

Topics:

[Data Categorization](#) [2], [security level](#) [3], [personal information](#) [4], [confidentiality](#) [5], [integrity](#) [6], [availability](#) [7], [data classification](#) [8], **Data Categorization - Impact Level** [1]

SS-08-014 Data Categorization ? Impact Level

Issue Date: 3/31/2008

Revision Effective Date: 3/31/2008

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.

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.

- For a Security Objective of CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.[44 U.S.C., Sec. 3542]
 - With a Potential Impact of LOW: The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, assets, or individuals.
 - With a Potential Impact of MODERATE: The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, assets, or individuals.
 - With a Potential Impact of HIGH: The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, assets, or individuals.