GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and systems supporting the operation and assets of the State.

SA-1 POLICY AND PROCEDURES

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, r5 Security and Privacy Controls.

The State has adopted the System and Service Acquisition principles established in National Institute of Standards and Technology (NIST) SP 800-53 “System and Service Acquisition” control guidelines as the official policy for this security domain. The “SA” designator identified in each control represents the NIST-specified identifier for the System and Service Acquisition control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections in this document outline the system and service acquisition requirements the State and executive-branch agencies shall implement and maintain.

This policy and associated procedures shall be reviewed and updated at least every three (3) years, or as State-defined events require more frequent review and update.

This policy and the associated procedures shall be developed, documented, and disseminated by the Agency Head, Chief Information Officer (CIO), Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level.

SA-2 ALLOCATION OF RESOURCES

Organizations shall expediently allocate resources for information security to provide rapid yet supervised allocation, ensuring the organization is modernized and protected against emerging and ongoing threats. Funding shall include allocation of resources for initial systems or system services acquisition and funding for their sustainment. The following shall be done:

a. Determine the high-level security and privacy requirements for the system or service in each mission or business-process planning.

b. Identify, document, and allocate the appropriate amount of resources which are required to protect the system or service as part of the capital planning and investment control process.
c. Establish discrete line items for information security and privacy in the budgeting process.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

Organizations shall acquire, develop, and manage systems using a System Development Life Cycle (SDLC) that incorporates information security and privacy considerations, including the following:

a. Identify qualified individuals having information security and privacy roles and responsibilities involved in creating the SDLC to ensure the system life cycle activities meet the security and privacy requirements for the State.
b. Define and document information security and privacy roles and responsibilities throughout the SDLC.
c. Integrate the agency information security and privacy risk management process into SDLC activities.
d. A business case justification of custom system development projects shall be required. When proposing the development of custom software, a strong business case shall:
    i. Support the rationale for not enhancing current systems
    ii. Demonstrate the inadequacies of packaged solutions
    iii. Justify the creation of custom software
e. A change management program shall be implemented which enables system engineers, architects, and security analysts to expediently perform necessary business functions, yet maintain a controlled, secure, and functioning environment.
f. The State/agencies shall plan for End-of-Life (EoL) and End-of-Support dates (EoS) for systems and services to ensure systems and services can receive security patches and updates throughout the system development lifecycle, and that the State is prepared to discontinue the system or service once no longer supported, or when security cannot be ensured.

Recommended Guidelines:

a. A general SDLC should include the following phases:
    i. Initiation
    ii. Acquisition/Development
    iii. Implementation/Assessment
    iv. Operations / Maintenance
    v. Sunset (disposition)
b. Each of these five phases should include a minimum set of tasks to incorporate security in the system development process. Including security early in the SDLC will usually result in less expensive and more effective security than retrofitting security into an operational system.
c. The following questions should be addressed in determining the security controls required for a system:
    i. How mission critical is it?

   ii. What are the security objectives required by the system, e.g., integrity, confidentiality, and availability?
   iii. What regulations, statutes, and policies are applicable in determining what is to be protected?
   iv. What are the applicable threats?
   v. What kinds of data will be used?

SA-4 ACQUISITION PROCESS

Functional security requirements shall be a part of any acquisition process. Agencies shall be capable of acquiring necessary solutions in an expedient manner in accordance with State requirements.

The following shall be done:

a. Security and privacy functional requirements shall include security capabilities, security functions, and security mechanisms.
b. Strength of mechanism requirements shall be determined by a categorization of the system and the information processed, stored, and transmitted based on an impact analysis. The process to determine a system categorization can be found in the NIST Federal Information Processing Standard 199 (FIPS 199) documentation. The results of this categorization will indicate a baseline of security controls to follow; either Low, Moderate, or High, and will correspond to the security controls identified in NIST SP 800-53.
c. Security and privacy assurance requirements shall include:
   i. Development processes, procedures, practices, and methodologies.
   ii. Evidence from development and assessment activities indicating the required security and/or privacy functionality is implemented, and the required security strength achieved.
d. Controls needed to satisfy security and privacy requirements.
e. Security and privacy documentation requirements.
f. Description of the information system development environment and environment in which the system is intended to operate.
g. Acceptance criteria requirements for assessing the ability of a system component, software, or system to perform intended functions.
h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management.
i. Vendor hardware design shall comply with information security and other State policies and standard security and technical specifications, such as:
   i. Adequate capacity to fulfill the functional requirements stated in the agency's design document.
   ii. Vendor-configured hardware security controls to adequately protect data. (Optionally, the vendor may assist the agency with the configuration of software security controls to provide adequate data protection on the vendor's hardware.)
j. Systems under consideration for acquisition shall be interoperable with current peripherals and systems.
k. Third-party applications shall be obtained from reputable sources to mitigate risk of covert channels exploitation.

l. Non-security functional and technical requirements shall be a part of the hardware, software, or firmware acquisition process.

m. Agencies shall follow State procurement policies when acquiring hardware to ensure that the purchase meets specified functional needs. Agencies shall include specific requirements for performance, reliability, cost, capacity, security, support, and compatibility in Requests for Proposals (RFPs) to rigorously evaluate quotes.

n. Agencies shall ensure vendor compliance with State and Federal security State and Federal laws, regulations, guidelines, standards, policies, and procedures. Agencies shall also obtain a Vendor Risk Assessment (VRA) for the vendor prior to contract approval. This document is intended to help agencies reach a decision for specific systems that will meet the State's security and compliance requirements. A VRA is required regardless of where the system is hosted.

o. New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by the agency.

SA-4 (1) ACQUISITION PROCESS – FUNCTIONAL PROPERTIES OF CONTROLS

Developer(s) of the system, system component, or information system service shall provide a description of the functional properties of the security controls to be employed. Functional properties of security controls describe the functionality (e.g., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

SA-4 (2) ACQUISITION PROCESS – DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS

Developer(s) of a system, system component, or information system service shall provide design and implementation information for the security controls to be employed that includes the following: security-relevant external system interfaces, high-level design, source code, or hardware schematics.

SA-4 (9) ACQUISITION PROCESS – FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE

Developer(s) of a system, system component, or information system service shall identify the functions, ports, protocols, and services intended for use.

SA-4 (10) ACQUISITION PROCESS – USE OF APPROVED PIV PRODUCTS

Agencies may use information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) within State systems.

SA-5 SYSTEM DOCUMENTATION

Organizations must obtain, develop, or document administrator and user documentation for the system, system component, or system service. Such documentation shall be distributed to designated agency officials that describes:

a. Secure configuration, installation, and operation of the system, component, or service.
b. Effective use and maintenance of security and privacy functions/mechanisms.
c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
d. User-accessible security and privacy functions/mechanisms and how to effectively use those functions/mechanisms.
e. Methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy.
f. End user responsibilities to maintain the security and privacy of the system.

The following shall also be done:

a. Ensure each new or updated system includes supporting system documentation and technical specifications of information technology hardware, whether the system is developed or updated by in-house staff or by a third-party vendor.
b. Create, manage, and secure system documentation libraries or data stores that are always available to only authorized personnel.
c. Ensure that system documentation is readily available to support the staff responsible for operating, securing, and maintaining new and updated systems.
d. Control system documentation to ensure that it is current and available for purposes such as auditing, troubleshooting, and staff turnover.
e. All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy.

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

Organizations shall apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of systems and their components.

Security and privacy engineering principles shall be primarily applied to new development information systems or systems undergoing major upgrades.

For legacy systems, agencies shall apply security engineering principles to system upgrades and modifications to the extent that it is technically configurable, given the current state of hardware, software, and firmware within those systems.

Security and privacy engineering principles shall include the following:

a. Developing layered protections.
b. Establishing sound security and privacy policy, architecture, and controls as the foundation for design.
c. Incorporating security and privacy requirements into the SDLC.
d. Delineating physical and logical security boundaries.
e. Ensuring that system developers are trained on how to build secure software.
f. Tailoring security and privacy controls to meet organizational and operational needs.
g. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk.

h. Reducing risk to acceptable levels, thus enabling informed risk management decisions.

SA-9 EXTERNAL SYSTEM SERVICES

Agencies shall require third parties and providers of external system services to comply with statewide information security and privacy requirements. Agencies shall employ controls as follows:

a. Define and document how external information systems comply with statewide information security and privacy controls to include user roles and responsibilities, and compliance auditing and reporting requirements. Agencies must ensure vendor compliance with State and Federal laws, regulations, guidelines, standards, policies, and procedures. It is also highly recommended that agencies obtain a third-party risk assessment prior to contract approval.
b. Monitor security and privacy control compliance by external service providers on an ongoing basis.
c. Restrict the location of information systems that receive, process, store, or transmit State and Federal data to the Continental United States (CONUS), United States Territories, Embassies and Military installations.
d. Agencies outsourcing their information processing shall ensure the service provider demonstrates compliance with State and Federal laws, regulations, guidelines, standards, policies, procedures, and related industry quality standards.
e. Outsourcing agreements shall include the following:
    i. The agency's course of action and remedy if the vendor's security and privacy controls are inadequate such that the confidentiality, integrity, or availability of the agency's data cannot be assured.
    ii. The vendor's ability to provide an acceptable level of processing and information security during contingencies or disasters.
    iii. The vendor's ability to provide processing in the event of failure(s).
f. To support service delivery, the outsourcing agreements shall contain, or incorporate by reference, all the relevant security and privacy requirements necessary to ensure compliance with the statewide information security standards, the agency's record retention schedules, its security policies, and its business continuity requirements.
g. Services, outputs, and products provided by third parties shall be reviewed and checked at least annually.
h. To monitor third party deliverables, agencies shall do the following:
    i. Monitor third-party service performance to ensure service levels meet contract requirements.
    ii. Review reports provided by third parties and arrange regular meetings as required by contract(s).
    iii. Resolve and manage any identified problem areas.
i. Contracts with vendors providing offsite hosting or cloud services that will host sensitive or confidential data must require the vendor to provide the State a third-party risk assessment due diligence response and supporting documentation such as, but not limited to Service Organization Control (SOC) 2 Type II, International Organization for Standardization (ISO) 27001, Federal Risk and Authorization Management Program (FedRAMP Moderate), or CSF (Common Security Framework) report before contract award and annually thereafter to

establish and maintain compliance with State policies.

j. Agencies shall approve any changes to services provided by a third party prior to implementation.
k. Agencies shall develop a process for engaging service providers and maintain a list of all service providers who store or share confidential data.
l. Agencies shall ensure that the service-level agreement (SLA) includes requirements for regular monitoring, review, and auditing of the service levels and security requirements as well as incident response and reporting requirements. The SLA shall state how the service provider is responsible for data stored or shared with the provider.
m. Agencies shall perform the monitoring, review, and auditing of services to monitor adherence to the SLA and identify new vulnerabilities that may present unreasonable risk. Agencies shall enforce compliance with the SLA and must be proactive with third parties to mitigate risk to a reasonable level.
n. Changes to an SLA and services provided shall be controlled through formal change management.
o. Agencies shall prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit confidential data, including Federal Tax Information (FTI), unless explicitly approved by OIT.

SA-9 (2) EXTERNAL SYSTEM SERVICES – IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES

Providers of external system services shall identify the functions, ports, protocols, and other services required for the use of such services. Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

System developers shall create and implement a configuration management plan that does the following:

a. Performs configuration management during system design, development, implementation, operation, and/or disposal for the following:
    i. Internal system development and system integration of commercial software.
    ii. External system development and system integration.
b. Documents, manages, and controls changes to the system or configuration items and the potential security and privacy impacts.
c. Implements only agency approved changes to the system.
d. Documents approved changes to the system.
e. Tracks security flaws and flaw resolution within the system.
f. Mitigates the risk of exploitation of covert channels by protecting the source code in custom developed applications.

SA-11 DEVELOPER TESTING AND EVALUATION

System developers shall assess for software faults that pose a security risk at all post-design stages of the system development life cycle prior to putting an application into production. The following shall be done:

a. Develop and implement a security and privacy assessment plan.
i. Develop and implement a plan that supports ongoing security and privacy assessments. Testing requirements must be defined and documented for both system development and system integration activities. The plan must include requirements for retesting after significant changes occur.
ii. Perform security testing/evaluation.
1. Sensitive or confidential data shall not be used for testing purposes, including FTI, unless explicitly approved by OIT or the agency owning the data.
2. Organizations may permit the use of production data during the testing of new systems or systems changes only when no other alternative allows for the validation of the functions and when permitted by other regulations and policies. Data anonymization or data masking tools shall be used if available.
3. If production data is used for testing, the same level of security controls required for a production system shall be used.
a. Produce evidence of the execution of the security and privacy assessment plan and the results of the security testing/evaluation
b. Implement a verifiable flaw remediation process.
c. Correct flaws identified during security testing/evaluation.
b. Teach and encourage software fault-reporting procedures through security training and awareness programs.
c. Designate a quality control team that consistently checks for faults and that is responsible for reporting them to software support.
d. Use a formal recording system for the following:
i. Tracking faults from initial reporting through to resolution.
ii. Monitoring the status of reported faults and confirms that satisfactory resolutions have been achieved.
iii. Providing reports and metrics for system development and software support management.
iv. Addressing and prioritizing prompt resolution of software faults to minimize the exposure resulting from the security vulnerability.
e. While faults are being tracked through to resolution, research shall also be conducted to ensure no security controls have been compromised and resolution activities have been appropriately authorized.
f. Perform unit, integration, and system regression testing/evaluation:
i. Require that information system developers/integrators perform a vulnerability assessment to document vulnerabilities, exploitation potential, and risk mitigations.
ii. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.
iii. To maintain the integrity of information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an

operational/production environment.

  iv. Test data and accounts shall be removed from an application or system prior to being deployed into a production environment if the application or system does not have a dedicated testing environment.
  v. Qualified personnel must certify that the upgrade or change has passed acceptance testing.
  vi. A rollback plan must be established in the event the upgrade or change has unacceptable ramifications.

g. The following issues and controls shall be included when developing acceptance criteria and acceptance test plans:
  i. Capacity requirements - both for performance and for the computer hardware needed.
  ii. Error response - recovery and restart procedures and contingency plans.
  iii. Routine operating procedures - prepared and tested according to defined policies.
  iv. Security controls - agreed to and put in place.
  v. Manual procedures - effective and available where technically configurable and appropriate.
  vi. Business continuity - meets the requirements defined in the business continuity plan.
  vii. Impact on production environment - able to demonstrate that installation of new system will not adversely affect current production systems (particularly at peak processing times).
  viii. Training - of operators, administrators, and users of the new or updated system.
  ix. Logs - logs of results shall be kept for a defined period once testing is completed.

h. Implement a verifiable flaw remediation process to correct security weaknesses and deficiencies identified during the security testing and evaluation process.

i. Controls that have been determined to be either absent or not operating as intended during security testing/evaluation must be remediated.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Developers of a system, system component, or system service shall follow a documented development plan that:

a. Explicitly addresses security requirements;
b. Identifies the standards and tools used in the development process;
c. Documents the specific tool options and tool configurations used in the development process; and
d. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

The development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy security and privacy requirements.

Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes.

Maintaining the integrity of changes to tools and processes assists effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development life cycle to track authorized changes and to prevent unauthorized changes.

SA-15 (3) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS – QUALITY METRICS

Developers of a system, system component, or system service shall:

a. Define quality metrics at the beginning of the development process; and
b. Provide evidence of meeting the quality metrics periodically, and at program review milestones and upon delivery.

Quality metrics are used by organizations to establish acceptable levels of system quality. Metrics may include quality gates to provide clear, unambiguous indications of progress. Quality gates are collections of completion criteria or sufficiency standards representing the satisfactory execution of specific phases of the system development project.

Other metrics apply to the entire development project. These metrics can include defining the severity thresholds of vulnerabilities. An example of this would be requiring no known vulnerabilities in the delivered system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

Agencies must replace system components when support for the components is no longer available from the developer, vendor, or manufacturer. Examples of system components can include, but are not limited to servers, workstations, laptops, and applications.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This is the first State of Alabama System and Services Acquisition Policy. All State agencies and vendors of the State are required to comply with the current implemented version of this policy.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	Daniel Urquhart
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK