GTA Georgia Technology Authority	**Georgia Technology Authority**	
Title:	**Data Categorization – Impact Level**	
PSG Number:	SS-08-014.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 5
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes Impact Level definitions and standards to be assigned to information assets throughout the enterprise.	

PURPOSE

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for state government, promotes effective management and oversight of information security programs, including the coordination of information security and data sharing efforts throughout the state. Determining the risk and potential impact of loss to information and processing systems is crucial to establishing appropriate protection, disaster recovery and business continuity measures.

This document establishes standards and guidelines to be used by all state agencies to assign risk levels to data and processing systems based on the security objective of providing appropriate levels of information security relevant to the potential impact of loss. This standard is based on the final report from the 2003 Georgia Digital Academy on Data Security (Appendix A and B) and is also consistent with the Federal Information Processing Standard 199 for security categorization.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

Data Owner/s shall inventory and assign a Security Categorization (high, moderate, or low) to all data and processing systems under their control.

Categorizations shall be commensurate to the potential impact of loss or compromise of the information and/or processing system, based on an assessment of risk, business objectives and the security objectives of confidentiality, integrity and availability.

Data Owners shall be responsible for implementing appropriate managerial, operational, physical, and technical controls for access, use, transmission, and disposal of State data commensurate to its security impact level as an integral part of its overall risk management approach.

The following definitions from FIPS 199 for Security Categorization shall be used for determining potential impact.

Security Objective	**Potential Impact: LOW**	**Potential Impact: MODERATE**	**Potential Impact: HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, and assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, assets, or individuals.

Data Owners shall ensure physical or logical segregation of data based on its impact level. An information system's overall impact level shall assume a value equal to the highest level assigned to the data resident on the system, except where system availability is more critical than the data.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Data & Asset Categorization (policy)
- Personal Information (standard)
- 2003 Georgia Digital Academy on Data Security (Appendices A and B) at http://gta.georgia.gov

REFERENCES

- FIPS 199 Standards for Security Categorization
- NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
- http://csrc.nist.gov

GUIDELINES

The following guidelines provide additional recommendations and best practices for effective data categorization and handling.

Security Categories should be used in conjunction with threat and vulnerability information when assessing risk to an organization.

Agencies must also consider the aggregate of the information when determining overall impact level. Where an employee's name alone may have an impact of Low; when this information is co-located with their SSN and/or medical data the overall classification becomes Medium.

Examples of Low Impact systems are systems/data that are available to the general public, or internal corporate systems requiring minimal access controls and have a high tolerance for delay, such as informational/public access web sites. There are usually no existing local, national or international restrictions on access or usage.

Examples of Medium Impact systems are systems/data containing corporate Proprietary, Privacy Act, or HIPPAA Information where need-to-know and access restrictions should be strongly enforced, data integrity or availability is important but there is a minimum tolerance for delay. Regulatory and/compliance requirements may apply.

Examples of High Impact data/systems contain or support highly sensitive information or processes. This may include systems or data that affect public safety, emergency preparedness, Homeland Security or other national-level interests. Access is highly restricted to authorized persons and data transmission is restricted to authorized communication channels. This information or system must **always** be available upon request, with **zero** tolerance for delay

In addition to classifying data, it is strongly recommended that each agency implement a process for labeling data and information systems with the security categorization and apply appropriate handling caveats where necessary to provide increased awareness to the sensitivity of the data and bring attention to unique data types and special handling requirements. Examples of handling caveats are:

- For Official Use Only or FOUO
- Contains Privacy Act Information
- Personnel Sensitive
- Procurement Sensitive
- Contains HIPPA Information

TERMS and DEFINITIONS

Information System - An information system (hereafter referred to as 'system') is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- **System:** A generic term used for briefness to mean either a major application or a general support system. Boundaries for a 'system' must be determined by security and/or IT personnel familiar with the environment.

Data Owner – The Agency Head is officially the owner of data/information within the authority of an agency, and may delegate ownership responsibilities. The Owner is responsible for the accuracy and integrity of the data/information; incurs the cost associated with gathering, managing, and storing the data/information; and is most affected by the loss of confidentiality, integrity, and availability of the data/information. Owners are also responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior). The data/information owner retains that responsibility even when the data/information is shared with other organizations. [Source: NIST SP 800-18].

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** is preserving authorized restrictions of information access and disclosure, including means for protecting privacy and proprietary information. The loss of confidentiality is the unauthorized disclosure of information. [44 U.S.C., Sec. 3542]

- **Integrity** is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The loss of integrity is the unauthorized modification or destruction of information. [44 U.S.C., Sec. 3542]

- **Availability** is ensuring timely and reliable access to and use of information. The loss of availability is the disruption of access to or use of information or an information system. [44 U.S.C., Sec. 3542]

Impact Level is the level assigned to data and processing systems relevant to the nature, sensitivity, or criticality to the primary business function of the agency or individuals and potential impact of loss or compromise.

Note: PSG number administratively changed from S-08-014.01 on September 1, 2008.