IT Publications and Standards

**NATIONAL PUBLICATIONS and STANDARDS:**

- **NIST 800-53**: Recommended Security Controls for Federal Information Systems
- **NIST 800-12**: NIST Handbook, An Introduction to Computer Security
- **NIST 800-53A**: Security Self-Assessment Guide
- **NISTIR 7628**: Guidelines for Smart Grid Cybersecurity
- **FIPS 200**: Federal Information Processing Standards
- **ISO 7498-1**: Information Processing Systems OSI Basic Model
- **ISO 7498-2**: Information Processing Systems OSI Security Architecture

**GTA SECURITY POLICIES:**

- **Access Control** - PS-08-009
  Access to State information assets is to be controlled and monitored
- **Accountability of Assets** - PS-08-002
  Establishes accountability for all hardware and software acquired using public funds
- **Appropriate Use of Information Technology Resources** - PS-08-003
  Defines appropriate use IT resources
- **Business Continuity and Disaster Recovery** - PS-08-025
  Requires plans to maintain continuity of essential state government operations and services
- **Change Management** - PS-08-015
  Requirements for a formal change management process
- **Computer Security Incident Management** - PS-08-004
  Establishes the process for detecting and responding to security incidents
- **Data and Asset Categorization** - PS-08-012
  Provides for inventory and classification of state data and information processing systems
- **Enterprise Information Security Charter** - PS-08-005
  Commits the State of Georgia to protecting information systems and data from unauthorized disclosure, modification, use, or destruction
- **Information Security - Risk Management** - PS-08-031
  Requires a risk-based approach to information security management
**Media Controls** - PS-08-026
Requirements protection of system media from unauthorized disclosure, modification, destruction or loss

**Network Security - Information Flow** - PS-08-030
Requires protection of information traversing networks

**Network Security Controls** - PS-08-027
Requires network security controls

**Outsourced Facilities Management** - PS-08-019
Establishes requirements over outsourcing data processing facilities

**Password Authentication** - PS-08-006
Establishes use of passwords as primary authentication mechanism

**Personnel Security** - PS-08-014
Provides for identity verification of IT employees and contractors

**Physical and Environmental Security** - PS-08-013
Physical security is an essential element to the overall security of IT resources

**Protection from Malicious Software** - PS-08-021
Requires protections against malicious software

**Public Access Systems** - PS-08-028
Requires security controls on public facing systems

**Reliance on Electronic Records** - PS-08-007
Establishes the State’s intent to rely on electronic data as a form of official record and adherence to proscribed records retention requirements

**Remote Access** - PS-08-023
Requires protection from risks associated with remote access

**Security Awareness Program** - PS-08-010
Establishes a need to increase user security awareness through an awareness and training program

**Security Controls Review and Assessments** - PS-08-029
Establishes requirement for agencies to assess security controls for IT systems

**Security Log Management** - PS-08-022
Requires log management practices

**Separation of Production and Development Environments** - PS-08-020
Requires separation of production from development and test environments

**Systems and Development Lifecycle** - PS-08-018
Requirements for a formal IT lifecycle management program

**Third-Party Access** - PS-08-011
Provisions for third-party access to state facilities and information systems
Use of Cryptography - PS-08-024
Requires the use of cryptographic controls

I. GTA SECURITY STANDARDS

SS-08-001 - Appropriate Use and Monitoring
Standards for appropriate use and monitoring of IT resources

SS-08-002 - Classification of Personal Information
Standards for categorizing personal information

SS-08-003 - Data Security - Electronic Records
Electronic records are 1) relied upon as official records and 2) must adhere to records retention requirements and 3) must be protected from unauthorized destruction, modification or disclosure.

SS-08-004 - Incident Response and Reporting
Requirements for information security incident response and reporting

SS-08-005 - Information Security Infrastructure
Requirements for creating an information security program and infrastructure

SS-08-006 - Information Security Management Organization
Minimum standards for an information security management organization

SS-08-007 - Password Security
Establishes standards for protecting passwords

SS-08-008 - Strong Password Use
Establishes standards for creating and using strong passwords

SS-08-009 - Electronic Communications Accountability
Fixes accountability for content and transfer of information through electronic communications

SS-08-010 - Authorization and Access Management
Requires managed access to state facilities and information resources

SS-08-011 - Email Use and Protection
Standards for appropriate use and security of email

SS-08-012 - Security Education and Awareness
Requires all employees and contractors to attend annual security awareness training

SS-08-013 - Third-Party Security Requirements
Establishes security requirements for conducting business with contractors, outsourcing vendors and/or other third-parties

SS-08-014 - Data Categorization - Impact Level
Impact Level definitions and standards of information assets

SS-08-015 - Facilities Security
Incorporates facilities security into overall protection of IT assets
SS-08-016 - Computer Operations Center Security
Minimum security requirements for computer operations centers

SS-08-017 - Personnel Identity Verification and Screening
Standards for verifying identities of state personnel and contractors

SS-08-025 - System Lifecycle Management
Requires a formal lifecycle management program for systems in development or operations

SS-08-026 - Operational Change Control
Requires that changes to operational systems be controlled and monitored

SS-08-027 - Systems Operations Documentation
Requires agencies to document system operational procedures

SS-08-028 - System Security Plans
Requires data and system owners to create and maintain system security plans

SS-08-031 - Separate Production and Development Environments
Establishes requirements for separating operational environments from test/development environments

SS-08-032 - System Implementation and Acceptance
Requires agencies to establish criteria for accepting a system from development to operations

SS-08-033 - Malicious Code Incident Prevention
Establishes controls to protect systems against malicious software

SS-08-034 - Surplus Electronic Media Disposal
Establishes statewide standard on disposition of surplus electronic media

SS-08-035 - Media Sanitization - Vendor Return
Establishes standards for sanitization and disposal of all electronic media subject to vendor return

SS-08-036 - Log Management Infrastructure
Requires monitoring and analyzing systems logs to record events and detect anomalies

SS-08-037 - Teleworking and Remote Access
Security requirements for telework and remote access to state information systems

SS-08-038 - Secure Remote Access
Requires protection of systems from risks associated with remote access

SS-08-039 - Wireless and Mobile Computing
Minimum security requirements for wireless network implementation

SS-08-040 - Cryptographic Controls
Minimum requirements for the use of cryptographic controls
SS-08-041 - Risk Management Framework
Adopts the NIST risk management framework

SS-08-042 - Independent Security Assessments
Requires IT systems to be assessed by an independent third-party

SS-08-043 - Media Protection and Handling media

SS-08-044 - Outsourced IT Services and Third-Party Interconnections
Requires third-party adherence to established State security requirements

SS-08-045 - Contingency Planning
Requires plans to sustain or recover/restore critical operations in the event of a system disruption or disaster

SS-08-046 - Disaster Recovery - System Backup
Requires backup and recovery procedures for critical software and data

SS-08-047 - Network Security - Boundary Protection
Requires network boundary protection

SS-08-048 - Network Access and Session Controls
Requires control and monitoring of network sessions

SS-08-049 - Web and E-Commerce Security
Requires control and management of web services

SS-08-053 - Information Technology Reporting
Annual reporting requirements

SS-12-001 - Privacy in the Workplace
No expectation of privacy shall be assumed when accessing non-public State information resources and assets

SS-12-002 - Non-State Technology and Computing Devices
Rules of appropriate use and all other governance regarding information and data security apply to non-State issued technology devices used to access non-public State information and technology resources

SS-15-002 - Data Storage Location
Requires all data to be processed, stored, transmitted and disposed in the geographical United States