GOVERNANCE

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

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 including those used, managed, or operated by a contractor, 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 supporting the operation and assets of the State.

APPLICABILITY

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. These controls are based on the National Institute of Standards and Technology (NIST) SP 800-53, r5 Planning Controls. This document addresses the requirements set forth by the State of Alabama to implement the family of Security Planning security controls at the organization, process, and/or system level for all information assets/State data.

PL-1 POLICY AND PROCEDURES

The State of Alabama (State) has adopted the Security Planning principles established in NIST SP 800-53, “Security Planning” control guidelines as the official policy for this security domain. The “PL” designator identified in each control represents the NIST-specified identifier for the Security Planning 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.

This policy provides requirements for the security planning process, which is essential to ensure that information systems are designed and configured using controls sufficient to safeguard the State’s information systems. The policy and associated procedures will be reviewed and/or updated at least every three (3) years or following State-defined events requiring off-cycle review and changes.

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

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

This policy applies to all information systems managed by Alabama OIT, including those used, managed, or operated by contractors or other organizations on behalf of the State. The policy encompasses all critical systems and must align with the agency’s enterprise architecture.

The State shall:

a. Include all critical systems and be consistent with the agency's enterprise architecture;
b. Explicitly define the constituent system components, e.g., the authorization boundary for the system, which includes all components authorized for operation by an agency head or delegate and excludes separately authorized systems connected to the information system;
c. Describe the operational context of the information system in terms of mission and business processes;
d. Identify individuals that fulfill system roles and responsibilities;
e. Identify the information types processed, stored, and transmitted by the system;
f. Describe any specific threats to the system that are of concern to the organization;
g. Provide the results of a privacy risk assessment for systems processing sensitive or confidential data;
h. Provide an overview of the privacy requirements for the system;
i. Identify any relevant control baselines or overlays;
j. Describe the controls in place or planned for meeting the privacy requirements;
k. Include risk determinations for security and privacy architecture and design decisions;
l. Include security and privacy-related activities affecting the system that require planning and coordination with agency-defined individuals or groups;
m. Provide the security categorization of the information system, including supporting rationale;
n. Describe the operational environment for the information system;
o. Describe relationships and/or interconnections with other information systems;
p. Provide an overview of the security and privacy requirements for the information system;
q. Describe the security controls in place or planned for meeting those requirements, including a rationale for the tailoring and supplementation decisions;
r. Ensure the security and privacy plan is reviewed and approved by the authorized representative before implementation;
s. Distribute copies of the security and privacy plan and communicate subsequent changes to appropriate agency personnel;
t. Review the security and privacy plan for the information system at least annually;
u. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
v. Explicitly define the information systems that receive, process, store, or transmit sensitive or confidential data.

PL-4 RULES OF BEHAVIOR

Rules of behavior represent a type of access agreement for organizational users. Other types of access agreements include nondisclosure agreements, conflict-of-interest agreements, and acceptable use agreements. Organizations will consider rules of behavior based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users. Documented acknowledgements for rules of behavior include electronic agreement check boxes or radio buttons and must have either an electronic or physical signature.

a. Establish and provide to individuals requiring access to the system the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
b. Receive a documented acknowledgment from such individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to information and the system;
c. Review and update the rules of behavior at least annually; and
d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

PL-4 (1) RULES OF BEHAVIOR – SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS

Include in the rules of behavior restrictions on:

a. Use of social media, social networking sites, and external sites/applications;
b. Posting organizational information on public websites; and
c. Use of organization-provided identifiers (i.e., email addresses) and authentication secrets (i.e., passwords) for creating accounts on external sites/applications.

PL-8 SECURITY AND PRIVACY ARCHITECTURES

The statewide technical architecture shall be utilized as a requirement for the project review process. Information security and privacy architectures shall include the following:

a. Description of the requirements and approach to be taken regarding protecting the confidentiality, integrity, and availability of State or federal information.
b. Description of the requirements and approach to be taken for processing sensitive and confidential data to minimize privacy risk to individuals.
c. Description of how the information security and privacy architectures are integrated into and support the enterprise architecture.
d. Description of any information security and privacy assumptions about, and dependencies on, external systems and services.
e. An annual review and update of the information security and privacy architectures to reflect changes in the enterprise architecture.
f. Planned architecture changes shall be reflected in the Security and Privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PL-10 BASELINE SELECTION

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or to address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints.

The State has selected the Moderate control baseline as provided in NIST 800-53 r5 and applied that baseline when creating and/or updating the most current State policies.

PL-11 BASELINE TAILORING

The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success.

The State has selected to follow the tailoring guidance as provided in NIST 800-53B r5 and applied that guidance when creating and/or updating the most current State policies. Agencies that have more restrictive guidance and/or standards that must be followed (e.g., IRS Publication 1075, HIPAA, etc.) will need to further tailor their own policies to account for any items not defined by a particular State policy.

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	01/13/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK