

 Georgia Technology Authority	<b>Georgia Technology Authority</b>	
<b>Title:</b>	<b>System Lifecycle Management</b>	
<b>PSG Number:</b>	SS-08-025.01	<b>Topical Area:</b> Security
<b>Document Type:</b>	Standard	<b>Pages:</b> 2
<b>Issue Date:</b>	3/31/08	<b>Effective Date:</b> 3/31/08
<b>POC for Changes:</b>	GTA Office of Information Security	
<b>Synopsis:</b>	Requires agencies to implement a formal lifecycle management program for systems in development or operations.	

## PURPOSE

System life-cycle management is a necessity for establishing procedures, practices and guidelines governing and managing the life of an information system from conception/initiation through disposition. Its purpose is to assist system owners, developers and management document the design and decisions made regarding a system.

Many security-relevant events and analyses occur during the life of a system. Like other aspects of information processing systems, security is most effective and efficient if it is planned for and managed throughout a computer system's life cycle, from initial planning through design, implementation, and operation to disposal. Including security at the beginning and throughout the information system development life cycle (SDLC) will usually result in less expensive and more effective security implementation and operation.

## SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

## STANDARD

System lifecycle management shall have processes for initiation, requirements, development, implementation, operations and disposal. Processes shall include work flow, traceability, accountability, management authority and separation of duties.

System and application security shall be planned for and incorporated throughout the lifecycle.

Development and test activities shall be physically or logically separate from

Title:	System Lifecycle Management
--------	-----------------------------

production systems.

Developers shall not have access to production systems. If access is required, it shall be limited and audited.

All phases within the systems lifecycle shall include processes that result in the generation of the appropriate level of documentation, including, but not limited to, requirements and design specs, security plans, configuration guides, transition plans, training plans, user and administration manuals.

**RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES**

- System and Development Lifecycle (Policy)
- System Security Plans (Standard)
- System Design Documentation (Standard)
- System Implementation and Acceptance (Standard)
- System Operations Documentation (Standard)
- Operational Change Control (Standard)
- Media Disposal (Policy)

**REFERENCES**

- NIST SP 800-12 Introduction to Computer Security NIST Handbook (Ch 8)
- NIST SP 800-100 Information Security Handbook for Managers (Ch 3)
- NIST SP 800-64 Security Consideration for SDLC
- NIST SP 800-65 Integrating IT Security into the Capital Planning and Investments Controls Process

**TERMS and DEFINITIONS**

**System Development Lifecycle** is the overall process of developing, implementing, and retiring information systems and applications through a multi-step process from initiation, design, implementation, and maintenance to disposal.

Note: The PSG number was changed from S-08-025.01 on September 1, 2008.

Effective Date:	March 31, 2008	2 of 2
-----------------	----------------	--------