

Title:	USG Information Technology (IT) & Information Security (IS) Risk Management	
Policy Number:	2009-Julian Date	Topical Area: Security
Document Type:	Program Policy	Pages: 2
Issue Date:	16-Feb-09	Effective Date: February 2009
POC for Changes:	USG Office of Information Security	
Synopsis:	Risk management is the process of taking actions to avoid or reduce risk to acceptable levels.	

Purpose

Risk management is an aggregation of three processes; risk assessment, risk mitigation, controls evaluation and measurement that helps an entity ensure that information security management processes are integrated with that entity's strategic and operational planning processes. Managing risk safeguards the mission, goals and provides an on-going evaluation and assessment of IT & IS related mission risks.

University System of Georgia (USG) Institutions must ensure the confidentiality, integrity and availability of information and information systems resources and assets by protecting them from unauthorized access, modification, destruction, or disclosure and ensure the physical security of IT resources and assets.

Policy Statement

Risk management is the process of taking actions to avoid or reduce risk to acceptable levels. This process includes both the identification and assessment of risk through risk analysis and the initiation and monitoring of appropriate practices in response to that analysis through the institution's risk management program.

The University System Office and USG Institutions need to ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure and to ensure the physical security of these resources. The USO and the USG Institutions shall also ensure that users, contractors, and third parties having access to institution computerized information resources are informed of and abide by this policy and the institution security plan, and are informed of applicable Federal Laws and State statutes related to computerized information resources.

Each USG Institution that employs information technology must establish risk management and disaster recovery planning processes for identifying, assessing, and responding to the risks associated with its information assets. The USG's information assets (its data processing capabilities, information technology infrastructure and data)

are an essential resource and asset. For many institutions, program operations would effectively cease in the absence of key computer systems. In some cases, public health and safety would be immediately jeopardized by the failure or disruption of a system. Furthermore, the unauthorized modification, deletion, or disclosure of information included in institution files and databases can compromise the integrity of University System of Georgia's programs, violate individual right to privacy, and constitute a criminal act.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

- USG Information Security Program Policy
- BOR Policy Manual – Section 700
- USG Appropriate Use Policy

References

[USG Risk Management Standard](#)

[ISO/IEC 27002:2005 \(formerly ISO/IEC 17799:2005\)](#)

[Federal Information Processing Standards \(FIPS\)](#)

[Risk Management Guide for Information Technology Systems \(NIST, SP 800-30\)](#)