	Georgia Technology Authority	
Title:	**Enterprise Information Security Policy**	
PSG Number:	**PS-08-005**	
Effective Date:	03/20/2008	**Revision Date:** 06/03/2024
Synopsis:	Commits the State of Georgia to protect information systems and data from unauthorized disclosure, modification, use, or destruction	

PURPOSE

The state of Georgia collects, manages, and stores information regularly and is committed to protecting the integrity, confidentiality, and availability of data and information assets of the state and its constituents. All state agencies are responsible for due diligence and care to that commitment. This policy reinforces that GTA is the authority to set Enterprise information security governance and establishes the requirement for each agency to develop and maintain an internal information security program that effectively protects the information, information assets, and resources used to conduct and support the state's business needs.

With the ever-increasing reliability and growing complexity of information assets and a constantly changing threat and risk environment, information security has become a mission-essential function for the state. This policy has been established to promote the following and demonstrates the requirement to create, maintain, and adhere to a uniform set of information security policies, standards, and general guidelines:

- Raise awareness of users to the potential risks associated with information technology
- Assure the consistent implementation of controls and management of information security threats and risks for information systems throughout the organization
- Minimize the impact of security incidents
- Accelerate the development of new application systems
- Enable compliance with applicable laws, regulations, and contractual obligations

- Enable sharing of information, expertise, and collaboration across organizations through common vocabulary and concepts related to information security practices and controls

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*
O.C.G.A. 50-25-4(a)(27) – State Government, Georgia Technology, General Powers
O.C.G.A 50-25-4(a)(28) State Government, Georgia Technology General Powers
PM-04-001 – *Information Technology Policies, Standards and Guidelines*

TERMS AND DEFINITIONS

Agency – "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).

Governance - 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 for managing technology and technology resources that must be followed.

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

Guidelines – A guideline is similar to either a standard or a policy, in that it outlines a specific principle, direction, directive, specification, or procedure but is not binding. Rather, a guideline is a recommended course of action.

Information Security Infrastructure – the interconnected elements (people, policies, processes, procedures and technology), that provide the framework to support an organization's 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:

- Recognized to be of value to the organization
- Data Classification defines the value of the organization or mission
- Difficult to substitute without incurring expenses, requiring specific skills, time, resources, or a combination thereof
- Contribute to the organization's corporate identity or reputation, the absence of which could pose a threat to the organization

POLICY

The state of Georgia, through the authority granted to the Georgia Technology Authority (GTA), shall create a framework of Enterprise policies, standards, and guidelines, to facilitate an information security infrastructure based on the methodologies and supporting publications established by the National Institute of Standards and Technology (NIST) that protects the integrity, confidentiality, and availability of its information assets from unauthorized disclosure, modification, use, or destruction.

The GTA Office of Information Security (OIS) shall develop and maintain Enterprise security policies, standards, and guidelines aligned with the current published versions of:

- NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations and the Cybersecurity Framework (CSF), including supporting publications
- NIST Special Publication 800-53 (SP 800-53), Security and Privacy Controls for Information Systems and Organizations), including publications that support the NIST control guidelines
- Center for Internet Security (CIS) Controls used to complement NIST SP 800-53

GTA shall establish the roles and responsibilities for key information security roles within the state of Georgia Information Security Program and conduct periodic reviews of Enterprise policies, standards, and guidelines to assess their effectiveness and relevance. GTA OIS will issue updates as necessary or establish policies, standards, and guidelines to maintain governance effectiveness.

All Agencies that own, create, use, or maintain information assets for the state of Georgia shall develop, document, implement, and maintain an internal information security infrastructure that establishes a security management organization that:

- Develops and implements policies, processes, and technology to adequately protect the information assets, personnel, and facilities under their control; and ensures compliance with Enterprise policies and standards, and federal and state regulatory requirements such as but not limited to IRS 1075, HIPAA, FERPA, PCI-DSS, SSA, CMS and CJIS.
- Utilizes NIST Special Publication 800-53 (current published version), as the basis for selecting information security controls. The selection and implementation of individual controls will be based upon the security categorizations using the methodologies and supporting publications developed by NIST and an overall understanding of the risks posed to that information and information system.
- Ensures that third-party providers, service integrators and managed service providers operating on their behalf operate within the security requirements outlined within Enterprise and Agency policy, standards, and procedures.

Agencies may exceed the security requirements put forth in Enterprise policies, standards, and guidelines in relation to system-specific or agency-defined applications and processes as needed to address business requirements. When security requirements are exceeded, the agency remains responsible for the maintenance and dissemination of policies, standards, guidelines associated with implementation and execution.

ENFORCEMENT

The state of Georgia's information security policies and standards are designed to comply with or complement federal and state laws and regulations; if there is a conflict, those applicable laws and regulations will take precedence and agencies shall implement whichever procedures are necessary to comply. Such conflicts must be communicated to the State’s Chief Information Security Officer for review.

Violations of policy could result in serious security incidents involving sensitive state or federal data. Violators may be subject to disciplinary actions which may include termination and/or criminal prosecution. Agencies may impose additional sanctions upon their employees for violations of policies.

The policies and standards will establish the minimum baseline for periodic security control reviews, assessments, and technical testing as well as audits by the State Department of Audits and Accounts (DOAA).

EXEMPTIONS

Agencies may request an exemption from the implementation of any enterprise information technology policy or standard by submitting an exemption form to gta.psg@gta.ga.gov. The exemption 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:

- Agency requesting the exemption
- Control(s) and standard(s) for which exception is being requested
- Business justification and impact for the exception
- Appropriate risk assessment associated with non-compliance
- Safeguards planned or implemented to mitigate risks (compensating controls)
- Residual risks
- Specific timeframe/duration to evaluate progress toward compliance
- Management or Agency leadership approval (to include the following: Business function owner, CIO, CISO/ISO/designated security representative, Agency Head, or delegate/Executive Director)

An exemption cannot be processed unless all residual risks have been identified and the Agency leadership has approved, indicating acceptance of these risks. Exemption requests must be re-evaluated periodically, and extension requests are required after one year.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

See all information security policies, standards, and guidelines.

REFERENCES

Additional terms and definitions used in this document can be found in the State of Georgia Enterprise Information Security Glossary *https://gta-psg.georgia.gov/glossary-terms.*

NIST SP 800-12: *An Introduction to Information Security*

NIST 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations

NIST SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations

NIST CSF 2.0: Cybersecurity Framework | NIST