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 Exemptions and Exceptions
e. Policy Reviews and Updates

SCOPE

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

All information assets that process, store, receive, transmit or otherwise could impact the confidentiality, integrity, and accessibility of State data must meet the security controls defined in this document as required by the State of Alabama's IT Governance Policy.

SR-1 POLICY AND PROCEDURES

The purpose of this policy and any supporting standard or procedure is to ensure the State's supply chain risks are appropriately identified, assessed, and managed to limit harm or consequences from supply chain-related events.

This document addresses the standards set forth by the State to implement the family of Supply Chain Risk Management security controls at the organization, process and/or system level for all State data and information assets.

The State has adopted the Supply Chain Risk Management security principles as defined in the State's IT Governance Policy. The "SR" designator identified in each control represents the NIST-specified identifier for the Supply Chain Risk Management 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 outline the Supply Chain Risk Management requirements which executive-branch agencies will implement and maintain to manage risks with sourcing, vendor management, and supply chain quality across State agencies.

This policy and associated procedures shall be reviewed at least every three (3) years, or more frequently, dependent upon State-defined events or information.

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

The following shall be implemented:

a. Develop a plan for managing supply chain risks associated with acquisition, delivery, integration, operations and maintenance, and disposal of the information systems and services:

   i. The Supply Chain Risk Management (SCRM) plan should provide the basis for determining whether a technology, service, or information system is fit for a specific purpose with appropriate controls.
   ii. The SCRM plan shall include the following:
      1. A statement of the supply chain risk tolerance.
      2. Acceptable supply chain risk mitigation strategies or controls.
      3. A process for consistently evaluating and monitoring supply chain risk.
      4. Approaches for implementing and communicating the plan.
      5. A description and justification for supply chain risk mitigation measures taken; and associated roles and responsibilities.

b. Review and update the supply chain risk management plan on a State-defined frequency or as required to address threat, organizational, or environmental changes.
c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

SR-2 (1) SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM

The following shall be implemented:

a. Establish a supply chain risk management team that consists of the State-defined roles and is responsible for identifying, assessing, and managing risks while using coordinated efforts;
b. The SCRM team shall consist of personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk managers, information technology, contracting, information security, privacy, mission, or business, legal, supply chain, and logistics and acquisition; and
c. The SCRM team shall be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES

The State shall:

a. Establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems in coordination with the identified supply chain personnel.
   i. Supply chain elements include organizations, entities, or tools employed for the acquisition, delivery, integration, operations and maintenance, and disposal of systems and their components.
   ii. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.
b. Use the following controls to mitigate supply chain risks to information assets, systems, components, and services to limit the harm or consequences from supply chain-related events:

i. Control Assessments (CA-Assessment, Authorization and Monitoring)
ii. External System Services (SA-Systems and Services Acquisition)
iii. Acquisition Process (SA-Systems and Services Acquisition)
iv. Controlled Maintenance (MA-Maintenance)
v. Component Authenticity (SR-11 Supply Chain Risk Management)
vi. Component Disposal (SR-12 Supply Chain Risk Management)

c. Document the selected and implemented supply chain processes and controls in a State-defined document such as a SCRM plan.

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

Acquisition strategies, contract tools, and procurement methods shall be employed to protect against, identify, and mitigate supply chain risks. Examples are as follows:

a. Incentive programs to system integrators, suppliers, or external services providers to ensure they provide verification of integrity and traceability;
b. Requiring tamper-evident packaging; and
c. Using trusted or controlled distribution.

SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

Supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide shall be assessed and reviewed annually.

An assessment and review of supplier risk should include security and supply chain risk management processes; foreign ownership, control, or influence (FOCI); and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors.

The reviews shall consider documented processes, documented controls, and publicly available information related to the supplier or contractor.

SR-8 NOTIFICATION AGREEMENTS

Agreements and procedures with entities involved in the supply chain shall be established for the notification of supply chain compromises including security incident and a privacy breach and the notification of assessment or audit results.

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

A process to inspect information systems annually or upon any indications of the tampering of information systems shall be implemented.

Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

SR-11 COMPONENT AUTHENTICITY

The following shall be implemented:

a. Develop and implement anti-counterfeit policy and procedures including the means to detect and prevent counterfeit components from entering the system;

b. Report counterfeit system components to State-specified personnel; and
c. The State anti-counterfeit policy and procedures ensure components acquired and used are authentic and not tampered with.

SR-11 (1) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING

The following State-defined roles shall be trained to detect counterfeit system components (including hardware, software, and firmware):

a. Personnel conducting configuration management activities
b. System Administrators
c. Database Administrators
d. Network Administrators
e. Personnel conducting procurement activities

SR-11 (2) COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR

The State shall maintain configuration control over system components awaiting service or repair and serviced or repaired components pending return to service.

Organizations shall manage risks associated with component repair including the repair process and any replacements, updates, and revisions of hardware and software components within the supply chain.

SR-12 COMPONENT DISPOSAL

Defined data, documentation, tools, or system components shall be disposed of without exposing sensitive or operational information that could compromise the supply chain.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This is the first State of Alabama Supply Chain Risk Management 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
01/14/2025	Policy Created

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