

Data Classification Policy

Security

DRAFT



STATE ACCOUNTING OFFICE
Security
Data Classification Policy

EFFECTIVE DATE: January 1, 2014

REVISION DATE: October 6, 2013

REFERENCE: *GTA Policy: Data and Asset Categorization (PS-08-012)*
 FIPS 199 Standards for Security Categorization
 GTA Policy: Data Categorization-Impact Level (SS-08-014)
 GTA Policy: Classification of Personal Information (SS-08-002)
 GTA Policy: Statewide Data Sharing (PM-07-003)
 GTA Policy: Georgia Open Records Act (O.C.G.A. § 50-14-1, ET SEQ)
 SAO Policy: Data Storage and Transmission Policy

[Purpose](#)

[Scope](#)

[Roles and Responsibilities](#)

[Policy](#)

[Exceptions](#)

[Compliance](#)

PURPOSE

The purpose of the Data Classification Policy is to provide a framework for securing State Accounting Office (SAO) system data that contains State of Georgia (SOG) agency or organization data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal. This policy provides general requirements for data classification.

SCOPE

This policy pertains to all information (obtained by employees in the course of performing job duties) for all SAO system data, and SOG agency or organization data maintained within SAO managed systems; regardless of the environment where the data resides. SAO managed systems include: TeamWorks (PeopleSoft Financials and Human Capital Management), Concur, Hyperion and supporting servers.

The term data includes:

- Electronic information both internal and external to SAO
- Visual or paper information that is shared and/or filed internal to SAO

All SOG agency or organization employees and third parties who request data from SAO systems should be made aware of this policy and adhere to this policy. Third parties include: external vendors, contractors, companies, or individuals.

ROLES AND RESPONSIBILITIES

Varying roles will aid in the classification of data. These roles are defined as follows:

Role	Definition
Data Owner	The Data Owner is the head of the agency or organization for which the data is owned. The Data Owner may delegate this responsibility to one or more individuals within the agency or organization. Data owners shall inventory and assign a security classification to the data for which they hold responsibility. Data Owners must adhere to this policy and educate users and the Agency Security Officer on how to properly classify data. Data owners will ensure the accuracy and completeness; protection of the data at rest/transit, based on its classification.
Data Steward	The specific employee or position assigned by a Data Owner to protect and manage the use of specific data.
Agency Security Officer (ASO)	The employee or position assigned by the Data Owner to protect specific data via management, security, and access. The ASO shall aid the Data Owner and Data Steward in the classification of agency or organization data. The ASO will be formally trained on how to properly classify data by SAO ISO.
SAO Information Security Officer (ISO)	The SAO Information Security Officer (ISO) defines the security governance for the data through the maintenance and implementation of policies, procedures and guidelines for the classification, management, security and access to data. The ISO is responsible for training the Agency Security Officers on how to classify data. The ISO also assists the ASO with agency or organization specific classification questions.
Data End User	Any individual who is eligible and authorized to access and use the data.

POLICY

Classification of Data

All SAO data is classified into levels of sensitivity to provide a basis for understanding and management. Accurate classification enables application of the appropriate level of security. These classifications of data take into account the legal protections (by statute, regulation, or by the data subject’s choice), contractual agreements, ethical considerations, and/or strategic or proprietary worth. Data can also be classified as a result of the application of “prudent stewardship”, where there is no reason to protect the data other than to reduce the possibility of harm or embarrassment to individuals or to the State.

The classification level definitions emphasize common sense steps to be taken to protect confidential data. SAO employees will have access to data for use in conducting SAO business. The classification level assigned to the data will act as a guide to those who may obtain or store data; for implementing security protections and access authorization mechanisms appropriate for that data.

Classification Levels

The classification of data in such levels encourages the discussion and subsequent full understanding of the nature of the data being displayed or manipulated. If an employee is uncertain of the classification of a particular piece of information, the employee should contact the Data Owner for clarification.

Data must be classified as one of the following:

Data Classification	Definition	Examples
Public	<p>Information maintained by SAO managed systems that is <u>not exempt</u> from disclosure under provisions of the Georgia Open Records Act (O.C.G.A. § 50-14-1, ET SEQ) or other applicable state or federal laws. Public information can be disclosed without restriction.</p> <p>If the information is classified as public: There are no requirements for marking or labeling as such.</p>	Open Record Requests for Public Information
Confidential	Information maintained by SAO that is exempt from disclosure under provisions of the Georgia Open Records Act (O.C.G.A. § 50-14-1, ET SEQ) or other applicable state or federal laws.	<ul style="list-style-type: none"> • Personally Identifiable Information • Proprietary research data • Certain confidential

Data Classification	Definition	Examples
	<p>Sensitive Information - information maintained by SAO that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of agency or organization financial transactions and regulatory actions.</p> <p>If the information is classified as confidential: All sensitive information should be clearly identified as “Confidential” and will be subject to the handling guidelines found in the Data Storage & Transmission Policy.</p>	<p>proprietary data</p> <ul style="list-style-type: none"> • Network diagrams and IP addresses • Server names and configurations • Contract cost estimates
Confidential (continued)	<p>Personal Information - is any non-public information about a living person that is factual in nature that would negatively impact his or her personal life if it were to become public. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to the individual who has data held about them upon request.</p> <p>Personally Identifiable Information (PII) - is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department</p> <p>Last name, and first name or initial, with any one of following:</p> <ul style="list-style-type: none"> • Address • Telephone numbers • Social Security Number • Driver’s License Number • Financial Personal Information • Tax Information • Health Records <p>Business/Financial Data Credit card numbers with/without expiration dates</p>	

EXCEPTIONS

Exceptions to this policy must be approved by SAO Information Security Officer (ISO) with review by the SAO Chief Information Officer (CIO). In each case the request for exception, 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. Denials of requests for exceptions may be appealed to the State Accounting Officer.

COMPLIANCE

Violation of this policy may result in disciplinary action, which may include termination for employees and temporary staff; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of SAO information system access privilege, and to civil and criminal prosecution.

DRAFT



200 Piedmont Ave
Atlanta GA 30334
sao.georgia.gov