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 information systems that support the operation and assets of the State.

The State has adopted the Risk Assessment security principles established in NIST SP 800-53 r 5, “Risk Assessment” control guidelines as the official policy for this security domain. The “RA” designator in each control represents the NIST-specified identifier for the Risk Assessment Control family. The following subsections outline requirements the State must implement and maintain to be compliant with this policy. 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.

This policy and associated procedures shall be reviewed and updated at least every three (3) years, or when State-defined events necessitate off-cycle assessment and updates.

RA-1 POLICY AND PROCEDURES

All information assets that process, store, receive, transmit or otherwise impact confidentiality, integrity, and accessibility of State data must meet the required security controls defined in this policy based on the NIST SP 800-53 r5, Risk Assessment Controls.

This document addresses the requirements set forth by the State to implement the family of Risk Assessment security controls at the organization, process and/or system level to protect the confidentiality, integrity, and availability of State information systems and data.

Risk management includes the identification, analysis, and management of risks associated with State information, business, IT systems, and physical security infrastructure to protect the state’s information technology assets, personnel, and business viability.

The State shall implement Risk Management program to ensure timely and reliable delivery of critical automated business services to the citizens of Alabama.

The Risk Management Program should establish a structured risk assessment process, prioritize assessments based on data and system criticality, identify threats, vulnerabilities, and continuously monitor/address those vulnerabilities. This program must include risk identification, classification, prioritization, mitigation and additionally provide for continuous improvement.

The Risk Management program at a minimum will focus on four types of activities:

a. **Identification of Risks:** A continuous effort to identify risks likely to affect business continuity and security functions;
b. **Analysis of Risks**: An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other;
c. **Mitigation Planning**: Decisions and actions to reduce risk impact, limit the probability of occurrence, or improve the response to an occurrence. For moderate or high rated risks, mitigation plans should be developed, documented, and assigned to management or specially designated and trained personnel. Plans should include individual accountability; and
d. **Tracking and Controlling Risks**: Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

Security Risk Management

The focus of security risk management is assessing security risks jeopardizing State assets, information, business functions, or services and addressing those risks with security risk impact analyses.

Agencies should identify those impacts to develop strategies and allocate required resources to provide appropriate prevention levels and responses. Risk assessments are important for protecting critical State functions and services and include but are not limited to:

a. Identification of the Federal, State, and local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for agency functions or services.
b. Identification of confidential information stored in the State's files and the potential for fraud, misuse, or other illegal activity.
c. Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical State functions and service.
d. Identification of the processes used to monitor and report to management on whatever applications, tools, and technologies the agency has implemented to adequately manage the risk as defined by the agency (e.g., baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).
e. Identification of agency's IT Change Management and Vulnerability Assessment processes.
f. Identification of security mechanisms in place to preserve and protect the confidentiality, integrity and availability of State data and systems (e.g., encryption, PKI, etc.).

RA-2 SECURITY CATEGORIZATION

Information is defined as ALL data, regardless of form or characteristics, created, stored, processed, transmitted, or received in connection with the transaction of State business. Information shall be classified and handled to protect it from unauthorized or accidental disclosure, modification, or loss.

All agencies (including OIT) shall address the following requirements:

a. Systems and the information processed, stored, transmitted, and received shall be categorized in accordance with applicable State and Federal laws, policies, regulations, standards, and guidance.
b. Security categories are based on anticipated impact if certain events occur to jeopardize the

confidentiality, integrity, and availability of the information and systems needed by the State to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain business as usual function, and protect individuals. The impact to the agency, State, personnel, and other external entities should be considered during the security categorization process.

c. System owners shall be involved with security categorization of an information system if that system shares information or interconnects with another system inheriting its security control(s) from their system.

d. The security categorization process shall be included in the system development lifecycle (SDLC), and security categorizations shall be developed in the initiation stage to ensure implementation of appropriate security controls throughout the SDLC.

e. Verify that the security categorization decision is reviewed and approved by the authorized or designated representative.

f. Update documents reflecting changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

g. The business owner, system owner, and supporting security personnel shall be identified and must assist with the development of the security categorization.

RA-3 RISK ASSESSMENT

Risk assessments consider risks posed to State agency operations and assets, or individuals from external parties, including but not limited to service providers; contractors operating agency information systems; individuals accessing State data and information systems; and outsourcing organizations.

Threats and vulnerabilities shall be identified in systems as part of the risk assessment process and security/risk assessments shall be conducted to evaluate the level of risk, including the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information contained.

Organizations shall also conduct privacy/risk assessments to evaluate the level of risk, including the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information (PII). Results from these assessments will be integrated with system-level risk assessments.

The State and its agencies will conduct security/risk assessments at least annually or when State-defined events require increased frequency.

Executive-branch agencies shall conduct an agency-wide third-party assessment of all critical systems (sensitive or confidential) and associated security controls at least every three (3) years.

The risk assessment(s) shall include a Likelihood Determination based on threat element motivation, vulnerability type, and existing control measures with a rating assigned to the vulnerability as indicated in Table 1 below:

Likelihood	Definition
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

Low	The threat source lacks motivation or capability, or controls are in place to prevent or significantly impede the vulnerability from being exercised.

Table 1: Likelihood Level Definitions

Risk assessment(s) shall include an impact analysis based on Table 2 below:

Magnitude	**Impact Definition**
High	Event could create a severe or catastrophic effect on State operations, assets, or individuals; and cause a loss of mission capability that poses a threat to human life or results in major asset loss.
Medium	Event could create serious adverse effects on State operations, assets, or individuals; cause significant degradation in mission capability; place the agency at a significant disadvantage; or result in major damage to assets requiring extensive corrective actions or repairs.
Low	Event could have limited adverse effect on State operations and cause negative outcomes with limited damage to operations or assets requiring minor corrective actions.

Table 2: Impact Definitions

RA-3 (1) RISK ASSESSMENT – SUPPLY CHAIN ASSESSMENT

Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information, and therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State. The supply chain-related events may be unintentional or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

As such, the State and its agencies will:

a. Assess supply chain risks associated with any information system or its components used to process, store, receive, or transmit data classified as sensitive or confidential.
b. Update the supply chain risk assessment at least every three (3) years, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

RA-5 VULNERABILITY MONITORING AND SCANNING

Monitor and scan for vulnerabilities in the system and hosted applications and when new vulnerabilities potentially affecting the system are identified and reported.

a. Employ vulnerability monitoring tools and techniques to foster interoperability among tools and automate parts of the vulnerability management process.
b. Analyze vulnerability scan reports and results from vulnerability monitoring.

c. Remediate legitimate vulnerabilities in accordance with an organizational assessment of risk.

d. Share information internally and interagency when obtained from the vulnerability monitoring process and control assessments to help eliminate similar vulnerabilities in other systems.

e. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5 (2) VULNERABILITY MONITORING AND SCANNING – UPDATE VULNERABILITIES TO BE SCANNED

Lists of system vulnerabilities shall be updated prior to a new scan or when new vulnerabilities are identified and reported.

RA-5 (5) VULNERABILITY MONITORING AND SCANNING – PRIVILEGED ACCESS

Privileged access authorization to an information system shall be implemented for vulnerability scanning activities. Thorough vulnerability scanning may be more intrusive and information system data scanned may reveal sensitive or confidential information.

RA-5 (11) VULNERABILITY MONITORING AND SCANNING – PUBLIC DISCLOSURE PROGRAM

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

RA-7 RISK RESPONSE

Findings from security and privacy assessments, monitoring, and audits shall be documented using a Plan of Action and Milestones (POA&M) as discussed in the CA Assessment Authorization and Monitoring Policy.

RA-9 CRITICALITY ANALYSIS

Identify critical system components and functions by performing a criticality analysis for any system or components storing, processing, or transmitting sensitive or confidential data at each stage of the SDLC.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This current policy supersedes all previous versions. All State agencies and contractors/vendors of the State are expected to comply with the current implemented version.

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