents from unauthorized disclosure, destruction, or modification as well as ensuring it is available, reliable and non-reputable when needed.

The Georgia Technology Authority (GTA) shall, through the authority granted by state law, develop and maintain a framework of statewide information security policies, standards and guidelines. The policies, standards, and guidelines shall be based on the risk management methodologies established by the Federal Information Security Management Act (FISMA) and the supporting guidance developed by the National Institute of Standards and Technology (NIST).

The assemblage of statewide information security policies and standards shall:

- Identify and establish governance for the following areas of information security risk:
  - Security Management
  - Operations Security
  - Technical Security
- Establish the direction and be the foundation on which each agency develops and maintains an internal information security management program
- Facilitate a balance between asset protection with business objectives
- Be cohesive, clear, concise, measurable, and verifiable
- Provide a basis for assessing risk, controls reviews, and compliance audits

All State agencies that own, create, use or maintain information assets for the State of Georgia shall ensure adequate and effective measures are taken to protect the information assets, personnel and facilities under their control and shall comply with all applicable Enterprise information security policies and standards, federal and state regulatory requirements (such as but not limited to HIPAA, FERPA, COPPA, GLBA and CJIS) and law.

Additionally, GTA shall:

- Establish the roles and responsibilities of chief information officers and chief information security officers for state agencies
- Establish and review policies, standards, and guidelines to maintain their effectiveness and relevance
- Issue updates and new governance as necessary
- Continually monitor and evaluate new vulnerabilities and areas of potential risk
- Provide a waiver for any policies, standards, specifications, or contracts developed by GTA for agencies as deemed applicable

TECHNOLOGY SECURITY AUTHORITY

GTA is authorized by law to "establish technology security standards and services to be used by all agencies." [Official Code of Georgia Annotated (O.C.G.A.) § 50-25-4(a) (21)]. These standards and services flow from the technology security policies adopted by the GTA Board and shall be adhered to by all agencies except when not applicable to that agency.[1]

This authority in the area of security is broader than the general statutory authority granted GTA with respect to technology policies. O.C.G.A. § 50-25-4(a)(10) vests GTA with the authority to "set technology policy for all agencies[1] except those under the authority, direction, or control of the General Assembly or state wide elected officials other than the Governor."

Statewide security standards are binding upon all agencies[2]. Exempt entities have the discretion to adopt a GTA security standard or policy, modify it as it pertains to the exempt agency, or follow another policy. GTA invites discussion with exempt entities when questions arise.

[1] Security Policies may only apply to certain agencies that are within a "common community of interest." An example may be certain Policies dealing with HIPAA related data may only apply to agencies that handle certain patient or medical data. The same may be true for certain Standards or Guidelines.

[2] Agency is defined as "every state department, agency, board, bureau, commission, and authority which shall not include any agency within the judicial branch of state government 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." O.C.G.A. § 50-25-1(b) (1).

ENFORCEMENT

The State of Georgia enterprise information security policies and standards are based upon the Federal Information Security Management Act (FISMA) and industry best practices. Each state agencies is responsible for developing additional internal policies and procedures to facilitate compliance with these enterprise security policies and standards. While these policies and standards are designed to comply with or compliment federal and state laws and regulations; if there is a conflict, those applicable laws and regulations will take precedence and agencies shall implement whatever procedures are necessary to comply. Such conflicts must be communicated to the state's Chief Information Security Officer for review.

Violations of policy or standards could result in serious security incidents involving sensitive state or federal data. Violators (organizations or individuals) may be subject to punitive actions which could include but are not limited to administrative reprimand, public discredit, fines, lawsuits, termination and/or criminal prosecution.

Agencies may impose internal personnel actions upon their employees for violations of administrative policies or standards that do not constitute a criminal act.

The enterprise information security policies and standards will establish the baseline for periodic security controls reviews, vulnerability assessments, as well as audits by the State Department of Audits and Accounts (DOAA).

EXCEPTIONS

Exceptions to a policy or standard must be approved by the State Chief Information Officer (CIO) with review by the State Chief Information Security Officer. In each case, the agency or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval.

REFERENCES

Refer to NIST Computer Resource Center - *http://csrc.nist.gov* for additional information on FISMA and publications on information security:

- SP 800-53 Recommended Security Controls

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

See All Enterprise Information Security Policies, Standards and Guidelines

TERMS and DEFINITIONS

Governance - is the set of management processes, customs, cohesive policies, laws, and expectations affecting the way a corporation (company or government entity) directs and balances management activities with sound business practices, objectivity, accountability and integrity.

Policy - A general or high level statement of a direction, purpose, principle, process, method, or procedure.

Standard – A prescribed or proscribed specification, approach, directive, procedure, solution, methodology, product or protocol which must be followed.

Confidentiality - "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

- A loss of *confidentiality* is the unauthorized disclosure of information.

Integrity - "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

- A loss of *integrity* is the unauthorized modification or destruction of information.

Availability - "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

- A loss of *availability* is the disruption of access to or use of information or an information system.

Information Security Infrastructure – the interconnected elements (people, policies, processes, procedures and technology), that provide the framework to support an organizations security philosophy regarding their assets and effectively meeting their business objectives.

Information Assets - a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization. Irrespective, the nature of the information assets themselves, they all have one or more of the following characteristics:

- They are recognized to be of value to the organization
- Their Data Classification defines the value to the organization or mission
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization's corporate identity or reputation, without which, the organizational may be threatened.

Fiduciary Duty - legal or ethical relationship of confidence or trust.

Due Diligence and Due Care - the degree of effort and care that a prudent person/organization is expected to exercise in the examination and evaluation of risks.

FISMA – Federal Information Security Management Act requires each [federal and federally funded] agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

NIST – National Institute of Standards and Technology is a non-regulatory federal agency within the U.S. Department of Commerce chartered to promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act (FISMA).