	Georgia Technology Authority	
Title:	**Data and Asset Categorization**	
PSG Number:	**PS-08-012.02**	
Effective Date:	12/15/2014	**Review Date:** 12/01/2023
Synopsis:	Establishes a policy requirement to inventory and classify all state data and information processing systems throughout the enterprise.	

PURPOSE

Data is a critical asset of the state. All agencies have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by the state, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form). However, to adequately protect the data, there must be an understanding of what to protect, why to protect it, and how to protect it.

Data and asset categorization is essential in this understanding and enables agencies to proactively implement appropriate information security controls based on the assessed potential impact on the organization should certain events occur that jeopardize information confidentiality, integrity, and availability and in turn support their mission in a cost-effective manner. An incorrect information system impact analysis (i.e., incorrect FIPS 199 security categorization) can result in the agency either overprotecting the information system thus wasting valuable security resources, or under protecting the information system and placing important operations, assets, or individuals at risk. The aggregation of such mistakes at the enterprise level can further compound the problem.

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 Charter*

TERMS AND DEFINITIONS

Security Categorization – the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information

system would have on organizational operations, organizational assets, or individuals.

Security Objective – Confidentiality, Integrity, and Availability

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.)

POLICY

Data Owners shall inventory their information systems and assign a security category of HIGH, MODERATE or LOW to each system for which they hold responsibility using the categorization process contained in FIPS 199 Standards for Security Categorization for Federal Information Systems. The information processing systems shall assume a security category equal to the highest level assigned to the data or information in aggregate except where a system function or process is more critical than the data it processes.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Data Categorization-Impact Level (SS-08-014)
Classification of Personal Information (SS-08-002)

REFERENCES

NIST Computer Security Resource Center – http://csrc.nist.gov/ FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

PM 5 Information System Inventory

RA 2 Security Categorization