STATE OF ALABAMA

Information Technology Policy

POLICY 606-00: RISK MANAGEMENT

Risk management encompasses the processes of risk assessment, which includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures; risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process, and a continual evaluation process to ensure a successful risk management program.

OBJECTIVE:

Define the elements of risk management, and establish the responsibilities for risk management of the State of Alabama computing environment.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management. Senior management must assess and incorporate the results of risk assessment activities into their decision-making processes.

System and Information Owners:

System and information owners shall fully support the risk management process. They are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own.

IT Managers and Information Security Officers:

IT Managers and Information Security Officers (ISOs) are responsible for their organizations' security programs, including risk management. They play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organizations' missions.

ISOs shall consult with senior management to ensure that risk management is an ongoing activity.

IT Security Practitioners:

IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems.

As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners shall use or support the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems

SUPPORTING DOCUMENTS:

- Information Technology Guideline 606G1: Risk Assessment and Mitigation

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
670-01	12/12/2006	Original document
606-00	09/01/2011	New number and format