	Georgia Technology Authority	
Title:	**Systems Operations Documentation**	
PSG Number:	**SS-08-027**	
Effective Date:	03/31/2008	**Review Date:** 12/02/2004
Synopsis:	Establishes a requirement that system owners maintain system documentation and standard operating procedures	

PURPOSE

To adequately protect state information resources and facilities, personnel must understand their roles, responsibilities and how to perform them.

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency during system transition to operations and to maintaining the security support structure. System documentation and formalizing operational procedures with sufficient detail helps to eliminate security incidents and oversights, gives new personnel sufficiently detailed instructions and provides a quality assurance function to help ensure that system operations will be performed correctly and efficiently.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(8) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

STANDARD

All phases of the systems lifecycle shall have supporting documentation.

System owners shall formally document, approve and maintain detailed system and security operations and maintenance manuals/procedures for day-to-day and emergency IT operations.

System Owners shall ensure that documentation is current and personnel know where to find and how to reference them.

Operational documentation containing sensitive information shall be assigned an appropriate security categorization and protected from unauthorized access and disclosure.

Operations and maintenance documentation shall include, where applicable:

- System and communications build/configuration specifications
- Documented authorization from senior management official to operate

the system
- System administration/maintenance manuals
- Security Plans
- Security operations policy and procedures for:
    - Access Management
    - Data center security and safety
    - Incident Response and Handling
    - Baseline security configurations (OS, hardware/software, network, applications)
- Service Level Agreements
- Back-ups, storage and restore procedures
- Virus Update and Patch Management procedures
- Information, data, equipment and media handling, processing and disposal procedures
- Business Continuity, Contingency, Disaster response and recovery plans
- Change Management procedures

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Systems and Development Lifecycle (PS-08-018)
System Security Plans (SS-08-028)
System Implementation and Acceptance (SS-08-032)

REFERENCES

NIST SP800-64 Security Considerations for the Systems Development Lifecycle
NIST SP800-100 Information Security Handbook for Managers