	Georgia Technology Authority	
Title:	**System Security Plans**	
PSG Number:	**SS-08-028**	
Effective Date:	03/31/2008	**Review Date: 12/01/2024**
Synopsis:	Requires data and system owners to create and maintain system security plans	

PURPOSE

System security planning is an important activity in the system development lifecycle and should be ongoing throughout the system's lifecycle so that events such as system changes or new threats trigger the need for updated security controls that can be accurately documented and effectively managed.

The purpose of the system security plan is to provide a documented overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates the responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should accurately reflect the most current state of the system.

Oversight and independent audit groups use security plan documentation to make an assessment of the management, operational and technical controls detailed in the security plan and to verify that system management has done an adequate job to highlight areas where security may be lacking and to accurately reflect how the system is actually being operated. It also provides a basis for senior management officials to make informed, risk-based decisions to authorize a system to operate.

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*

Supplemental Authority: OCGA 50-18-72(a)(15)(A) Public disclosure shall not be required for records that the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, or public property, which shall be limited to the following: (i) Security plans and vulnerability assessments for any public utility, technology infrastructure, building, facility, function, or activity in effect at

the time of the request for disclosure or pertaining to a plan or assessment in effect at such time.

TERMS AND DEFINITIONS

System Security Plan - a formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Information System - an information system (hereafter referred to as 'system') is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

System - a generic term used for briefness to mean either a major application or a general support system. Boundaries for a 'system' must be determined by security and/or IT personnel familiar with the environment.

STANDARD

System security requirements and controls shall be planned for, managed and documented throughout the system lifecycle.

System security plans shall reflect input from various system stakeholders, including information owners, system owner and the agency information security officer.

Security plans are living documents that shall be developed, reviewed and updated throughout the systems lifecycle to accurately reflect the current state of the information system.

Security plans contain sensitive information and shall be protected from unauthorized access and disclosure. (Reference: Supplemental Authority)

Security plans shall contain the following details in accordance with NIST SP800-18:

- Key Contacts (ISO, Data Owner, System Owner, etc)
- System purpose or function
- Security Classification in accordance with FIPS 199
- Technical descriptions (hardware, software, communications)
- System boundaries, interconnections and data sharing agreements (MOUs/MOAs/SLAs)
- Description of security controls in accordance with NIST SP800-53

The following roles and responsibilities shall correspond with security plan

development and maintenance:

- Data Owner shall:
    - In coordination with System Owner, establish the security requirements and controls and formally document security plans for all operational information systems under their control
    - Review and approve the security plans prior to system operations or prior to major system changes
- System Owner and/or ISO shall:
    - Develop the security plan in coordination with the Data Owners
    - Ensure the system is developed, deployed and operated in accordance with the established security requirements detailed in the security plan
    - Establish a plan of action to mitigate vulnerabilities
    - Update and maintain the security plan consistent with and throughout the system lifecycle
    - Provide Sr. management an assessment of the effectiveness of controls, risks and mitigation plans associated with operating the information system
- CIO or other appointed senior management official shall:
    - Approve the security plan by formally authorizing the operation of the information system and accepting the risks provided by ISO
    - Deny or halt the operation of a system if the risks are unacceptable

REFERENCES

NIST SP800-18 Guide for Developing Security Plans for Federal Information Systems
NIST SP800-53 Security Controls for Federal Information Systems
NIST SP800-64 Security Consideration for SDLC

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Data Sharing (PM-07-003)
System Lifecycle Management (SS-08-025)
System Operations Documentation (SS-08-027)